Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: AC-01 -Access Control Policy And Procedures

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:
1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
b. Reviews and updates the current:
1. Access control policy [%Assignment: organization-defined frequency (b)(1)%]; and
2. Access control procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: HUD IT security policy (inclusive of access control) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Access control compliance policy is specifically addressed in Sections 4.6.1, 5.2, 5.2.1, 5.2.2, and 5.2.3 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 5.2 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a hybrid common control, the implementation of which is the responsibility of the HUD Office of IT Security.
Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented access control policy within Section 5.2. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to access controls. The access control policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The access control procedures to facilitate the implementation of the access control policy and associated access security controls are documented within the Section 5.2 of the Information Technology Security Procedures, dated November 1, 2013. The access control procedures contained within the Information Technology Security Procedures is disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal. The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: AC-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Access control policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with access control responsibilities
* Organizational personnel with information security responsibilities

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-01 (a)(01)[01] - The organization develops and documents an access control policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AC-01 (a)(01)[02] - The organization defines personnel or roles to whom the access control policy are to be disseminated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: HUD IT security policy (inclusive of access control) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Access control compliance policy is specifically addressed in Sections 4.6.1, 5.2, 5.2.1, 5.2.2, and 5.2.3 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 5.2 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
Implementation Statement for Develop IT Security Standards and Policy
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented access control policy within Section 5.2. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to access controls.
The access control policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The access control procedures to facilitate the implementation of the access control policy and associated access security controls are documented within the Section 5.2 of the Information Technology Security Procedures, dated November 1, 2013.
The access control procedures contained within the Information Technology Security Procedures is disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: Referred to HUD IT security policy

Determine If Statement: AC-01 (a)(01)[03] - The organization disseminates the access control policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the access control policy and associated access control controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AC-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: HUD IT security policy (inclusive of access control) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Access control compliance policy is specifically addressed in Sections 4.6.1, 5.2, 5.2.1, 5.2.2, and 5.2.3 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 5.2 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
Implementation Statement for Develop IT Security Standards and Policy
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented access control policy within Section 5.2. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to access controls. The access control policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The access control procedures to facilitate the implementation of the access control policy and associated access security controls are documented within the Section 5.2 of the Information Technology Security Procedures, dated November 1, 2013. The access control procedures contained within the Information Technology Security Procedures is disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal. The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: Referred to HUD IT security policy

Determine If Statement: AC-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AC-01 (b)(01) - The organization
* defines the frequency to review and update the current access control policy;
* reviews and updates the current access control policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AC-01 (b)(02)[01] - The organization defines the frequency to review and update the current access control procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-01 (b)(02)[02] - The organization reviews and updates the current access control procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: AC-02 -Account Management

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [%Assignment: organization-defined information system account types%];
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by [%Assignment: organization-defined personnel or roles%] for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [%Assignment: organization-defined procedures or conditions%];
g. Monitors the use of information system accounts;
h. Notifies account managers:
1. When accounts are no longer required;
2. When users are terminated or transferred; and
3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements [%Assignment: organization-defined frequency%]; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Implementation Statement: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year. Terminations occur with "HUD Gone" action as they occur.

Assessment Objective: AC-2 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Access control policy
* Procedures addressing account management
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* List of active system accounts along with the name of the individual associated with each account
* List of conditions for group and role membership
* Notifications or records of recently transferred, separated, or terminated employees
* List of recently disabled information system accounts along with the name of the individual associated with each account
* Access authorization records
* Account management compliance reviews
* Information system monitoring records
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with account management responsibilities
* System/network administrators
* Organizational personnel with information security responsibilities

Test

* Organizational processes account management on the information system
* Automated mechanisms for implementing account management

Determine If Statement: AC-02 (a)[01] - The organization defines information system account types to be identified and selected to support organizational missions/business functions.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: TRACS Security Officer specifies intranet access based on
authorized users of the information system;
Supervisor's request for role or action codes.
Account managers grant internet access based on authorized access and account assignment.
Annually the project manager reviews inactive accounts for removal.

Actual Methods and Objects: Examined SSP; Data Control Group tracks number of accounts.

Determine If Statement: AC-02 (a)[02] - The organization identifies and selects organization-defined information system account types to support organizational missions/business functions.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (b) - The organization assigns account managers for information system accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (c) - The organization establishes conditions for group and role membership.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-02 (d) - The organization specifies for each account (as required):
* authorized users of the information system;
* group and role membership;
* access authorizations (i.e., privileges);
* other attributes.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (e)[01] - The organization defines personnel or roles required to approve requests to create information system accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (e)[02] - The organization requires approvals by organization-defined personnel or roles for requests to create information system accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (f)[01] - The organization defines procedures or conditions to:
* create information system accounts;
* enable information system accounts;
* modify information system accounts;
* disable information system accounts;
* remove information system accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (f)[02][a] - The organization in accordance with organization-defined procedures or conditions creates information system accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (f)[02][b] - The organization in accordance with organization-defined procedures or conditions enables information system accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-02 (f)[02][c] - The organization in accordance with organization-defined procedures or conditions modifies information system accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (f)[02][d] - The organization in accordance with organization-defined procedures or conditions disables information system accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (f)[02][e] - The organization in accordance with organization-defined procedures or conditions removes information system accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (g) - The organization monitors the use of information system accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (h)(01) - The organization notifies account managers when accounts are no longer required.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (h)(02) - The organization notifies account managers when users are terminated or transferred.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (h)(03) - The organization notifies account managers when individual information system usage or need to know changes.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (i)(01) - The organization authorizes access to the information system based on; a valid access authorization.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-02 (i)(02) - The organization authorizes access to the information system based on; intended system usage.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (i)(03) - The organization authorizes access to the information system based on; other attributes as required by the organization or associated missions/business functions.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (j)[01] - The organization defines the frequency to review accounts for compliance with account management requirements.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (j)[02] - The organization reviews accounts for compliance with account management requirements with the organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Determine If Statement: AC-02 (k) - The organization establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts once a year.

Actual Methods and Objects: Examined SSP

Control Title: AC-02(1) -Automated System Account Management

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization employs automated mechanisms to support the management of information system accounts.

Implementation Statement: TRACS manages accounts through the CHAMPS request process to activate, modify, disable or remove user access. The HUDGone process in CHAMPS is used by TRACS security administrator to remove all access to the system when a user leaves the organization or the project.

Assessment Objective: AC-2(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing account management
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with account management responsibilities
* System/network administrators
* Organizational personnel with information security responsibilities
* System developers

Test
* Automated mechanisms implementing account management functions

Determine If Statement: AC-02(01) - The organization employs automated mechanisms to support the management of information system accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: TRACS manages accounts through the CHAMPS request process to activate, modify, disable or remove user access. The HUDGone process in CHAMPS is used by TRACS security administrator to remove all access to the system when a user leaves the organization or the project.

Actual Methods and Objects: Reviewed SSP

Control Title: AC-02(2) -Removal Of Temporary / Emergency Accounts

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system automatically [%Selection: removes; disables%] temporary and emergency accounts after [%Assignment: organization-defined time period for each type of account%].

Implementation Statement: The SSA grants role and action based access, as needed. Temporary WASS accounts are not authorized to access TRACS.

Assessment Objective: AC-2(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing account management
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system-generated list of temporary accounts removed and/or disabled
* Information system-generated list of emergency accounts removed and/or disabled
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with account management responsibilities
* System/network administrators
* Organizational personnel with information security responsibilities
* System developers

Test
* Automated mechanisms implementing account management functions

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-02(02) [01] - The organization defines the time period after which the information system automatically removes or disables temporary and emergency accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The information system does not automatically terminate temporary and emergency accounts after 48 hours.

Actual Methods and Objects: 27 days as defined

Determine If Statement: AC-02(02) [02] - The information system automatically removes or disables temporary and emergency accounts after the organization-defined time period for each type of account.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The information system does not automatically terminate temporary and emergency accounts after 48 hours.

Actual Methods and Objects: 27 days as defined

Control Title: AC-02(3) -Disable Inactive Accounts

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system automatically disables inactive accounts after [%Assignment: organization-defined time period%].

Implementation Statement: The information system automatically disables inactive accounts after 27 Days.

Assessment Objective: AC-2(3) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing account management
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system-generated list of temporary accounts removed and/or disabled
* Information system-generated list of emergency accounts removed and/or disabled
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with account management responsibilities
* System/network administrators
* Organizational personnel with information security responsibilities
* System developers

Test
* Automated mechanisms implementing account management functions

Determine If Statement: AC-02(03) [01] - The organization defines the time period after which the information system automatically disables inactive accounts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The information system automatically disables inactive accounts after 27 Days.

Actual Methods and Objects: Reviewed Rev3

Determine If Statement: AC-02(03) [02] - The information system automatically disables inactive accounts after the organization-defined time period.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The information system automatically disables inactive accounts after 27 Days.

Actual Methods and Objects: Reviewed Rev3

Control Title: AC-02(4) -Automated Audit Actions

Applicability: Applicable **Result:** Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [%Assignment: organization-defined personnel or roles%].

Implementation Statement: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals

Assessment Objective: AC-2(4) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing account management
* Information system design documentation
* Information system configuration settings and associated documentation
* Notifications/alerts of account creation, modification, enabling, disabling, and removal actions
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with account management responsibilities
* System/network administrators
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms implementing account management functions

Determine If Statement: AC-02(04) [01][a] - The information system automatically audits the following account actions creation.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals

Actual Methods and Objects: Reviewed Rev3

Determine If Statement: AC-02(04) [01][b] - The information system automatically audits the following account actions modification.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals

Actual Methods and Objects: Reviewed Rev3

Determine If Statement: AC-02(04) [01][c] - The information system automatically audits the following account actions enabling.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals

Actual Methods and Objects: Reviewed Rev3

Determine If Statement: AC-02(04) [01][d] - The information system automatically audits the following account actions disabling.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals

Actual Methods and Objects: Reviewed Rev3

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-02(04) [01][e] - The information system automatically audits the following account actions removal.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals

Actual Methods and Objects: Reviewed Rev3

Determine If Statement: AC-02(04) [02] - The organization defines personnel or roles to be notified of the following account actions:
* creation;
* modification;
* enabling;
* disabling;
* removal.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals

Actual Methods and Objects: Reviewed Rev3

Determine If Statement: AC-02(04) [03][a] - The information system notifies organization-defined personnel or roles of the following account actions creation.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals

Actual Methods and Objects: Reviewed Rev3

Determine If Statement: AC-02(04) [03][b] - The information system notifies organization-defined personnel or roles of the following account actions modification.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals

Actual Methods and Objects: Reviewed Rev3

Determine If Statement: AC-02(04) [03][c] - The information system notifies organization-defined personnel or roles of the following account actions enabling.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals

Actual Methods and Objects: Reviewed Rev3

Determine If Statement: AC-02(04) [03][d] - The information system notifies organization-defined personnel or roles of the following account actions disabling.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals

Actual Methods and Objects: Reviewed Rev3

Determine If Statement: AC-02(04) [03][e] - The information system notifies organization-defined personnel or roles of the following account actions removal.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/12/2015

Finding: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals

Actual Methods and Objects: Reviewed Rev3

Control Title: AC-03 -Access Enforcement

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Implementation Statement: The information system enforces assigned authorizations for logical access to the system in accordance with applicable policy.

Assessment Objective: AC-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing access enforcement
* Information system design documentation
* Information system configuration settings and associated documentation
* List of approved authorizations (user privileges)
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with access enforcement responsibilities
* System/network administrators
* Organizational personnel with information security responsibilities
* System developers

Test
* Automated mechanisms implementing access control policy

Determine If Statement: AC-03 - The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

Actual Methods and Objects: Reviewed SSP

Control Title: AC-04 -Information Flow Enforcement

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [%Assignment: organization-defined information flow control policies%].

Implementation Statement: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Assessment Objective: AC-4 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Information flow control policies
* Procedures addressing information flow enforcement
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system baseline configuration
* List of information flow authorizations
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developers

Test
* Automated mechanisms implementing information flow enforcement policy

Determine If Statement: AC-04 [01] - The organization defines information flow control policies to control the flow of information within the system and between interconnected systems.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-04 [02] - The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Actual Methods and Objects: Reviewed SSP

Control Title: AC-05 -Separation Of Duties

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Separates [%Assignment: organization-defined duties of individuals%];
b. Documents separation of duties of individuals; and
c. Defines information system access authorizations to support separation of duties.

Implementation Statement: The information system enforces separation of duties through assigned access authorizations.

Assessment Objective: AC-5 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Access control policy
* Procedures addressing divisions of responsibility and separation of duties
* Information system configuration settings and associated documentation
* List of divisions of responsibility and separation of duties
* Information system access authorizations
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Automated mechanisms implementing separation of duties policy

Determine If Statement: AC-05 (a)[01] - The organization defines duties of individuals to be separated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces separation of duties through assigned access authorizations

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-05 (a)[02] - The organization separates organization-defined duties of individuals.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces separation of duties through assigned access authorizations

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-05 (b) - The organization documents separation of duties.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces separation of duties through assigned access authorizations

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-05 (c) - The organization defines information system access authorizations to support separation of duties.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces separation of duties through assigned access authorizations

Actual Methods and Objects: Reviewed SSP

Control Title: AC-06 -Least Privilege

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Implementation Statement: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Assessment Objective: AC-6 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Access control policy
* Procedures addressing least privilege
* List of assigned access authorizations (user privileges)
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Automated mechanisms implementing least privilege functions

Determine If Statement: AC-06 - The organization employs the principle of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Actual Methods and Objects: Reviewed SSP

Control Title: AC-06(1) -Authorize Access To Security Functions

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization explicitly authorizes access to [%Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information%].

Implementation Statement: Access to security functions for the information system is authorized only for the system administrator(s), TRACS Security Officer.

Assessment Objective: AC-6(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Access control policy
* Procedures addressing least privilege
* List of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Automated mechanisms implementing least privilege functions

Determine If Statement: AC-06(01) [01] - The organization defines security-relevant information for which access must be explicitly authorized.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: Access to security functions for the information system is authorized only for the system administrator(s), TRACS Security Officer.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-06(01) [02] - The organization defines security functions deployed in:
* hardware;
* software;
* firmware.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: Access to security functions for the information system is authorized only for the system administrator(s), TRACS Security Officer.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-06(01) [03][a] - The organization explicitly authorizes access to organization-defined security functions.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: Access to security functions for the information system is authorized only for the system administrator(s), TRACS Security Officer.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-06(01) [03][b] - The organization explicitly authorizes access to security-relevant information.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: Access to security functions for the information system is authorized only for the system administrator(s), TRACS Security Officer.

Actual Methods and Objects: Reviewed SSP

Control Title: AC-06(2) -Non-Privileged Access For Nonsecurity Functions

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization requires that users of information system accounts, or roles, with access to [%Assignment: organization-defined security functions or security-relevant information%], use non-privileged accounts or roles, when accessing nonsecurity functions.

Implementation Statement: The organization requires that users with access to security functions use non-privileged roles when accessing other system functions. All roles are audited.

Assessment Objective: AC-6(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing least privilege
* List of system-generated security functions or security-relevant information assigned to information system accounts or roles
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Automated mechanisms implementing least privilege functions

Determine If Statement: AC-06(02) [01] - The organization defines security functions or security-relevant information to which users of information system accounts, or roles, have access.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization requires that users with access to security functions use non-privileged roles when accessing other system functions. All roles are audited.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-06(02) [02] - The organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing nonsecurity functions.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization requires that users with access to security functions use non-privileged roles when accessing other system functions. All roles are audited.

Actual Methods and Objects: Reviewed SSP

Control Title: AC-06(5) -Privileged Accounts

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization restricts privileged accounts on the information system to [%Assignment: organization-defined personnel or roles%].

Implementation Statement: The organization restricts privileged accounts on the information system, such as TRACS Security Officer assigns office and role access to TRACS users. Some HQ users can access all offices. There are no super user accounts and data changes go through an approval process.

Assessment Objective: AC-6(5) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing least privilege
* List of system-generated privileged accounts
* List of system administration personnel
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Automated mechanisms implementing least privilege functions

Determine If Statement: AC-06(05) [01] - The organization defines personnel or roles for which privileged accounts on the information system are to be restricted.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: HUD's TRACS Security Officer assigns pre-defined roles to personnel as requested by a supervisor or administrator for pre-assigned accounts on the information system.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-06(05) [02] - The organization restricts privileged accounts on the information system to organization-defined personnel or roles.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: HUD's TRACS Security Officer assigns pre-defined roles to personnel as requested by a supervisor or administrator for pre-assigned accounts on the information system.

Actual Methods and Objects: Reviewed SSP

Control Title: AC-06(9) -Auditing Use Of Privileged Functions

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system audits the execution of privileged functions.

Implementation Statement: There are audits of privileged functions.

Assessment Objective: AC-6(9) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Access control policy
* Procedures addressing least privilege
* Information system design documentation
* Information system configuration settings and associated documentation
* List of privileged functions to be audited
* List of audited events
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for reviewing least privileges necessary to accomplish specified tasks
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test

* Automated mechanisms auditing the execution of least privilege functions

Determine If Statement: AC-06(09) - The information system audits the execution of privileged functions.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system audits the execution of privileged functions, such as catching attempted updates in production without authorization.

Actual Methods and Objects: Reviewed SSP

Control Title: AC-06(10) -Prohibit Non-Privileged Users From Executing Privileged Functions

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Implementation Statement: TRACS mainframe prevents non-privileged users from executing privileged functions such as disabling or altering security safeguards or countermeasures. Many users have no access, some have view and HUD users with update privilege use an application with edits.

Implementation Statement for **P207 - Mainframe (IBM)**

[None Entered]

Assessment Objective: AC-6(10) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Access control policy
* Procedures addressing least privilege
* Information system design documentation
* Information system configuration settings and associated documentation
* List of privileged functions and associated user account assignments
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks
* Organizational personnel with information security responsibilities
* System developers

Test

* Automated mechanisms implementing least privilege functions for non-privileged users

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-06(10) [01] - The information system prevents non-privileged users from executing privileged functions to include disabling implemented security safeguards/countermeasures.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: TRACS mainframe prevents non-privileged users from executing privileged functions such as disabling or altering security safeguards or countermeasures.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-06(10) [02] - The information system prevents non-privileged users from executing privileged functions to include circumventing security safeguards/countermeasures.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: AC-06(10) [03] - The information system prevents non-privileged users from executing privileged functions to include altering implemented security safeguards/countermeasures.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: TRACS mainframe prevents non-privileged users from executing privileged functions such as disabling or altering security safeguards or countermeasures.

Actual Methods and Objects: Reviewed SSP

Control Title: AC-07 -Unsuccessful Logon Attempts

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system:
a. Enforces a limit of [%Assignment: organization-defined number%] consecutive invalid logon attempts by a user during a [%Assignment: organization-defined time period%]; and
b. Automatically [%Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]%] when the maximum number of unsuccessful attempts is exceeded.

Implementation Statement: The information system enforces a limit of three consecutive invalid access attempts by a user during a 30 minute time period. The information system automatically locks the account until an appropriate security administrator manually intervenes to unlock accounts on moderate and high systems when the maximum number of unsuccessful attempts is exceeded.

Assessment Objective: AC-7 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Access control policy
* Procedures addressing unsuccessful logon attempts
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with information security responsibilities
* System developers
* System/network administrators

Test
* Automated mechanisms implementing access control policy for unsuccessful logon attempts

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-07 (a)[01] - The organization defines the number of consecutive invalid logon attempts allowed to the information system by a user during an organization-defined time period.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces a limit of three consecutive invalid access attempts by a user during a 30 minute time period. The information system automatically locks the account until an appropriate security administrator manually intervenes to unlocks accounts on moderate and high systems when the maximum number of unsuccessful attempts is exceeded.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-07 (a)[02] - The organization defines the time period allowed by a user of the information system for an organization-defined number of consecutive invalid logon attempts.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces a limit of three consecutive invalid access attempts by a user during a 30 minute time period. The information system automatically locks the account until an appropriate security administrator manually intervenes to unlocks accounts on moderate and high systems when the maximum number of unsuccessful attempts is exceeded.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-07 (a)[03] - The information system enforces a limit of organization-defined number of consecutive invalid logon attempts by a user during an organization-defined time period.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces a limit of three consecutive invalid access attempts by a user during a 30 minute time period. The information system automatically locks the account until an appropriate security administrator manually intervenes to unlocks accounts on moderate and high systems when the maximum number of unsuccessful attempts is exceeded.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-07 (b)[01] - The organization defines account/node lockout time period or logon delay algorithm to be automatically enforced by the information system when the maximum number of unsuccessful logon attempts is exceeded.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces a limit of three consecutive invalid access attempts by a user during a 30 minute time period. The information system automatically locks the account until an appropriate security administrator manually intervenes to unlocks accounts on moderate and high systems when the maximum number of unsuccessful attempts is exceeded.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-07 (b)[02] - The information system, when the maximum number of unsuccessful logon attempts is exceeded, automatically:
* locks the account/node for the organization-defined time period;
* locks the account/node until released by an administrator; or
* delays next logon prompt according to the organization-defined delay algorithm.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system enforces a limit of three consecutive invalid access attempts by a user during a 30 minute time period. The information system automatically locks the account until an appropriate security administrator manually intervenes to unlocks accounts on moderate and high systems when the maximum number of unsuccessful attempts is exceeded.

Actual Methods and Objects: Reviewed SSP

Control Title: AC-08 -System Use Notification

Applicability: Applicable **Result:** Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The information system:
a. Displays to users [%Assignment: organization-defined system use notification message or banner%] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
1. Users are accessing a U.S. Government information system;
2. Information system usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
4. Use of the information system indicates consent to monitoring and recording;
b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
c. For publicly accessible systems:
1. Displays system use information [%Assignment: organization-defined conditions%], before granting further access;
2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Includes a description of the authorized uses of the system.

Implementation Statement: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Assessment Objective: AC-8 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Access control policy
* Privacy and security policies, procedures addressing system use notification
* Documented approval of information system use notification messages or banners
* Information system audit records
* User acknowledgements of notification message or banner
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system use notification messages
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel with responsibility for providing legal advice
* System developers

Test
* Automated mechanisms implementing system use notification

Determine If Statement: AC-08 (a)[01] - The organization defines a system use notification message or banner to be displayed by the information system to users before granting access to the system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Actual Methods and Objects: Reviewed SSP/ROB

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-08 (a)[02](01) - The information system displays to users the organization-defined system use notification message or banner before granting access to the information system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance, and states that users are accessing a U.S. Government information system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Actual Methods and Objects: Reviewed SSP/ROB

Determine If Statement: AC-08 (a)[02](02) - The information system displays to users the organization-defined system use notification message or banner before granting access to the information system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance, and states that information system usage may be monitored, recorded, and subject to audit.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Actual Methods and Objects: Reviewed SSP/ROB

Determine If Statement: AC-08 (a)[02](03) - The information system displays to users the organization-defined system use notification message or banner before granting access to the information system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance, and states that unauthorized use of the information system is prohibited and subject to criminal and civil penalties.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Actual Methods and Objects: Reviewed SSP/ROB

Determine If Statement: AC-08 (a)[02](04) - The information system displays to users the organization-defined system use notification message or banner before granting access to the information system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance, and states that use of the information system indicates consent to monitoring and recording.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Actual Methods and Objects: Reviewed SSP/ROB

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-08 (b) - The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Actual Methods and Objects: Reviewed SSP/ROB

Determine If Statement: AC-08 (c)(01)[01] - For publicly accessible systems the organization defines conditions for system use to be displayed by the information system before granting further access.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Actual Methods and Objects: Reviewed SSP/ROB

Determine If Statement: AC-08 (c)(01)[02] - For publicly accessible systems the information system displays organization-defined conditions before granting further access.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Actual Methods and Objects: Reviewed SSP/ROB

Determine If Statement: AC-08 (c)(02) - For publicly accessible systems the information system displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Actual Methods and Objects: Reviewed SSP/ROB

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-08 (c)(03) - For publicly accessible systems the information system includes a description of the authorized uses of the system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Actual Methods and Objects: Reviewed SSP/ROB

Control Title: AC-11 -Session Lock

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system:
a. Prevents further access to the system by initiating a session lock after [%Assignment: organization-defined time period%] of inactivity or upon receiving a request from a user; and
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Implementation Statement: The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Assessment Objective: AC-11 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Access control policy
* Procedures addressing session lock
* Procedures addressing identification and authentication
* Information system design documentation
* Information system configuration settings and associated documentation
* Security plan
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developers

Test
* Automated mechanisms implementing access control policy for session lock

Determine If Statement: AC-11 (a)[01] - The organization defines the time period of user inactivity after which the information system initiates a session lock.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-11 (a)[02] - The information system prevents further access to the system by initiating a session lock after organization-defined time period of user inactivity or upon receiving a request from a user.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-11 (b) - The information system retains the session lock until the user reestablishes access using established identification and authentication procedures.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Actual Methods and Objects: Reviewed SSP

Control Title: AC-11(1) -Pattern-Hiding Displays

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Assessment Objective: AC-11(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing session lock
* Display screen with session lock activated
* Information system design documentation
* Information system configuration settings and associated documentation
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developers

Test
* Information system session lock mechanisms

Determine If Statement: AC-11(01) - The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Actual Methods and Objects: Based on experience with system timeout.

Control Title: AC-12 -Session Termination

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system automatically terminates a user session after [%Assignment: organization-defined conditions or trigger events requiring session disconnect%].

Implementation Statement: The information system automatically terminates a user session after 30 minutes of inactivity occurs.

Assessment Objective: AC-12 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:
Examine
* Access control policy
* Procedures addressing session termination
* Information system design documentation
* Information system configuration settings and associated documentation
* List of conditions or trigger events requiring session disconnect
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developers

Test
* Automated mechanisms implementing user session termination

Determine If Statement: AC-12 [01] - The organization defines conditions or trigger events requiring session disconnect.
Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system automatically terminates a user session after 30 minutes of inactivity occurs.

Actual Methods and Objects: Based on user experience

Determine If Statement: AC-12 [02] - The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect occurs.
Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The information system automatically terminates a user session after 30 minutes of inactivity occurs.

Actual Methods and Objects: Based on user experience

Control Title: AC-14 -Permitted Actions Without Identification Or Authentication
Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Identifies [%Assignment: organization-defined user actions%] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

Implementation Statement: The organization identifies specific user actions that can be performed on the information system without identification or authentication.

Assessment Objective: AC-14 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Access control policy
* Procedures addressing permitted actions without identification or authentication
* Information system configuration settings and associated documentation
* Security plan
* List of user actions that can be performed without identification or authentication
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-14 (a) - The organization
* defines user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions;
* identifies organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization identifies specific user actions that can be performed on the information system without identification or authentication.
Control Artifacts0

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-14 (b) - The organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization identifies specific user actions that can be performed on the information system without identification or authentication.
Control Artifacts0

Actual Methods and Objects: Reviewed SSP

Control Title: AC-17 -Remote Access
Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The organization:
a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorizes remote access to the information system prior to allowing such connections.

Assessment Objective: AC-17 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Access control policy
* Procedures addressing remote access implementation and usage (including restrictions)
* Configuration management plan
* Security plan
* Information system configuration settings and associated documentation
* Remote access authorizations
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for managing remote access connections
* System/network administrators
* Organizational personnel with information security responsibilities

Test
* Remote access management capability for the information system

Determine If Statement: AC-17 (a) - The organization
* identifies the types of remote access allowed to the information system;
* establishes for each type of remote access allowed usage restrictions; configuration/connection requirements; implementation guidance;
* documents for each type of remote access allowed usage restrictions; configuration/connection requirements; implementation guidance.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-17 (b) - The organization authorizes remote access to the information system prior to allowing such connections.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Control Title: AC-17(1) -Automated Monitoring / Control

Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The information system monitors and controls remote access methods.

Assessment Objective: AC-17(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing remote access to the information system
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Information system monitoring records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developers

Test
* Automated mechanisms monitoring and controlling remote access methods

Determine If Statement: AC-17(01) - The information system monitors and controls remote access methods.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Control Title: AC-17(2) -Protection Of Confidentiality / Integrity Using Encryption

Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Assessment Objective: AC-17(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing remote access to the information system
* Information system design documentation
* Information system configuration settings and associated documentation
* Cryptographic mechanisms and associated configuration documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developers

Test
* Cryptographic mechanisms protecting confidentiality and integrity of remote access sessions

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-17(02) - The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Control Title: AC-17(3) -Managed Access Control Points

Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The information system routes all remote accesses through [%Assignment: organization-defined number%] managed network access control points.

Assessment Objective: AC-17(3) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing remote access to the information system
* Information system design documentation
* List of all managed network access control points
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms routing all remote accesses through managed network access control points

Determine If Statement: AC-17(03) [01] - The organization defines the number of managed network access control points through which all remote accesses are to be routed.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Determine If Statement: AC-17(03) [02] - The information system routes all remote accesses through the organization-defined number of managed network access control points.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Control Title: AC-17(4) -Privileged Commands / Access

Applicability: Hybrid **Result:** Implemented

Control Requirement: The organization:
(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [%Assignment: organization-defined needs%]; and
(b) Documents the rationale for such access in the security plan for the information system.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Telecommunications Processing Division (TPD).

Assessment Objective: AC-17(4) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing remote access to the information system
* Information system configuration settings and associated documentation
* Security plan
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms implementing remote access management

Determine If Statement: AC-17(04) (a)[01] - The organization defines needs to authorize the execution of privileged commands and access to security-relevant information via remote access.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: This is a hybrid control, the implementation of which is also the responsibility of HUD Telecommunications Processing Division (TPD). Secure remote access is required.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-17(04) (a)[02] - The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for organization-defined needs.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Determine If Statement: AC-17(04) (b) - The organization documents the rationale for such access in the information system security plan.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Control Title: AC-18 -Wireless Access

Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The organization:
a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
b. Authorizes wireless access to the information system prior to allowing such connections.

Assessment Objective: AC-18 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing wireless access implementation and usage (including restrictions)
* Configuration management plan
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Wireless access authorizations
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for managing wireless access connections
* Organizational personnel with information security responsibilities

Test
* Wireless access management capability for the information system

Determine If Statement: AC-18 (a) - The organization establishes for wireless access:
* usage restrictions;
* configuration/connection requirement;
* implementation guidance.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Determine If Statement: AC-18 (b) - The organization authorizes wireless access to the information system prior to allowing such connections.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Control Title: AC-18(1) -Authentication And Encryption

Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The information system protects wireless access to the system using authentication of [%Selection (one or more): users; devices%] and encryption.

Assessment Objective: AC-18(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing wireless implementation and usage (including restrictions)
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developers

Test
* Automated mechanisms implementing wireless access protections to the information system

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-18(01) - The information system protects wireless access to the system using encryption and one or more of the following:
* authentication of users; and/or
* authentication of devices.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Control Title: AC-19 -Access Control For Mobile Devices

Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The organization:
a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. Authorizes the connection of mobile devices to organizational information systems.

Assessment Objective: AC-19 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Access control policy
* Procedures addressing access control for mobile device usage (including restrictions)
* Configuration management plan
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Authorizations for mobile device connections to organizational information systems
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel using mobile devices to access organizational information systems
* System/network administrators
* Organizational personnel with information security responsibilities

Test
* Access control capability authorizing mobile device connections to organizational information systems

Determine If Statement: AC-19 (a) - The organization establishes for organization-controlled mobile devices:
* usage restrictions;
* configuration/connection requirement;
* implementation guidance.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Determine If Statement: AC-19 (b) - The organization authorizes the connection of mobile devices to organizational information systems.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Control Title: AC-19(5) -Full Device / Container-Based Encryption

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization employs [%Selection: full-device encryption; container encryption%] to protect the confidentiality and integrity of information on [%Assignment: organization-defined mobile devices%].

Implementation Statement: The organization employs WinZip Encryption for sensitive email. ISSO is in the process of moving from Secure Sockets Layer Version 3.0 (SSL3.0) to the more secure Transport Layer Security Version 1.0 (TLS1.0).

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Assessment Objective: AC-19(5) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing access control for mobile devices
* Information system design documentation
* Information system configuration settings and associated documentation
* Encryption mechanism s and associated configuration documentation
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with access control responsibilities for mobile devices
* System/network administrators
* Organizational personnel with information security responsibilities

Test
* Encryption mechanisms protecting confidentiality and integrity of information on mobile devices

Determine If Statement: AC-19(05) [01] - The organization defines mobile devices for which full-device encryption or container encryption is required to protect the confidentiality and integrity of information on such devices.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization defines mobile devices for which full-device encryption or container encryption is required to protect the confidentiality and integrity of information on such devices.

Actual Methods and Objects: Agency guidelines

Determine If Statement: AC-19(05) [02] - The organization employs full-device encryption or container encryption to protect the confidentiality and integrity of information on organization-defined mobile devices.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization defines mobile devices for which full-device encryption or container encryption is required to protect the confidentiality and integrity of information on such devices.

Actual Methods and Objects: Agency guidelines

Control Title: AC-20 -Use Of External Information Systems

Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
a. Access the information system from external information systems; and
b. Process, store, or transmit organization-controlled information using external information systems.

Assessment Objective: AC-20 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Access control policy
* Procedures addressing the use of external information systems
* External information systems terms and conditions
* List of types of applications accessible from external information systems
* Maximum security categorization for information processed, stored, or transmitted on external information systems
* Information system configuration settings and associated documentation
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for defining terms and conditions for use of external information systems to access organizational systems
* System/network administrators
* Organizational personnel with information security responsibilities

Test

* Automated mechanisms implementing terms and conditions on use of external information systems

Determine If Statement: AC-20 (a) - The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Determine If Statement: AC-20 (b) - The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store, or transmit organization-controlled information using external information systems.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Control Title: AC-20(1) -Limits On Authorized Use

Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
(a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
(b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

Assessment Objective: AC-20(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Access control policy
* Procedures addressing the use of external information systems
* Security plan
* Information system connection or processing agreements
* Account management documents
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities

Test

* Automated mechanisms implementing limits on use of external information systems

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-20(01) - The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
* verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
* retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Control Title: AC-20(2) -Portable Storage Devices

Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The organization [%Selection: restricts; prohibits%] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

Assessment Objective: AC-20(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing the use of external information systems
* Security plan
* Information system configuration settings and associated documentation
* Information system connection or processing agreements
* Account management documents
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for restricting or prohibiting use of organization-controlled storage devices on external information systems
* System/network administrators
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms implementing restrictions on use of portable storage devices

Determine If Statement: AC-20(02) - The organization restricts or prohibits the use of organization-controlled portable storage devices by authorized individuals on external information systems.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Control Title: AC-21 -Information Sharing

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [%Assignment: organization-defined information sharing circumstances where user discretion is required%]; and
b. Employs [%Assignment: organization-defined automated mechanisms or manual processes%] to assist users in making information sharing/collaboration decisions.

Implementation Statement: Control-level:Not Required based on selected RTM factors.

Assessment Objective: AC-21 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Access control policy
* Procedures addressing user-based collaboration and information sharing (including restrictions)
* Information system design documentation
* Information system configuration settings and associated documentation
* List of users authorized to make information sharing/collaboration decisions
* List of information sharing circumstances requiring user discretion
* Other relevant documents or records

Interview

* Organizational personnel responsible for making information sharing/collaboration decisions
* System/network administrators
* Organizational personnel with information security responsibilities

Test

* Automated mechanisms or manual process implementing access authorizations supporting information sharing/user collaboration decisions

Determine If Statement: AC-21 (a)[01] - The organization defines information sharing circumstances where user discretion is required.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances, such as trusted business partners.

Actual Methods and Objects: Agency agreements

Determine If Statement: AC-21 (a)[02] - The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances, such as trusted business partners.

Actual Methods and Objects: Agency agreements

Determine If Statement: AC-21 (b)[01] - The organization defines automated mechanisms or manual processes to be employed to assist users in making information sharing/collaboration decisions.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances, such as trusted business partners.

Actual Methods and Objects: Agency agreements

Determine If Statement: AC-21 (b)[02] - The organization employs organization-defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances, such as trusted business partners.

Actual Methods and Objects: Agency agreements

Control Title: AC-22 -Publicly Accessible Content

Applicability: Applicable **Result:** Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Designates individuals authorized to post information onto a publicly accessible information system;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
d. Reviews the content on the publicly accessible information system for nonpublic information [%Assignment: organization-defined frequency%] and removes such information, if discovered.

Implementation Statement: This is a common control under the purview of the department web administrator as well as the program area web administrators.

Assessment Objective: AC-22 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Access control policy
* Procedures addressing publicly accessible content
* List of users authorized to post publicly accessible content on organizational information systems
* Training materials and/or records
* Records of publicly accessible information reviews
* Records of response to nonpublic information on public web sites
* System audit logs
* Security awareness training records
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for managing publicly accessible information posted on organizational information systems
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms implementing management of publicly accessible content

Determine If Statement: AC-22 (a) - The organization designates individuals authorized to post information onto a publicly accessible information system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: This is a common control under the purview of the department web administrator as well as the program area web administrators.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-22 (b) - The organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: This is a common control under the purview of the department web administrator as well as the program area web administrators.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-22 (c) - The organization reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: This is a common control under the purview of the department web administrator as well as the program area web administrators.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AC-22 (d)[01] - The organization defines the frequency to review the content on the publicly accessible information system for nonpublic information.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: This is a common control under the purview of the department web administrator as well as the program area web administrators.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-22 (d)[02] - The organization reviews the content on the publicly accessible information system for nonpublic information with the organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: This is a common control under the purview of the department web administrator as well as the program area web administrators.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AC-22 (d)[03] - The organization removes nonpublic information from the publicly accessible information system, if discovered.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: This is a common control under the purview of the department web administrator as well as the program area web administrators.

Actual Methods and Objects: Reviewed SSP

Control Title: AP-01 -Authority to Collect

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.

Implementation Statement: The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), such as social security number.

Assessment Objective: AP-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* If PII is collected, completion of Initial Privacy Assessment, and subsequent documentation (e.g. Privacy Impact Assessment, System of Record Notices, Computer Matching Agreements), if necessary.

Interview

* Organizational personnel with privacy review responsibilities. [note: interview component system owner/manager and OPCL].

Determine If Statement: AP-01 - The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), such as social security number.

Actual Methods and Objects: Reviewed SSP

Control Title: AP-02 -Purpose Specification

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

Implementation Statement: The organization describes the purpose for which personally identifiable information (PII) is collected, used, and maintained in its privacy notices.

Assessment Objective: AP-2 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:
Examine
* If PII is collected, completion of Initial Privacy Assessment, and subsequent documentation (e.g. Privacy Impact Assessment, System of Record Notices, Computer Matching Agreements, Privacy Act (e)(3) notices), if necessary.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview component system owner/manager and OPCL].

Determine If Statement: AP-02 - The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

Actual Methods and Objects: Income verification guidelines

Control Title: AR-01 -Governance and Privacy Program
Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems;
b. Monitors federal privacy laws and policy for changes that affect the privacy program;
c. Allocates [%Assignment: organization-defined allocation of budget and staffing%] sufficient resources to implement and operate the organization-wide privacy program;
d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;
e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and
f. Updates privacy plan, policies, and procedures [%Assignment: organization-defined frequency, at least biennially%].

Implementation Statement: The organization develops, disseminates, implements and updates operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII. For example, only partial 4-digit social security number is viewable to authorized users.

Assessment Objective: AR-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Federal law and Department policy.
* Budget and personnel needs and resources.
* Privacy plans and reports.
* Privacy policies and procedures.
* Privacy plan, policies and procedures.
Interview
* Organizational personnel with privacy review responsibilities. [Note: Interview OPCL].
* Organizational personnel with privacy review responsibilities. [Note: Interview component SCOPs and OPCL].
* Organizational personnel with privacy review responsibilities. [Note: Interview component SCOPs and OPCL/CPCLO].

Determine If Statement: AR-01 (a) - The organization appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization develops, disseminates, implements and updates operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII.

Actual Methods and Objects: Privacy Policy

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AR-01 (b) - The organization monitors federal privacy laws and policy for changes that affect the privacy program.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization develops, disseminates, implements and updates operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII.

Actual Methods and Objects: Privacy Policy

Determine If Statement: AR-01 (c) - The organization (1) defines the allocation of budget and staffing for implementing privacy program; (2) allocates staffing sufficient resources to implement and operate privacy program based on organization-defined allocation of budget.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization develops, disseminates, implements and updates operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII.

Actual Methods and Objects: Privacy Policy

Determine If Statement: AR-01 (d) - The organization develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization develops, disseminates, implements and updates operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII.

Actual Methods and Objects: Privacy Policy

Determine If Statement: AR-01 (e) - The organization develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization develops, disseminates, implements and updates operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII.

Actual Methods and Objects: Privacy Policy

Determine If Statement: AR-01 (f) - The organization (1) defines the frequency to update privacy plan, policies, and procedures (at least biennially); (2) Updates privacy plan, policies, and procedures with organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization develops, disseminates, implements and updates operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII.

Actual Methods and Objects: Privacy Policy

Control Title: AR-02 -Privacy Impact and Risk Assessment

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and
b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Implementation Statement: The organization conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or HUD policies and procedures.

Assessment Objective: AR-2 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:
Examine
* Privacy risk management process.
* Privacy Impact Assessment, if necessary.
Interview
* Organizational personnel with privacy review responsibilities. [Note: Interview component SCOPs and OPCL/CPCLO].
* Organizational personnel with privacy review responsibilities. [note: interview component system owner/manager and OPCL].

Determine If Statement: AR-02 (a) - The organization documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII).

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or HUD policies and procedures.

Actual Methods and Objects: Privacy policy

Determine If Statement: AR-02 (b) - The organization conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or HUD policies and procedures.

Actual Methods and Objects: Privacy policy

Control Title: AR-03 -Privacy Requirements for Contractors and Service Providers
Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and
b. Includes privacy requirements in contracts and other acquisition-related documents.

Implementation Statement: The organization establishes privacy roles, responsibilities, and access requirements for contractors and service providers, such as password encrypted email attachments containing PII.

Assessment Objective: AR-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Roles, responsibilities, and access requirements for contractors and service providers.
* Privacy requirements in contracts and other acquisition-related documents.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview component SCOP and system owner/manager].

Determine If Statement: AR-03 (a) - The organization establishes privacy roles, responsibilities, and access requirements for contractors and service providers.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization establishes privacy roles, responsibilities, and access requirements for contractors and service providers, such as password encrypted email attachments containing PII.

Actual Methods and Objects: Project practice

Determine If Statement: AR-03 (b) - The organization includes privacy requirements in contracts and other acquisition-related documents.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization establishes privacy roles, responsibilities, and access requirements for contractors and service providers, such as password encrypted email attachments containing PII.

Actual Methods and Objects: Project practice

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: AR-04 -Privacy Monitoring and Auditing
Applicability: Applicable **Result:** Implemented

Control Requirement: The organization monitors and audits privacy controls and internal privacy policy [%Assignment: organization-defined frequency%] to ensure effective implementation.

Implementation Statement: The organization (a) Defines frequency of auditing privacy controls and internal privacy policy; (b) Monitors and audits privacy controls and internal privacy policy to ensure effective implementation based on organization defined frequency.

Assessment Objective: AR-4 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Privacy controls, internal privacy policy, and federal law compliance reports.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview component SCOP and OPCL].

Determine If Statement: AR-04 - The organization (a) Defines frequency of auditing privacy controls and internal privacy policy; (b) Monitors and audits privacy controls and internal privacy policy to ensure effective implementation based on organization defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization (a) Defines frequency of auditing privacy controls and internal privacy policy; (b) Monitors and audits privacy controls and internal privacy policy to ensure effective implementation based on organization defined frequency.

Actual Methods and Objects: Privacy policy

Control Title: AR-05 -Privacy Awareness and Training
Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;
b. Administers basic privacy training [%Assignment: organization-defined frequency, at least annually (b1)%] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [%Assignment: organization-defined frequency, at least annually (b2)%]; and
c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [%Assignment: organization-defined frequency, at least annually (c)%].

Implementation Statement: The organization develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.

Assessment Objective: AR-5 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Training activities and programs.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview OPCL].
* Organizational personnel with privacy review responsibilities. [note: interview component SCOP and OPCL].
* Organizational personnel with privacy review responsibilities. [note: interview component SCOP and OCIO].

Determine If Statement: AR-05 (a) - The organization develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.

Actual Methods and Objects: Privacy policy and training

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AR-05 (b) - The organization (1) Defines frequency of administering basic and targeted role-based privacy training; (2) Administers basic and targeted, role-based privacy training with organization-defined frequency for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.

Actual Methods and Objects: Privacy policy and training

Determine If Statement: AR-05 (c) - The organization (1) Defines frequency of certifying personnel of their responsibilities for privacy requirements; (2) Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements with organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.

Actual Methods and Objects: Privacy policy and training

Control Title: AR-06 -Privacy Reporting

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Implementation Statement: The organization develops, disseminates, and updates reports to OMB, Congress, and other oversight bodies, to demonstrate accountability with specific statutory and regulatory privacy program mandates.

Assessment Objective: AR-6 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Reports.

Interview

* Organizational personnel with privacy review responsibilities. [note: interview OPCL].

Determine If Statement: AR-06 - The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization develops, disseminates, and updates reports to OMB, Congress, and other oversight bodies, to demonstrate accountability with specific statutory and regulatory privacy program mandates.

Actual Methods and Objects: Privacy program

Control Title: AR-07 -Privacy-Enhanced System Design and Development

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization designs information systems to support privacy by automating privacy controls.

Implementation Statement: The organization designs information systems to support privacy by automating privacy controls, such as partial SSN.

Assessment Objective: AR-7 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Information Systems for privacy controls.

Interview

* Organizational personnel with privacy review responsibilities. [note: interview component system owners/managers].

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AR-07 - The organization designs information systems to support privacy by automating privacy controls.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization designs information systems to support privacy by automating privacy controls, such as partial ssn.

Actual Methods and Objects: Privacy policy

Control Title: AR-08 -Accounting Of Disclosures

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:
(1) Date, nature, and purpose of each disclosure of a record; and
(2) Name and address of the person or agency to which the disclosure was made;
b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and
c. Makes the accounting of disclosures available to the person named in the record upon request.

Implementation Statement: The organization keeps an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made.

Assessment Objective: AR-8 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Disclosure accounting logs and documentation.
* Disclosure accounting logs and documentation to ensure compliance with applicable record retention schedules.
* Disclosure accounting procedures.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and record managers].

Determine If Statement: AR-08 (a) - The organization keeps an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization keeps an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made.

Actual Methods and Objects: Program office procedure

Determine If Statement: AR-08 (b) - The organization retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization keeps an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made.

Actual Methods and Objects: Program office procedure

Determine If Statement: AR-08 (c) - The organization makes the accounting of disclosures available to the person named in the record upon request.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/13/2015

Finding: The organization keeps an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made.

Actual Methods and Objects: Program office procedure

Control Title: AT-01 -Security Awareness And Training Policy And Procedures

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:
1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
b. Reviews and updates the current:
1. Security awareness and training policy [%Assignment: organization-defined frequency (b)(1)%]; and
2. Security awareness and training procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: HUD IT security policy (inclusive of security awareness and training) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Security awareness and training compliance policy is specifically addressed in Section 4.1.4 of this handbook.
Procedures to facilitate implementation of this policy are formally documented in Section 4.9 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors.
Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 contains the policy for Training and Security Awareness. Section 4.1.4. This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security. This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.

Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented security awareness and training policy within Section 4.9. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to security awareness and training.
The security awareness and training policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The security awareness and training procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training security controls are documented within the Section 4.9 of the Information Technology Security Procedures, dated November 1, 2013.
The security awareness and training procedures contained within the Information Technology Security Procedures is disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: AT-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Security awareness and training policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with security awareness and training responsibilities
* Organizational personnel with information security responsibilities

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AT-01 (a)(01)[01] - The organization develops and documents an security awareness and training policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AT-01 (a)(01)[02] - The organization defines personnel or roles to whom the security awareness and training policy are to be disseminated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The security awareness and training policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.

Actual Methods and Objects: HUD Intranet portal

Determine If Statement: AT-01 (a)(01)[03] - The organization disseminates the security awareness and training policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AT-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AT-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The security awareness and training procedures contained within the Information Technology Security Procedures is disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.

Actual Methods and Objects: HUD Intranet portal

Determine If Statement: AT-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AT-01 (b)(01)[01] - The organization defines the frequency to review and update the current security awareness and training policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AT-01 (b)(01)[02] - The organization reviews and updates the current security awareness and training policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AT-01 (b)(02)[01] - The organization defines the frequency to review and update the current security awareness and training procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AT-01 (b)(02)[02] - The organization reviews and updates the current security awareness and training procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: AT-02 -Security Awareness Training

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
a. As part of initial training for new users;
b. When required by information system changes; and
c. [%Assignment: organization-defined frequency%] thereafter.

Implementation Statement: Implementation Statement for **HUD Security Awareness and Training**

FISMA mandates that users, including contractors, receive annual awareness training. The Office ofManagement and Budget (OMB) and the Department ofHomeland Security (DHS) track the number of users who complete the annual training in annual FISMA reports.
HUD leverages the Annual Security AwarenessTraining created, maintained and provided by theDepartment of Defense's Defense Information Systems Agency (DISA): http://iase.disa.mil/eta/onlinecatalog.html#iaatraining. DISA provides a web based product that walks users through an overview of the principles of informationsystems security and critical infrastructure protection and the differences between threats and vulnerabilities.The user is also presented with the dangers contained in the constantly changing world of information technology, such as social networking sites and services, web based applications andservices, and peer-to-peer applications. The concept of malicious code, its impact, and themethods it uses to infect information systems are explored. The awareness training also covers important guidelines that define information sensitivity levels and personally identifiable information (PII), including their role as a user in protecting this information. The awareness material also explains threats associated with identity theft, social engineering, phishing, spyware, and insider threats. Finally it provides users with computer security tips and practices that may be used at work and at home.

Assessment Objective: AT-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Security awareness and training policy
* Procedures addressing security awareness training implementation
* Appropriate codes of federal regulations
* Security awareness training curriculum
* Security awareness training materials
* Security plan
* Training records
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for security awareness training
* Organizational personnel with information security responsibilities
* Organizational personnel comprising the general information system user community

Test
* Automated mechanisms managing security awareness training

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AT-02 (a) - The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users.

Inherited From: HUD Security Awareness and Training

Result: Not Assessed

Determine If Statement: AT-02 (b) - The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) when required by information system changes.

Inherited From: HUD Security Awareness and Training

Result: Not Assessed

Determine If Statement: AT-02 (c)[01] - The organization defines the frequency to provide refresher security awareness training thereafter to information system users (including managers, senior executives, and contractors).

Inherited From: HUD Security Awareness and Training

Result: Not Assessed

Determine If Statement: AT-02 (c)[02] - The organization provides refresher security awareness training to information users (including managers, senior executives, and contractors) with the organization-defined frequency.

Inherited From: HUD Security Awareness and Training

Result: Not Assessed

Control Title: AT-02(2) -Insider Threat

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Implementation Statement: The organization includes security awareness training on recognizing and reporting potential indicators of insider threat. This is part of DISA online course.

Assessment Objective: AT-2(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Security awareness and training policy
* Procedures addressing security awareness training implementation
* Security awareness training curriculum
* Security awareness training materials
* Security plan
* Other relevant documents or records

Interview

* Organizational personnel that participate in security awareness training
* Organizational personnel with responsibilities for basic security awareness training
* Organizational personnel with information security responsibilities

Determine If Statement: AT-02(02) - The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Actual Methods and Objects: Security awareness training

Control Title: AT-03 -Role-Based Security Training

Applicability: Fully Inherited **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization provides role-based security training to personnel with assigned security roles and responsibilities:
a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. [%Assignment: organization-defined frequency%] thereafter.

Implementation Statement: Implementation Statement for **HUD Security Awareness and Training**
All Federal organizations rely on a cadre of people who are assigned specific responsibilities for ensuring and maintaining the information security of information systems. It is critical for this cadre of people to maintain their expertise and information security proficiency to ensure the Department's security posture is not degraded. Specialized cyber security training is also known as role-based training or specialized cybersecurity training. This training focuses on providing the knowledge, skills, and abilities specific to an individual's role and responsibilities relative to information systems. It focuses on information security disciplines such as vulnerability management, security risk management, security system testing and evaluation, incident response, network security administration, log review, identity and access management, security regulatory compliance, security governance,etc.

Assessment Objective: AT-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Security awareness and training policy
* Procedures addressing security training implementation
* Codes of federal regulations
* Security training curriculum
* Security training materials
* Security plan
* Training records
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for role-based security training
* Organizational personnel with assigned information system security roles and responsibilities

Test
* Automated mechanisms managing role-based security training

Determine If Statement: AT-03 (a) - The organization provides role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties.

Inherited From: HUD Security Awareness and Training

Result: Not Assessed

Determine If Statement: AT-03 (b) - The organization provides role-based security training to personnel with assigned security roles and responsibilities when required by information system changes.

Inherited From: HUD Security Awareness and Training

Result: Not Assessed

Determine If Statement: AT-03 (c)[01] - The organization defines the frequency to provide refresher role-based security training thereafter to personnel with assigned security roles and responsibilities.

Inherited From: HUD Security Awareness and Training

Result: Not Assessed

Determine If Statement: AT-03 (c)[02] - The organization provides refresher role-based security training to personnel with assigned security roles and responsibilities with the organization-defined frequency.

Inherited From: HUD Security Awareness and Training

Result: Not Assessed

Control Title: AT-04 -Security Training Records
Applicability: Fully Inherited **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
b. Retains individual training records for [%Assignment: organization-defined time period%].

Implementation Statement: Implementation Statement for **HUD Security Awareness and Training**
Federal Departments are required to provide annual reports to the Department of Homeland Security on the number of federal employees identified as having significant security responsibilities and whether they have met the organization's annual training requirements. HVU will provide completion data to OITS for all HUD employees who meet their specialized cyber security training requirements through HVU. HUD employees who obtain specialized cyber security training from sources other than HVU must report that completion to OITS.
Because the contractors access the Awareness Training directly from the DISA website, there is no central tracking and reporting mechanism. OITS has established a SharePoint site to track contractor completions. [http://hudsharepoint.hud.gov/sites/ocio/CISO/default.aspx] OITS requests a report of all the "C" number accounts from CHAMPS in January. The reporting elements asked for include "C" numbers, contractor first name, and contractor last name. OITS saves this list of contractors in an excel spreadsheet to the CISO SharePoint site to the folder named: http://hudsharepoint.hud.gov/sites/ocio/CISO/default.aspx; Mandatory Contractor awareness Training folder.

Assessment Objective: AT-4 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Security awareness and training policy
* Procedures addressing security training records
* Security awareness and training records
* Security plan
* Other relevant documents or records
Interview
* Organizational personnel with security training record retention responsibilities
Test
* Automated mechanisms supporting management of security training records

Determine If Statement: AT-04 (a)[01][a] - The organization documents individual information system security training activities including basic security awareness training.
Inherited From: HUD Security Awareness and Training
Result: Not Assessed

Determine If Statement: AT-04 (a)[01][b] - The organization documents individual information system security training activities including specific role-based information system security training.
Inherited From: HUD Security Awareness and Training
Result: Not Assessed

Determine If Statement: AT-04 (a)[02][a] - The organization monitors individual information system security training activities including basic security awareness training.
Inherited From: HUD Security Awareness and Training
Result: Not Assessed

Determine If Statement: AT-04 (a)[02][b] - The organization monitors individual information system security training activities including specific role-based information system security training.
Inherited From: HUD Security Awareness and Training
Result: Not Assessed

Determine If Statement: AT-04 (b)[01] - The organization defines a time period to retain individual training records.
Inherited From: HUD Security Awareness and Training
Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AT-04 (b)[02] - The organization retains individual training records for the organization-defined time period.

Inherited From: HUD Security Awareness and Training

Result: Not Assessed

Control Title: AU-01 -Audit And Accountability Policy And Procedures

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:
1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
b. Reviews and updates the current:
1. Audit and accountability policy [%Assignment: organization-defined frequency (b)(1)%]; and
2. Audit and accountability procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: HUD IT security policy (inclusive of audit and accountability) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Audit and accountability compliance policy is specifically addressed in Section 5.3 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 5.3 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 contains the policy for Auditing and Accountability. Section 5.3A

Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented audit and accountability policy within Section 5.3. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to audit and accountability.
The audit and accountability policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The audit and accountability procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability security controls are documented within the Section 5.3 of the Information Technology Security Procedures, dated November 1, 2013.
The audit and accountability procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: AU-1 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:
Examine
* Audit and accountability policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with audit and accountability responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: AU-01 (a)(01)[01] - The organization develops and documents an audit and accountability policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AU-01 (a)(01)[02] - The organization defines personnel or roles to whom the audit and accountability policy are to be disseminated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented audit and accountability policy within Section 5.3. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to audit and accountability.
The audit and accountability policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The audit and accountability procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability security controls are documented within the Section 5.3 of the Information Technology Security Procedures, dated November 1, 2013.
The audit and accountability procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 contains the policy for Auditing and Accountability. Section 5.3A

Determine If Statement: AU-01 (a)(01)[03] - The organization disseminates the audit and accountability policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AU-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented audit and accountability policy within Section 5.3. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to audit and accountability.
The audit and accountability policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The audit and accountability procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability security controls are documented within the Section 5.3 of the Information Technology Security Procedures, dated November 1, 2013.
The audit and accountability procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 contains the policy for Auditing and Accountability. Section 5.3A

Determine If Statement: AU-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AU-01 (b)(01)[01] - The organization defines the frequency to review and update the current audit and accountability policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AU-01 (b)(01)[02] - The organization reviews and updates the current audit and accountability policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AU-01 (b)(02)[01] - The organization defines the frequency to review and update the current audit and accountability procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: AU-01 (b)(02)[02] - The organization reviews and updates the current audit and accountability procedures in accordance with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: AU-02 -Audit Events

Applicability: Applicable **Result:** Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Determines that the information system is capable of auditing the following events: [%Assignment: organization-defined auditable events%];
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d. Determines that the following events are to be audited within the information system: [%Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event%].

Implementation Statement: The information system generates audit records to support after-the-fact investigations of how, when, and why normal operations ceased. The information system generates audit records to support after-the-fact investigations of how, when, and why normal operations ceased. Based on rules, a history is recorded for tenants moving in or out or transferring; voucher status is tracked from receipt through payment; transactions are sent and confirmed. History is archived, but can be accessed if requested.
Auditable Events: The information system generates audit records for the following events:
-- System transactions
-- Subsidy paidAU-2.3: The organization periodically reviews and updates the list of organization-defined auditable events. TRACS is a legacy system from a time prior to the audit table requirement. When new applications are developed, the design incorporates tables such as audit recapture with auditable events like create and update with user id. Periodically, TRACS reviews how much history to display and how long to keep historical archives.

Assessment Objective: AU-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Audit and accountability policy
* Procedures addressing auditable events
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Information system auditable events
* Other relevant documents or records
Interview
* Organizational personnel with audit and accountability responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
Test
* Automated mechanisms implementing information system auditing

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-02 (a)[01] - The organization defines the auditable events that the information system must be capable of auditing.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system generates audit records to support after-the-fact investigations of how, when, and why normal operations ceased. The information system generates audit records to support after-the-fact investigations of how, when, and why normal operations ceased. Based on rules, a history is recorded for tenants moving in or out or transferring; voucher status is tracked from receipt through payment; transactions are sent and confirmed. History is archived, but can be accessed if requested.

Auditable Events: The information system generates audit records for the following events:
-- System transactions
-- Subsidy paid
AU-2.3: The organization periodically reviews and updates the list of organization-defined auditable events. TRACS is a legacy system from a time prior to the audit table requirement. When new applications are developed, the design incorporates tables such as audit recapture with auditable events like create and update with user id. Periodically, TRACS reviews how much history to display and how long to keep historical archives.

Actual Methods and Objects: Legacy design

Determine If Statement: AU-02 (a)[02] - The organization determines that the information system is capable of auditing organization-defined auditable events.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system generates audit records to support after-the-fact investigations of how, when, and why normal operations ceased. The information system generates audit records to support after-the-fact investigations of how, when, and why normal operations ceased. Based on rules, a history is recorded for tenants moving in or out or transferring; voucher status is tracked from receipt through payment; transactions are sent and confirmed. History is archived, but can be accessed if requested.

Auditable Events: The information system generates audit records for the following events:
-- System transactions
-- Subsidy paid
AU-2.3: The organization periodically reviews and updates the list of organization-defined auditable events. TRACS is a legacy system from a time prior to the audit table requirement. When new applications are developed, the design incorporates tables such as audit recapture with auditable events like create and update with user id. Periodically, TRACS reviews how much history to display and how long to keep historical archives.

Actual Methods and Objects: Legacy design

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-02 (b) - The organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system generates audit records to support after-the-fact investigations of how, when, and why normal operations ceased. The information system generates audit records to support after-the-fact investigations of how, when, and why normal operations ceased. Based on rules, a history is recorded for tenants moving in or out or transferring; voucher status is tracked from receipt through payment; transactions are sent and confirmed. History is archived, but can be accessed if requested.

Auditable Events: The information system generates audit records for the following events:
-- System transactions
-- Subsidy paid
AU-2.3: The organization periodically reviews and updates the list of organization-defined auditable events. TRACS is a legacy system from a time prior to the audit table requirement. When new applications are developed, the design incorporates tables such as audit recapture with auditable events like create and update with user id. Periodically, TRACS reviews how much history to display and how long to keep historical archives.

Actual Methods and Objects: Legacy design

Determine If Statement: AU-02 (c) - The organization provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system generates audit records to support after-the-fact investigations of how, when, and why normal operations ceased. The information system generates audit records to support after-the-fact investigations of how, when, and why normal operations ceased. Based on rules, a history is recorded for tenants moving in or out or transferring; voucher status is tracked from receipt through payment; transactions are sent and confirmed. History is archived, but can be accessed if requested.

Auditable Events: The information system generates audit records for the following events:
-- System transactions
-- Subsidy paid
AU-2.3: The organization periodically reviews and updates the list of organization-defined auditable events. TRACS is a legacy system from a time prior to the audit table requirement. When new applications are developed, the design incorporates tables such as audit recapture with auditable events like create and update with user id. Periodically, TRACS reviews how much history to display and how long to keep historical archives.

Actual Methods and Objects: Legacy design

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-02 (d) - The organization
* defines the subset of auditable events defined in AU-2a that are to be audited within the information system;
* determines that the subset of auditable events defined in AU-2a are to be audited within the information system; and
* determines the frequency of (or situation requiring) auditing for each identified event.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system generates audit records to support after-the-fact investigations of how, when, and why normal operations ceased. The information system generates audit records to support after-the-fact investigations of how, when, and why normal operations ceased. Based on rules, a history is recorded for tenants moving in or out or transferring; voucher status is tracked from receipt through payment; transactions are sent and confirmed. History is archived, but can be accessed if requested.

Auditable Events: The information system generates audit records for the following events:
-- System transactions
-- Subsidy paid
AU-2.3: The organization periodically reviews and updates the list of organization-defined auditable events. TRACS is a legacy system from a time prior to the audit table requirement. When new applications are developed, the design incorporates tables such as audit recapture with auditable events like create and update with user id. Periodically, TRACS reviews how much history to display and how long to keep historical archives.

Actual Methods and Objects: Legacy design

Control Title: AU-02(3) -Reviews And Updates
Applicability: Applicable **Result:** Implemented

Control Requirement: The organization reviews and updates the audited events [%Assignment: organization-defined frequency%].

Implementation Statement: The organization periodically reviews and updates the list of organization-defined auditable events.

Assessment Objective: AU-2(3) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Audit and accountability policy
* Procedures addressing auditable events
* Security plan
* List of organization-defined auditable events
* Auditable events review and update records
* Information system audit records
* Information system incident reports
* Other relevant documents or records
Interview
* Organizational personnel with audit and accountability responsibilities
* Organizational personnel with information security responsibilities
Test
* Automated mechanisms supporting review and update of auditable events

Determine If Statement: AU-02(03) [01] - The organization defines the frequency to review and update the audited events.
Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization periodically reviews and updates the list of organization-defined auditable events.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-02(03) [02] - The organization reviews and updates the auditable events with organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization periodically reviews and updates the list of organization-defined auditable events.

Actual Methods and Objects: Reviewed SSP

Control Title: AU-03 -Content Of Audit Records

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Implementation Statement: The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events. Content of Audit Records: The information system does not provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject. The system captures each transaction submitted to TRACS – including the updating user/organization.

Assessment Objective: AU-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Audit and accountability policy
* Procedures addressing content of audit records
* Information system design documentation
* Information system configuration settings and associated documentation
* List of organization-defined auditable events
* Information system audit records
* Information system incident reports
* Other relevant documents or records

Interview
* Organizational personnel with audit and accountability responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Automated mechanisms implementing information system auditing of auditable events

Determine If Statement: AU-03 - The information system generates audit records containing information that establishes:
* what type of event occurred;
* when the event occurred;
* where the event occurred;
* the source of the event;
* the outcome of the event; and
* the identity of any individuals or subjects associated with the event.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events. Content of Audit Records: The information system does not provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject. The system captures each transaction submitted to TRACS – including the updating user/organization.

Actual Methods and Objects: Reviewed SSP

Control Title: AU-03(1) -Additional Audit Information

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system generates audit records containing the following additional information: [%Assignment: organization-defined additional, more detailed information%].

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Implementation Statement: The information system does not provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
TRACS does include last updater id and date and record history and archive. There are no group account users or privileged commands. Data changes require authorization.

Assessment Objective: AU-3(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Audit and accountability policy
* Procedures addressing content of audit records
* Information system design documentation
* Information system configuration settings and associated documentation
* List of organization-defined auditable events
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with audit and accountability responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test
* Information system audit capability

Determine If Statement: AU-03(01) [01] - The organization defines additional, more detailed information to be contained in audit records that the information system generates.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system does not provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

Actual Methods and Objects: Legacy design

Determine If Statement: AU-03(01) [02] - The information system generates audit records containing the organization-defined additional, more detailed information.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system does not provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

Actual Methods and Objects: Legacy design

Control Title: AU-04 -Audit Storage Capacity

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization allocates audit record storage capacity in accordance with [%Assignment: organization-defined audit record storage requirements%].

Implementation Statement: The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded. Database size / capacity monitoring occurs. Archives are in place to remove data from the production database. Data warehouse has a view of Sybase audit tables for research.

Assessment Objective: AU-4 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Audit and accountability policy
* Procedures addressing audit storage capacity
* Information system design documentation
* Information system configuration settings and associated documentation
* Audit record storage requirements
* Audit record storage capability for information system components
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with audit and accountability responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test

* Audit record storage capacity and related configuration settings

Determine If Statement: AU-04 [01] - The organization defines audit record storage requirements.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded. Database size / capacity monitoring occurs. Archives are in place to remove data from the production database. Data warehouse has a view of Sybase audit tables for research.

Actual Methods and Objects: Data warehouse

Determine If Statement: AU-04 [02] - The organization allocates audit record storage capacity in accordance with the organization-defined audit record storage requirements.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded. Database size / capacity monitoring occurs. Archives are in place to remove data from the production database. Data warehouse has a view of Sybase audit tables for research.

Actual Methods and Objects: Data warehouse

Control Title: AU-05 -Response To Audit Processing Failures

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system:
a. Alerts [%Assignment: organization-defined personnel or roles%] in the event of an audit processing failure; and
b. Takes the following additional actions: [%Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)%].

Implementation Statement: In the event of an audit failure or audit storage capacity being reached, TRACS production control alerts appropriate organizational officials and takes additional actions. There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues, and action taken as designated by the stakeholders: Carolyn Cockrell, system owner; the MFH project manager; and the GTR.
If capacity is reached, an archive process can be created after Change Request approval by MFH. This was accomplished for arams_to_pas_data, where audit data is history. MFH monitors a daily job which failed. Data was moved from production to preserve history from 12 years. Support staff has a view of audit recapture tables that capture create, update and delete where audit is a database function.
On the mainframe, audit is history, and if a function fails, the function stops and alerts are sent with error message for research and resolution.

Assessment Objective: AU-5 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Audit and accountability policy
* Procedures addressing response to audit processing failures
* Information system design documentation
* Security plan
* Information system configuration settings and associated documentation
* List of personnel to be notified in case of an audit processing failure
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with audit and accountability responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test

* Automated mechanisms implementing information system response to audit processing failures

Determine If Statement: AU-05 (a)[01] - The organization defines the personnel or roles to be alerted in the event of an audit processing failure.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: In the event of an audit failure or audit storage capacity being reached, TRACS production control alerts appropriate organizational officials and takes additional actions. There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues, and action taken as designated by the stakeholders: Caroln Cockrell, system owner; the MFH project manager; and the GTR.
If capacity is reached, an archive process can be created after Change Request approval by MFH. This was accomplished for arams_to_pas_data, where audit data is history. MFH monitors a daily job which failed. Data was moved from production to preserve history from 12 years. Support staff has a view of audit recapture tables that capture create, update and delete where audit is a database function.
On the mainframe, audit is history, and if a function fails, the function stops and alerts are sent with error message for research and resolution.

Actual Methods and Objects: Examined SSP

Determine If Statement: AU-05 (a)[02] - The information system alerts the organization-defined personnel or roles in the event of an audit processing failure.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: In the event of an audit failure or audit storage capacity being reached, TRACS production control alerts appropriate organizational officials and takes additional actions. There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues, and action taken as designated by the stakeholders: Caroln Cockrell, system owner; the MFH project manager; and the GTR.
If capacity is reached, an archive process can be created after Change Request approval by MFH. This was accomplished for arams_to_pas_data, where audit data is history. MFH monitors a daily job which failed. Data was moved from production to preserve history from 12 years. Support staff has a view of audit recapture tables that capture create, update and delete where audit is a database function.
On the mainframe, audit is history, and if a function fails, the function stops and alerts are sent with error message for research and resolution.

Actual Methods and Objects: Examined SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-05 (b)[01] - The organization defines additional actions to be taken (e.g., shutdown information system, overwrite oldest audit records, stop generating audit records) in the event of an audit processing failure.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: In the event of an audit failure or audit storage capacity being reached, TRACS production control alerts appropriate organizational officials and takes additional actions. There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues, and action taken as designated by the stakeholders: Caroln Cockrell, system owner; the MFH project manager; and the GTR.
If capacity is reached, an archive process can be created after Change Request approval by MFH. This was accomplished for arams_to_pas_data, where audit data is history. MFH monitors a daily job which failed. Data was moved from production to preserve history from 12 years. Support staff has a view of audit recapture tables that capture create, update and delete where audit is a database function.
On the mainframe, audit is history, and if a function fails, the function stops and alerts are sent with error message for research and resolution.

Actual Methods and Objects: Examined SSP

Determine If Statement: AU-05 (b)[02] - The information system takes the additional organization-defined actions in the event of an audit processing failure.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: In the event of an audit failure or audit storage capacity being reached, TRACS production control alerts appropriate organizational officials and takes additional actions. There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues, and action taken as designated by the stakeholders: Caroln Cockrell, system owner; the MFH project manager; and the GTR.
If capacity is reached, an archive process can be created after Change Request approval by MFH. This was accomplished for arams_to_pas_data, where audit data is history. MFH monitors a daily job which failed. Data was moved from production to preserve history from 12 years. Support staff has a view of audit recapture tables that capture create, update and delete where audit is a database function.
On the mainframe, audit is history, and if a function fails, the function stops and alerts are sent with error message for research and resolution.

Actual Methods and Objects: Examined SSP

Control Title: AU-06 -Audit Review, Analysis, And Reporting

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Reviews and analyzes information system audit records [%Assignment: organization-defined frequency%] for indications of [%Assignment: organization-defined inappropriate or unusual activity%]; and
b. Reports findings to [%Assignment: organization-defined personnel or roles%].

Implementation Statement: The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues. Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Assessment Objective: AU-6 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Audit and accountability policy
* Procedures addressing audit review, analysis, and reporting
* Reports of audit findings
* Records of actions taken in response to reviews/analyses of audit records
* Other relevant documents or records

Interview

* Organizational personnel with audit review, analysis, and reporting responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: AU-06 (a)[01] - The organization defines the types of inappropriate or unusual activity to look for when information system audit records are reviewed and analyzed.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues. Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-06 (a)[02] - The organization defines the frequency to review and analyze information system audit records for indications of organization-defined inappropriate or unusual activity.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues. Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-06 (a)[03] - The organization reviews and analyzes information system audit records for indications of organization-defined inappropriate or unusual activity with the organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues. Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-06 (b)[01] - The organization defines personnel or roles to whom findings resulting from reviews and analysis of information system audit records are to be reported.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues. Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-06 (b)[02] - The organization reports findings to organization-defined personnel or roles.
Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues. Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Actual Methods and Objects: Reviewed SSP

Control Title: AU-06(1) -Process Integration
Applicability: Applicable **Result:** Implemented

Control Requirement: The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Implementation Statement: The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support investigation and response to suspicious activities. This is part of the HITS responsibility. TRACS security officer can review user roles and office access. There are periodic IG audits that may require ad hoc reports or paper trails.

Assessment Objective: AU-6(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Audit and accountability policy
* Procedures addressing audit review, analysis, and reporting
* Procedures addressing investigation and response to suspicious activities
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with audit review, analysis, and reporting responsibilities
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms integrating audit review, analysis, and reporting processes

Determine If Statement: AU-06(01) [01][a] - The organization employs automated mechanisms to integrate audit review.
Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization uses automated / integrated audit review, analysis and reporting processes to support organizational processes for investigation of suspicious activities.

Actual Methods and Objects: HUD security policy

Determine If Statement: AU-06(01) [01][b] - The organization employs automated mechanisms to integrate analysis.
Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization uses automated / integrated audit review, analysis and reporting processes to support organizational processes for investigation of suspicious activities.

Actual Methods and Objects: HUD security policy

Determine If Statement: AU-06(01) [01][c] - The organization employs automated mechanisms to integrate reporting processes.
Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization uses automated / integrated audit review, analysis and reporting processes to support organizational processes for investigation of suspicious activities.

Actual Methods and Objects: HUD security policy

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-06(01) [02][a] - The organization uses integrated audit review, analysis and reporting processes to support organizational processes for investigation of suspicious activities.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization uses automated / integrated audit review, analysis and reporting processes to support organizational processes for investigation of suspicious activities.

Actual Methods and Objects: HUD security policy

Determine If Statement: AU-06(01) [02][b] - The organization uses integrated audit review, analysis and reporting processes to support organizational processes for response to suspicious activities.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization uses automated / integrated audit review, analysis and reporting processes to support organizational processes for investigation of suspicious activities.

Actual Methods and Objects: HUD security policy

Control Title: AU-06(3) -Correlate Audit Repositories

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Implementation Statement: HUD analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. Periodically, numbers are rolled up to provide totals for Congressional requests.

Assessment Objective: AU-6(3) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Audit and accountability policy
* Procedures addressing audit review, analysis, and reporting
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records across different repositories
* Other relevant documents or records

Interview

* Organizational personnel with audit review, analysis, and reporting responsibilities
* Organizational personnel with information security responsibilities

Test

* Automated mechanisms supporting analysis and correlation of audit records

Determine If Statement: AU-06(03) - The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. The organization sends email notification of phishing attempts.

Actual Methods and Objects: Audit policy

Control Title: AU-07 -Audit Reduction And Report Generation

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system provides an audit reduction and report generation capability that:
a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
b. Does not alter the original content or time ordering of audit records.

Implementation Statement: The information system provides an audit reduction and report generation capability.
There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues. Standard and adhoc reporting is available. Data is also subjected to detailed edits and suspended for manual HUD review, as appropriate. Transaction data is available in the production and archive databases.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Assessment Objective: AU-7 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Audit and accountability policy
* Procedures addressing audit reduction and report generation
* Information system design documentation
* Information system configuration settings and associated documentation
* Audit reduction, review, analysis, and reporting tools
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with audit reduction and report generation responsibilities
* Organizational personnel with information security responsibilities

Test
* Audit reduction and report generation capability

Determine If Statement: AU-07 (a)[01] - The information system provides an audit reduction and report generation capability that supports on-demand audit review.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides an audit reduction and report generation capability.
There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues. Standard and adhoc reporting is available. Data is also subjected to detailed edits and suspended for manual HUD review, as appropriate. Transaction data is available in the production and archive databases.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-07 (a)[02] - The information system provides an audit reduction and report generation capability that supports analysis.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides an audit reduction and report generation capability.
There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues. Standard and adhoc reporting is available. Data is also subjected to detailed edits and suspended for manual HUD review, as appropriate. Transaction data is available in the production and archive databases.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-07 (a)[03] - The information system provides an audit reduction and report generation capability that supports reporting requirements.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides an audit reduction and report generation capability.
There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues. Standard and adhoc reporting is available. Data is also subjected to detailed edits and suspended for manual HUD review, as appropriate. Transaction data is available in the production and archive databases.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-07 (a)[04] - The information system provides an audit reduction and report generation capability that supports after-the-fact investigations of security incidents.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides an audit reduction and report generation capability.
There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues. Standard and adhoc reporting is available. Data is also subjected to detailed edits and suspended for manual HUD review, as appropriate. Transaction data is available in the production and archive databases.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-07 (b) - The information system provides an audit reduction and report generation capability that supports does not alter the original content or time ordering of audit records.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides an audit reduction and report generation capability.
There is production oversight that occurs on a daily basis for business days. Daily reports are sent to the OCIO and MFH stakeholders regarding system status and any issues. Standard and adhoc reporting is available. Data is also subjected to detailed edits and suspended for manual HUD review, as appropriate. Transaction data is available in the production and archive databases.

Actual Methods and Objects: Reviewed SSP

Control Title: AU-07(1) -Automatic Processing

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system provides the capability to process audit records for events of interest based on [%Assignment: organization-defined audit fields within audit records%].

Implementation Statement: The information system provides the capability to automatically process audit records for events of interest.

Assessment Objective: AU-7(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Audit and accountability policy
* Procedures addressing audit reduction and report generation
* Information system design documentation
* Information system configuration settings and associated documentation
* Audit reduction, review, analysis, and reporting tools
* Audit record criteria (fields) establishing events of interest
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with audit reduction and report generation responsibilities
* Organizational personnel with information security responsibilities
* System developers

Test
* Audit reduction and report generation capability

Determine If Statement: AU-07(01) [01] - The organization defines audit fields within audit records in order to process audit records for events of interest.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides the capability to automatically process audit records for events of interest.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-07(01) [02] - The information system provides the capability to process audit records for events of interest based on the organization-defined audit fields within audit records.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides the capability to automatically process audit records for events of interest.

Actual Methods and Objects: Reviewed SSP

Control Title: AU-08 -Time Stamps

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The information system:
a. Uses internal system clocks to generate time stamps for audit records; and
b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [%Assignment: organization-defined granularity of time measurement%].

Implementation Statement: The information system provides time stamps for use in audit record generation.

Implementation Statement for **P207 - Mainframe (IBM)**
The IBM mainframe internal system clock is used generate time stamps for audit records.

Assessment Objective: AU-8 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Audit and accountability policy
* Procedures addressing time stamp generation
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test
* Automated mechanisms implementing time stamp generation

Determine If Statement: AU-08 (a) - The information system uses internal system clocks to generate time stamps for audit records.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides time stamps for use in audit record generation.
Implementation Statement for P207 - Mainframe (IBM)
The IBM mainframe internal system clock is used generate time stamps for audit records.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-08 (b)[01] - The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: AU-08 (b)[02] - The organization defines the granularity of time measurement to be met when recording time stamps for audit records.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-08 (b)[03] - The organization records time stamps for audit records that meet the organization-defined granularity of time measurement.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: AU-08(1) -Synchronization With Authoritative Time Source

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system:
(a) Compares the internal information system clocks [%Assignment: organization-defined frequency%] with [%Assignment: organization-defined authoritative time source%]; and
(b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [%Assignment: organization-defined time period%].

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors.

Assessment Objective: AU-8(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Audit and accountability policy
* Procedures addressing time stamp generation
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test
* Automated mechanisms implementing internal information system clock synchronization

Determine If Statement: AU-08(01) (a)[01] - The organization defines the authoritative time source to which internal information system clocks are to be compared.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides time stamps for use in audit record generation.
Implementation Statement for P207 - Mainframe (IBM)
The IBM mainframe internal system clock is used generate time stamps for audit records.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-08(01) (a)[02] - The organization defines the frequency to compare the internal information system clocks with the organization-defined authoritative time source.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides time stamps for use in audit record generation.
Implementation Statement for P207 - Mainframe (IBM)
The IBM mainframe internal system clock is used generate time stamps for audit records.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-08(01) (a)[03] - The information system compares the internal information system clocks with the organization-defined authoritative time source with organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides time stamps for use in audit record generation.
Implementation Statement for P207 - Mainframe (IBM)
The IBM mainframe internal system clock is used generate time stamps for audit records.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-08(01) (b)[01] - The organization defines the time period that, if exceeded by the time difference between the internal system clocks and the authoritative time source, will result in the internal system clocks being synchronized to the authoritative time source.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides time stamps for use in audit record generation.
Implementation Statement for P207 - Mainframe (IBM)
The IBM mainframe internal system clock is used generate time stamps for audit records.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-08(01) (b)[02] - The information system synchronizes the internal information system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system provides time stamps for use in audit record generation.
Implementation Statement for P207 - Mainframe (IBM)
The IBM mainframe internal system clock is used generate time stamps for audit records.

Actual Methods and Objects: Reviewed SSP

Control Title: AU-09 -Protection Of Audit Information

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Implementation Statement: The information system protects audit information and audit tools from unauthorized access, modification, and deletion. All access to the systems and databases are restricted. Users must access via HUD security approved protocols (e.g., WASS, siteminder, ldap.) Furthermore, Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Assessment Objective: AU-9 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Audit and accountability policy
* Access control policy and procedures
* Procedures addressing protection of audit information
* Information system design documentation
* Information system configuration settings and associated documentation, information system audit records
* Audit tools
* Other relevant documents or records

Interview
* Organizational personnel with audit and accountability responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test
* Automated mechanisms implementing audit information protection

Determine If Statement: AU-09 [01][a] - The information system protects audit information from unauthorized access.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system protects audit information and audit tools from unauthorized access, modification, and deletion. All access to the systems and databases are restricted. Users must access via HUD security approved protocols (e.g., WASS, siteminder, ldap.) Furthermore, Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-09 [01][b] - The information system protects audit information from unauthorized modification.
Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system protects audit information and audit tools from unauthorized access, modification, and deletion. All access to the systems and databases are restricted. Users must access via HUD security approved protocols (e.g., WASS, siteminder, ldap.) Furthermore, Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-09 [01][c] - The information system protects audit information from unauthorized deletion.
Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system protects audit information and audit tools from unauthorized access, modification, and deletion. All access to the systems and databases are restricted. Users must access via HUD security approved protocols (e.g., WASS, siteminder, ldap.) Furthermore, Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-09 [02][a] - The information system protects audit tools from unauthorized access.
Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system protects audit information and audit tools from unauthorized access, modification, and deletion. All access to the systems and databases are restricted. Users must access via HUD security approved protocols (e.g., WASS, siteminder, ldap.) Furthermore, Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-09 [02][b] - The information system protects audit tools from unauthorized modification.
Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system protects audit information and audit tools from unauthorized access, modification, and deletion. All access to the systems and databases are restricted. Users must access via HUD security approved protocols (e.g., WASS, siteminder, ldap.) Furthermore, Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-09 [02][c] - The information system protects audit tools from unauthorized deletion.
Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system protects audit information and audit tools from unauthorized access, modification, and deletion. All access to the systems and databases are restricted. Users must access via HUD security approved protocols (e.g., WASS, siteminder, ldap.) Furthermore, Unauthorized attempted update of DB2 and other databases is controlled by database access. Reports or attempt to update DB2 inappropriately are monitored by HUD security and reported to the GTM.

Actual Methods and Objects: Reviewed SSP

Control Title: AU-09(4) -Access By Subset Of Privileged Users
Applicability: Applicable **Result:** Implemented

Control Requirement: The organization authorizes access to management of audit functionality to only [%Assignment: organization-defined subset of privileged users%].

Implementation Statement: The organization authorizes access to management of audit functionality to only project leaders for special reports or to HITS contractors with access to logs.

Assessment Objective: AU-9(4) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Audit and accountability policy
* Access control policy and procedures
* Procedures addressing protection of audit information
* Information system design documentation
* Information system configuration settings and associated documentation, system-generated list of privileged users with access to management of audit functionality
* Access authorizations
* Access control list
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with audit and accountability responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Automated mechanisms managing access to audit functionality

Determine If Statement: AU-09(04) [01] - The organization defines a subset of privileged users to be authorized access to management of audit functionality.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization defines and authorizes access to management of audit functionality only to the organization-defined subset of privileged users.

Actual Methods and Objects: HUD audit policy

Determine If Statement: AU-09(04) [02] - The organization authorizes access to management of audit functionality to only the organization-defined subset of privileged users.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization defines and authorizes access to management of audit functionality only to the organization-defined subset of privileged users.

Actual Methods and Objects: HUD audit policy

Control Title: AU-11 -Audit Record Retention

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization retains audit records for [%Assignment: organization-defined time period consistent with records retention policy%] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Implementation Statement: The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Assessment Objective: AU-11 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Audit and accountability policy
* Audit record retention policy and procedures
* Security plan
* Organization-defined retention period for audit records
* Audit record archives
* Audit logs
* Audit records
* Other relevant documents or records

Interview

* Organizational personnel with audit record retention responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Determine If Statement: AU-11 [01] - The organization defines a time period to retain audit records that is consistent with records retention policy.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-11 [02][a] - The organization retains audit records for the organization-defined time period consistent with records retention policy to provide support for after-the-fact investigations of security incidents.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-11 [02][b] - The organization retains audit records for the organization-defined time period consistent with records retention policy to meet regulatory and organizational information retention requirements.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Actual Methods and Objects: Reviewed SSP

Control Title: AU-12 -Audit Generation

Applicability: Applicable **Result:** Implemented

Control Requirement: The information system:
a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [%Assignment: organization-defined information system components%];
b. Allows [%Assignment: organization-defined personnel or roles%] to select which auditable events are to be audited by specific components of the information system; and
c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Implementation Statement: The information system does: a. Provides audit record generation capability for the list of auditable events defined in AU-2 as information system components; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.
The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Transactional data is retained in current and archive databases.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Assessment Objective: AU-12 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Audit and accountability policy
* Procedures addressing audit record generation
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* List of auditable events
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with audit record generation responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test
* Automated mechanisms implementing audit record generation capability

Determine If Statement: AU-12 (a)[01] - The organization defines the information system components which are to provide audit record generation capability for the auditable events defined in AU-2a.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system does: a. Provides audit record generation capability for the list of auditable events defined in AU-2 as information system components; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Transactional data is retained in current and archive databases.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-12 (a)[02] - The information system provides audit record generation capability, for the auditable events defined in AU-2a, at organization-defined information system components.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system does: a. Provides audit record generation capability for the list of auditable events defined in AU-2 as information system components; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Transactional data is retained in current and archive databases.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: AU-12 (b)[01] - The organization defines the personnel or roles allowed to select which auditable events are to be audited by specific components of the information system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system does: a. Provides audit record generation capability for the list of auditable events defined in AU-2 as information system components; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Transactional data is retained in current and archive databases.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-12 (b)[02] - The information system allows the organization-defined personnel or roles to select which auditable events are to be audited by specific components of the system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system does: a. Provides audit record generation capability for the list of auditable events defined in AU-2 as information system components; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Transactional data is retained in current and archive databases.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: AU-12 (c) - The information system generates audit records for the events defined in AU-2d with the content in defined in AU-3.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The information system does: a. Provides audit record generation capability for the list of auditable events defined in AU-2 as information system components; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Transactional data is retained in current and archive databases.

Actual Methods and Objects: Reviewed SSP

Control Title: CA-01 -Security Assessment And Authorization Policy And Procedures

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:
1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
b. Reviews and updates the current:
1. Security assessment and authorization policy [%Assignment: organization-defined frequency (b)(1)%]; and
2. Security assessment and authorization procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: HUD IT security policy (inclusive of security assessment, certification and accreditation) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Handbook 2400.25, Rev 2.0 April 2007. Security assessment, certification and accreditation compliance policy is specifically addressed in Section 3.10 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 3.4 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 Section 3.10 contains the policy for Certification and Accreditation. HUD Guide for Certification and Accreditation Process Guide documents procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented security assessment and authorization policy within Section 3.4. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to security assessment and authorization.
The security assessment and authorization policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The security assessment and authorization procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization security controls are documented within the Section 3.4 of the Information Technology Security Procedures, dated November 1, 2013.
The security assessment and authorization procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: CA-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Security assessment and authorization policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with security assessment and authorization responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: CA-01 (a)(01)[01] - The organization develops and documents a security assessment and authorization policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-01 (a)(01)[02] - The organization defines personnel or roles to whom the security assessment and authorization policy is to be disseminated.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CA-01 (a)(01)[03] - The organization disseminates the security assessment and authorization policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CA-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the security assessment and authorization policy and associated assessment and authorization controls.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: HUD IT security policy (inclusive of security assessment, certification and accreditation) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Security assessment, certification and accreditation compliance policy is specifically addressed in Section 3.10 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 3.4 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 Section 3.10 contains the policy for Certification and Accreditation. HUD Guide for Certification and Accreditation Process Guide documents procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.
Implementation Statement for Develop IT Security Standards and Policy
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented security assessment and authorization policy within Section 3.4. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to security assessment and authorization.
The security assessment and authorization policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The security assessment and authorization procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization security controls are documented within the Section 3.4 of the Information Technology Security Procedures, dated November 1, 2013.
The security assessment and authorization procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: HUD IT security policy (inclusive of security assessment, certification and accreditation) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Security assessment, certification and accreditation compliance policy is specifically addressed in Section 3.10 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 3.4 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 Section 3.10 contains the policy for Certification and Accreditation. HUD Guide for Certification and Accreditation Process Guide documents procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.
Implementation Statement for Develop IT Security Standards and Policy
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented security assessment and authorization policy within Section 3.4. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to security assessment and authorization.
The security assessment and authorization policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The security assessment and authorization procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization security controls are documented within the Section 3.4 of the Information Technology Security Procedures, dated November 1, 2013.
The security assessment and authorization procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: HUD IT security policy (inclusive of security assessment, certification and accreditation) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Security assessment, certification and accreditation compliance policy is specifically addressed in Section 3.10 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 3.4 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 Section 3.10 contains the policy for Certification and Accreditation. HUD Guide for Certification and Accreditation Process Guide documents procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.
Implementation Statement for Develop IT Security Standards and Policy
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented security assessment and authorization policy within Section 3.4. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to security assessment and authorization.
The security assessment and authorization policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The security assessment and authorization procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization security controls are documented within the Section 3.4 of the Information Technology Security Procedures, dated November 1, 2013.
The security assessment and authorization procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-01 (b)(01)[01] - The organization defines the frequency to review and update the current security assessment and authorization policy.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: HUD IT security policy (inclusive of security assessment, certification and accreditation) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Security assessment, certification and accreditation compliance policy is specifically addressed in Section 3.10 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 3.4 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 Section 3.10 contains the policy for Certification and Accreditation. HUD Guide for Certification and Accreditation Process Guide documents procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.
Implementation Statement for Develop IT Security Standards and Policy
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented security assessment and authorization policy within Section 3.4. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to security assessment and authorization.
The security assessment and authorization policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The security assessment and authorization procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization security controls are documented within the Section 3.4 of the Information Technology Security Procedures, dated November 1, 2013.
The security assessment and authorization procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-01 (b)(01)[02] - The organization reviews and updates the current security assessment and authorization policy with the organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: HUD IT security policy (inclusive of security assessment, certification and accreditation) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Security assessment, certification and accreditation compliance policy is specifically addressed in Section 3.10 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 3.4 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 Section 3.10 contains the policy for Certification and Accreditation. HUD Guide for Certification and Accreditation Process Guide documents procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.
Implementation Statement for Develop IT Security Standards and Policy
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented security assessment and authorization policy within Section 3.4. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to security assessment and authorization.
The security assessment and authorization policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The security assessment and authorization procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization security controls are documented within the Section 3.4 of the Information Technology Security Procedures, dated November 1, 2013.
The security assessment and authorization procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-01 (b)(02)[01] - The organization defines the frequency to review and update the current security assessment and authorization procedures.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: HUD IT security policy (inclusive of security assessment, certification and accreditation) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Security assessment, certification and accreditation compliance policy is specifically addressed in Section 3.10 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 3.4 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 Section 3.10 contains the policy for Certification and Accreditation. HUD Guide for Certification and Accreditation Process Guide documents procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.
Implementation Statement for Develop IT Security Standards and Policy
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented security assessment and authorization policy within Section 3.4. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to security assessment and authorization.
The security assessment and authorization policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The security assessment and authorization procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization security controls are documented within the Section 3.4 of the Information Technology Security Procedures, dated November 1, 2013.
The security assessment and authorization procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-01 (b)(02)[02] - The organization reviews and updates the current security assessment and authorization procedures with the organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: HUD IT security policy (inclusive of security assessment, certification and accreditation) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Security assessment, certification and accreditation compliance policy is specifically addressed in Section 3.10 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 3.4 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 Section 3.10 contains the policy for Certification and Accreditation. HUD Guide for Certification and Accreditation Process Guide documents procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.
Implementation Statement for Develop IT Security Standards and Policy
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented security assessment and authorization policy within Section 3.4. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to security assessment and authorization.
The security assessment and authorization policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The security assessment and authorization procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization security controls are documented within the Section 3.4 of the Information Technology Security Procedures, dated November 1, 2013.
The security assessment and authorization procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: Reviewed SSP

Control Title: CA-02 -Security Assessments

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Develops a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine security control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;
b. Assesses the security controls in the information system and its environment of operation [%Assignment: organization-defined frequency%] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
c. Produces a security assessment report that documents the results of the assessment; and
d. Provides the results of the security control assessment to [%Assignment: organization-defined individuals or roles%].

Implementation Statement: The organization conducts an assessment of the security controls in the information system annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Assessment Objective: CA-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Security assessment and authorization policy
* Procedures addressing security assessment planning
* Procedures addressing security assessments
* Security assessment plan
* Other relevant documents or records

Interview
* Organizational personnel with security assessment responsibilities
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms supporting security assessment, security assessment plan development, and/or security assessment reporting

Determine If Statement: CA-02 (a) - The organization develops a security assessment plan that describes the scope of the assessment including:
* security controls and control enhancements under assessment;
* assessment procedures to be used to determine security control effectiveness;
* assessment environment; assessment team; assessment roles and responsibilities.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization conducts an assessment of the security controls in the information system annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-02 (b)[01] - The organization defines the frequency to assess the security controls in the information system and its environment of operation.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization conducts an assessment of the security controls in the information system annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-02 (b)[02] - The organization assesses the security controls in the information system with the organization-defined frequency to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization conducts an assessment of the security controls in the information system annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-02 (c) - The organization produces a security assessment report that documents the results of the assessment.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization conducts an assessment of the security controls in the information system annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-02 (d)[01] - The organization defines individuals or roles to whom the results of the security control assessment are to be provided.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization conducts an assessment of the security controls in the information system annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-02 (d)[02] - The organization provides the results of the security control assessment to organization-defined individuals or roles.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization conducts an assessment of the security controls in the information system annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Actual Methods and Objects: Reviewed SSP

Control Title: CA-02(1) -Independent Assessors

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization employs assessors or assessment teams with [%Assignment: organization-defined level of independence%] to conduct security control assessments.

Implementation Statement: An independent assessment team delivers a periodic report on the system security controls.

Assessment Objective: CA-2(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Security assessment and authorization policy
* Procedures addressing security assessments
* Security authorization package (including security plan, security assessment plan, security assessment report, plan of action and milestones, authorization statement)
* Other relevant documents or records

Interview

* Organizational personnel with security assessment responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: CA-02(01) [01] - The organization defines the level of independence to be employed to conduct security control assessments.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: An independent assessment team delivers a periodic report on the system security controls.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-02(01) [02] - The organization employs assessors or assessment teams with the organization-defined level of independence to conduct security control assessments.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: An independent assessment team delivers a periodic report on the system security controls.

Actual Methods and Objects: Reviewed SSP

Control Title: CA-03 -System Interconnections

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Reviews and updates Interconnection Security Agreements [%Assignment: organization-defined frequency%].

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Implementation Statement: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.

Assessment Objective: CA-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Access control policy
* Procedures addressing information system connections
* System and communications protection policy
* Information system Interconnection Security Agreements
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Other relevant documents or records

Interview
* Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements
* Organizational personnel with information security responsibilities
* Personnel managing the system(s) to which the Interconnection Security Agreement applies

Determine If Statement: CA-03 (a) - The organization authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-03 (b) - The organization documents, for each interconnection:
* the interface characteristics;
* the security requirements;
* the nature of the information communicated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-03 (c) - The organization
* defines the frequency to review and update Interconnection Security Agreements; and
* reviews and updates Interconnection Security Agreements with the organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.

Actual Methods and Objects: Reviewed SSP

Control Title: CA-03(5) -Restrictions On External System Connections

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization employs [%Selection: allow-all, deny-by-exception; deny-all, permit-by-exception%] policy for allowing [%Assignment: organization-defined information systems%] to connect to external information systems.

Implementation Statement: The organization employs deny-all, permit-by-exception policy for allowing staff and

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

contractors to connect to external information systems.

Assessment Objective: CA-3(5) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Access control policy
* Procedures addressing information system connections
* System and communications protection policy
* Information system interconnection agreements
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Security assessment report
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with responsibility for managing connections to external information systems
* Network administrators
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms implementing restrictions on external system connections

Determine If Statement: CA-03(05) [01] - The organization defines information systems to be allowed to connect to external information systems.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization defines information systems to be allowed to connect to external information systems.

Actual Methods and Objects: HUD policy

Determine If Statement: CA-03(05) [02] - The organization employs one of the following policies for allowing organization-defined information systems to connect to external information systems:
* allow-all policy;
* deny-by-exception policy;
* deny-all policy; or
* permit-by-exception policy.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization defines information systems to be allowed to connect to external information systems.

Actual Methods and Objects: HUD policy

Control Title: CA-05 -Plan Of Action And Milestones

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and milestones [%Assignment: organization-defined frequency%] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Implementation Statement: The organization develops and updates quarterly, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Assessment Objective: CA-5 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Security assessment and authorization policy
* Procedures addressing plan of action and milestones
* Security plan
* Security assessment plan
* Security assessment report
* Security assessment evidence
* Plan of action and milestones
* Other relevant documents or records

Interview

* Organizational personnel with plan of action and milestones development and implementation responsibilities
* Organizational personnel with information security responsibilities

Test

* Automated mechanisms for developing, implementing, and maintaining plan of action and milestones

Determine If Statement: CA-05 (a) - The organization develops a plan of action and milestones for the information system to:
* document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls;
* reduce or eliminate known vulnerabilities in the system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization develops and updates quarterly, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-05 (b)[01] - The organization defines the frequency to update the existing plan of action and milestones.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization develops and updates quarterly, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-05 (b)[02][a] - The organization updates the existing plan of action and milestones with the organization-defined frequency based on the findings from security controls assessments.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization develops and updates quarterly, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-05 (b)[02][b] - The organization updates the existing plan of action and milestones with the organization-defined frequency based on the findings from security impact analyses.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization develops and updates quarterly, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-05 (b)[02][c] - The organization updates the existing plan of action and milestones with the organization-defined frequency based on the findings from continuous monitoring activities.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization develops and updates quarterly, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Actual Methods and Objects: Reviewed SSP

Control Title: CA-06 -Security Authorization

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Assigns a senior-level executive or manager as the authorizing official for the information system;
b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
c. Updates the security authorization [%Assignment: organization-defined frequency%].

Implementation Statement: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization every 3 years. A senior organizational official signs and approves the security accreditation.

Assessment Objective: CA-6 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Security assessment and authorization policy
* Procedures addressing security authorization
* Security authorization package (including security plan
* Security assessment report
* Plan of action and milestones
* Authorization statement)
* Other relevant documents or records

Interview
* Organizational personnel with security authorization responsibilities
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms that facilitate security authorizations and updates

Determine If Statement: CA-06 (a) - The organization assigns a senior-level executive or manager as the authorizing official for the information system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization every 3 years. A senior organizational official signs and approves the security accreditation.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-06 (b) - The organization ensures that the authorizing official authorizes the information system for processing before commencing operations.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization every 3 years. A senior organizational official signs and approves the security accreditation.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-06 (c)[01] - The organization defines the frequency to update the security authorization.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization every 3 years. A senior organizational official signs and approves the security accreditation.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-06 (c)[02] - The organization updates the security authorization with the organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization every 3 years. A senior organizational official signs and approves the security accreditation.

Actual Methods and Objects: Reviewed SSP

Control Title: CA-07 -Continuous Monitoring

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:
a. Establishment of [%Assignment: organization-defined metrics%] to be monitored;
b. Establishment of [%Assignment: organization-defined frequencies (b)[1]%] for monitoring and [%Assignment: organization-defined frequencies (b)[2]%] for assessments supporting such monitoring;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
e. Correlation and analysis of security-related information generated by assessments and monitoring;
f. Response actions to address results of the analysis of security-related information; and
g. Reporting the security status of organization and the information system to [%Assignment: organization-defined personnel or roles%] [%Assignment: organization-defined frequency%].

Implementation Statement: A formal, structured configuration management process ensures continuous monitoring of security controls for the TRACS System. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all TRACS security controls is also conducted.
This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Assessment Objective: CA-7 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Security assessment and authorization policy
* Procedures addressing continuous monitoring of information system security controls
* Procedures addressing configuration management
* Security plan
* Security assessment report
* Plan of action and milestones
* Information system monitoring records
* Configuration management records, security impact analyses
* Status reports
* Other relevant documents or records

Interview
* Organizational personnel with continuous monitoring responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Mechanisms implementing continuous monitoring

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-07 (a)[01] - The organization develops a continuous monitoring strategy that defines metrics to be monitored.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (a)[02] - The organization develops a continuous monitoring strategy that includes monitoring of organization-defined metrics.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (a)[03] - The organization implements a continuous monitoring program that includes monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (b)[01] - The organization develops a continuous monitoring strategy that defines frequencies for monitoring.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-07 (b)[02] - The organization defines frequencies for assessments supporting monitoring.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (b)[03] - The organization develops a continuous monitoring strategy that includes establishment of the organization-defined frequencies for monitoring and for assessments supporting monitoring.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (b)[04] - The organization implements a continuous monitoring program that includes establishment of organization-defined frequencies for monitoring and for assessments supporting such monitoring in accordance with the organizational continuous monitoring strategy.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (c)[01] - The organization develops a continuous monitoring strategy that includes ongoing security control assessments.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-07 (c)[02] - The organization implements a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (d)[01] - The organization develops a continuous monitoring strategy that includes ongoing security status monitoring of organization-defined metrics.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (d)[02] - The organization implements a continuous monitoring program that includes ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (e)[01] - The organization develops a continuous monitoring strategy that includes correlation and analysis of security-related information generated by assessments and monitoring.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-07 (e)[02] - The organization implements a continuous monitoring program that includes correlation and analysis of security-related information generated by assessments and monitoring in accordance with the organizational continuous monitoring strategy.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (f)[01] - The organization develops a continuous monitoring strategy that includes response actions to address results of the analysis of security-related information.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (f)[02] - The organization implements a continuous monitoring program that includes response actions to address results of the analysis of security-related information in accordance with the organizational continuous monitoring strategy.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (g)[01] - The organization develops a continuous monitoring strategy that defines the personnel or roles to whom the security status of the organization and information system are to be reported.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CA-07 (g)[02] - The organization develops a continuous monitoring strategy that defines the frequency to report the security status of the organization and information system to organization-defined personnel or roles.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted.
This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (g)[03] - The organization develops a continuous monitoring strategy that includes reporting the security status of the organization or information system to organizational-defined personnel or roles with the organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted.
This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07 (g)[04] - The organization implements a continuous monitoring program that includes reporting the security status of the organization and information system to organization-defined personnel or roles with the organization-defined frequency in accordance with the organizational continuous monitoring strategy.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted.
This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Control Title: CA-07(1) -Independent Assessment

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization employs assessors or assessment teams with [%Assignment: organization-defined level of independence%] to monitor the security controls in the information system on an ongoing basis.

Implementation Statement: A formal, structured configuration management process ensures continuous monitoring of security controls for the TRACS System. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all TRACS F87 security controls is also conducted.
This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Assessment Objective: CA-7(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Security assessment and authorization policy
* Procedures addressing continuous monitoring of information system security controls
* Security plan
* Security assessment report
* Plan of action and milestones
* Information system monitoring records
* Security impact analyses
* Status reports
* Other relevant documents or records

Interview

* Organizational personnel with continuous monitoring responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: CA-07(01) [01] - The organization defines a level of independence to be employed to monitor the security controls in the information system on an ongoing basis.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-07(01) [02] - The organization employs assessors or assessment teams with the organization-defined level of independence to monitor the security controls in the information system on an ongoing basis.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: A formal, structured configuration management process ensures continuous monitoring of security controls for the [System Name]. Changes to the system go through a design review that includes security impact analysis, testing which incorporates a documented test and evaluation plan inclusive of related security controls, and board review and approval of test results prior to production deployment. Annual self-assessment of all [System Name] security controls is also conducted. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Control Title: CA-09 -Internal System Connections

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization:
a. Authorizes internal connections of [%Assignment: organization-defined information system components or classes of components%] to the information system; and
b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

Implementation Statement: The organization defines information system components or classes of components to be authorized as internal connections to the information system, such as email on certain smart phones.

Assessment Objective: CA-9 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Access control policy
* Procedures addressing information system connections
* System and communications protection policy
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* List of components or classes of components authorized as internal system connections
* Security assessment report
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibility for developing, implementing, or authorizing internal system connections
* Organizational personnel with information security responsibilities

Determine If Statement: CA-09 (a)[01] - The organization defines information system components or classes of components to be authorized as internal connections to the information system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization defines information system components or classes of components to be authorized as internal connections to the information system, such as contract and funding information and PII.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-09 (a)[02] - The organization authorizes internal connections of organization-defined information system components or classes of components to the information system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization defines information system components or classes of components to be authorized as internal connections to the information system, such as contract and funding information and PII.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CA-09 (b) - The organization documents, for each internal connection:

* the interface characteristics;
* the security requirements; and
* the nature of the information communicated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: The organization defines information system components or classes of components to be authorized as internal connections to the information system, such as contract and funding information and PII.

Actual Methods and Objects: Reviewed SSP

Control Title: CM-01 -Configuration Management Policy And Procedures

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:

a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:

1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and

b. Reviews and updates the current:

1. Configuration management policy [%Assignment: organization-defined frequency (b)(1)%]; and
2. Configuration management procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: Configuration Management Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

configuration management controls.
HUD IT security policy (inclusive of configuration management) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Configuration management compliance policy is specifically addressed in Section 3.8 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 4.4 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.

Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented configuration management policy within Section 4.4. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to configuration management.
The configuration management policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The configuration management procedures to facilitate the implementation of the configuration management policy and associated configuration management security controls are documented within the Section 4.4 of the Information Technology Security Procedures, dated November 1, 2013.
The configuration management procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: CM-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Configuration management policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with configuration management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Determine If Statement: CM-01 (a)(01)[01] - The organization develops and documents a configuration management policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CM-01 (a)(01)[02] - The organization defines personnel or roles to whom the configuration management policy is to be disseminated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: Configuration Management Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
HUD IT security policy (inclusive of configuration management) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Configuration management compliance policy is specifically addressed in Section 3.8 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 4.4 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
Implementation Statement for Develop IT Security Standards and Policy
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented configuration management policy within Section 4.4. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to configuration management.
The configuration management policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The configuration management procedures to facilitate the implementation of the configuration management policy and associated configuration management security controls are documented within the Section 4.4 of the Information Technology Security Procedures, dated November 1, 2013.
The configuration management procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CM-01 (a)(01)[03] - The organization disseminates the configuration management policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CM-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CM-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: Configuration Management Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
HUD IT security policy (inclusive of configuration management) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Configuration management compliance policy is specifically addressed in Section 3.8 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 4.4 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
Implementation Statement for Develop IT Security Standards and Policy
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented configuration management policy within Section 4.4. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to configuration management.
The configuration management policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The configuration management procedures to facilitate the implementation of the configuration management policy and associated configuration management security controls are documented within the Section 4.4 of the Information Technology Security Procedures, dated November 1, 2013.
The configuration management procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CM-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CM-01 (b)(01)[01] - The organization defines the frequency to review and update the current configuration management policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CM-01 (b)(01)[02] - The organization reviews and updates the current configuration management policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CM-01 (b)(02)[01] - The organization defines the frequency to review and update the current configuration management procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CM-01 (b)(02)[02] - The organization reviews and updates the current configuration management procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: CM-02 -Baseline Configuration

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Office of IT Security & HITS Contractors.

The scope of the Information System CM Plan is to describe how the Tenant Rental Assistance Certification System (TRACS) will manage changes in the TRACS software environment in accordance with the U.S. Department of Housing and Urban Development (HUD) System Development Methodology (SDM) documentation standards. The TRACS CM plan addresses application software and documentation only.

Assessment Objective: CM-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Configuration management policy
* Procedures addressing the baseline configuration of the information system
* Configuration management plan
* Enterprise architecture documentation
* Information system design documentation
* Information system architecture and configuration documentation
* Information system configuration settings and associated documentation
* Change control records
* Other relevant documents or records

Interview
* Organizational personnel with configuration management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for managing baseline configurations
* Automated mechanisms supporting configuration control of the baseline configuration

Determine If Statement: CM-02 [01] - The organization develops and documents a current baseline configuration of the information system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: This is a common control, the implementation of which is the responsibility of HUD Office of IT Security & HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CM-02 [02] - The organization maintains, under configuration control, a current baseline configuration of the information system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: This is a common control, the implementation of which is the responsibility of HUD Office of IT Security & HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: CM-02(1) -Reviews And Updates

Applicability: Applicable **Result:** Implemented

Control Requirement: The organization reviews and updates the baseline configuration of the information system:
(a) [%Assignment: organization-defined frequency%];
(b) When required due to [%Assignment organization-defined circumstances%]; and
(c) As an integral part of information system component installations and upgrades.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Office of IT Security & HITS Contractors.
The organization reviews and updates the baseline configuration of the TRACS information system quarterly as an integral part of information system component installations and upgrades.

Assessment Objective: CM-2(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Configuration management policy
* Configuration management plan
* Procedures addressing the baseline configuration of the information system
* Procedures addressing information system component installations and upgrades
* Information system architecture and configuration documentation
* Information system configuration settings and associated documentation
* Records of information system baseline configuration reviews and updates
* Information system component installations/upgrades and associated records
* Change control records
* Other relevant documents or records

Interview
* Organizational personnel with configuration management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for managing baseline configurations
* Automated mechanisms supporting review and update of the baseline configuration

Determine If Statement: CM-02(01) (a)[01] - The organization defines the frequency to review and update the baseline configuration of the information system.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: This is a common control, the implementation of which is the responsibility of HUD Office of IT Security & HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CM-02(01) (a)[02] - The organization reviews and updates the baseline configuration of the information system with the organization-defined frequency.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: This is a common control, the implementation of which is the responsibility of HUD Office of IT Security & HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CM-02(01) (b)[01] - The organization defines circumstances that require the baseline configuration of the information system to be reviewed and updated.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: This is a common control, the implementation of which is the responsibility of HUD Office of IT Security & HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CM-02(01) (b)[02] - The organization reviews and updates the baseline configuration of the information system when required due to organization-defined circumstances.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: This is a common control, the implementation of which is the responsibility of HUD Office of IT Security & HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Determine If Statement: CM-02(01) (c) - The organization reviews and updates the baseline configuration of the information system as an integral part of information system component installations and upgrades.

Result: Satisfied **Assessed by:** jbarker **Date:** 11/16/2015

Finding: This is a common control, the implementation of which is the responsibility of HUD Office of IT Security & HITS Contractors.

Actual Methods and Objects: Reviewed SSP

Control Title: CM-02(3) -Retention Of Previous Configurations

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization retains [%Assignment: organization-defined previous versions of baseline configurations of the information system%] to support rollback.

Implementation Statement: HUD production contractor retains prior versions of the configuration to support a rollback if necessary. The system maintains version control lists of updated software files.

Assessment Objective: CM-2(3) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Configuration management policy
* Procedures addressing the baseline configuration of the information system
* Configuration management plan
* Information system architecture and configuration documentation
* Information system configuration settings and associated documentation
* Copies of previous baseline configuration versions
* Other relevant documents or records

Interview
* Organizational personnel with configuration management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for managing baseline configurations

Determine If Statement: CM-02(03) [01] - The organization defines previous versions of baseline configurations of the information system to be retained to support rollback.

Result: Not Assessed

Determine If Statement: CM-02(03) [02] - The organization retains organization-defined previous versions of baseline configurations of the information system to support rollback.

Result: Not Assessed

Control Title: CM-02(7) -Configure Systems, Components, Or Devices For High-Risk Areas

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
(a) Issues [%Assignment: organization-defined information systems, system components, or devices%] with [%Assignment: organization-defined configurations%] to individuals traveling to locations that the organization deems to be of significant risk; and
(b) Applies [%Assignment: organization-defined security safeguards%] to the devices when the individuals return.

Implementation Statement: HUD does not supply equipment or devices to off-site contractors. TRACS access is by a secure tunnel.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Assessment Objective: CM-2(7) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Configuration management policy
* Configuration management plan
* Procedures addressing the baseline configuration of the information system
* Procedures addressing information system component installations and upgrades
* Information system architecture and configuration documentation
* Information system configuration settings and associated documentation
* Records of information system baseline configuration reviews and updates
* Information system component installations/upgrades and associated records
* Change control records
* Other relevant documents or records

Interview
* Organizational personnel with configuration management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for managing baseline configurations

Determine If Statement: CM-02(07) (a)[01] - The organization defines information systems, system components, or devices to be issued to individuals traveling to locations that the organization deems to be of significant risk.

Result: Not Assessed

Determine If Statement: CM-02(07) (a)[02] - The organization defines configurations to be employed on organization-defined information systems, system components, or devices issued to individuals traveling to such locations.

Result: Not Assessed

Determine If Statement: CM-02(07) (a)[03] - The organization issues organization-defined information systems, system components, or devices with organization-defined configurations to individuals traveling to locations that the organization deems to be of significant risk.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Determine If Statement: CM-02(07) (b)[01] - The organization defines security safeguards to be applied to the devices when the individuals return.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Determine If Statement: CM-02(07) (b)[02] - The organization applies organization-defined safeguards to the devices when the individuals return.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Control Title: CM-03 -Configuration Change Control

Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Determines the types of changes to the information system that are configuration-controlled;
b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
c. Documents configuration change decisions associated with the information system;
d. Implements approved configuration-controlled changes to the information system;
e. Retains records of configuration-controlled changes to the information system for [%Assignment: organization-defined time period%];
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
g. Coordinates and provides oversight for configuration change control activities through [%Assignment: organization-defined configuration change control element (e.g., committee, board)%] that convenes [%Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]%].

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Configuration Change Management Board (CCMB) & HITS Contractors.

Assessment Objective: CM-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Configuration management policy
* Procedures addressing information system configuration change control
* Configuration management plan
* Information system architecture and configuration documentation
* Security plan
* Change control records
* Information system audit records
* Change control audit and review reports
* Agenda /minutes from configuration change control oversight meetings
* Other relevant documents or records

Interview
* Organizational personnel with configuration change control responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* Members of change control board or similar

Test
* Organizational processes for configuration change control
* Automated mechanisms that implement configuration change control

Determine If Statement: CM-03 (a) - The organization determines the type of changes to the information system that must be configuration-controlled.

Result: Not Assessed

Determine If Statement: CM-03 (b) - The organization reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses.

Result: Not Assessed

Determine If Statement: CM-03 (c) - The organization documents configuration change decisions associated with the information system.

Result: Not Assessed

Determine If Statement: CM-03 (d) - The organization implements approved configuration-controlled changes to the information system.

Result: Not Assessed

Determine If Statement: CM-03 (e)[01] - The organization defines a time period to retain records of configuration-controlled changes to the information system.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CM-03 (e)[02] - The organization retains records of configuration-controlled changes to the information system for the organization-defined time period.

Result: Not Assessed

Determine If Statement: CM-03 (f) - The organization audits and reviews activities associated with configuration-controlled changes to the information system.

Result: Not Assessed

Determine If Statement: CM-03 (g)[01] - The organization defines a configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities.

Result: Not Assessed

Determine If Statement: CM-03 (g)[02,03] - The organization
* defines the frequency with which the configuration change control element must convene; and/or
* defines configuration change conditions that prompt the configuration change control element to convene;

Result: Not Assessed

Determine If Statement: CM-03 (g)[04] - The organization coordinates and provides oversight for configuration change control activities through organization-defined configuration change control element that convenes at organization-defined frequency and/or for any organization-defined configuration change conditions.

Result: Not Assessed

Control Title: CM-03(2) -Test / Validate / Document Changes

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Implementation Statement: The organization does test, validate and document changes to the information system before any changes are implemented on the production system. Changes are approved and documented and HUD staff are part of User Acceptance Testing in integration region before changes are loaded to the production system.

Assessment Objective: CM-3(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Configuration management policy
* Configuration management plan
* Procedures addressing information system configuration change control
* Information system design documentation
* Information system architecture and configuration documentation
* Information system configuration settings and associated documentation
* Test records
* Validation records
* Change control records
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with configuration change control responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for configuration change control
* Automated mechanisms supporting and/or implementing testing, validating, and documenting information system changes

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CM-03(02) - The organization, before implementing changes on the operational system:
* tests changes to the information system;
* validates changes to the information system; and
* documents changes to the information system.

Result: Not Assessed

Control Title: CM-04 -Security Impact Analysis

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Configuration Change Management Board (CCMB) & HITS Contractors.

Assessment Objective: CM-4 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Configuration management policy
* Procedures addressing security impact analysis for changes to the information system
* Configuration management plan
* Security impact analysis documentation
* Analysis tools and associated outputs
* Change control records
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with responsibility for conducting security impact analysis
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for security impact analysis

Determine If Statement: CM-04 - The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Result: Not Assessed

Control Title: CM-05 -Access Restrictions For Change

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Configuration Change Management Board (CCMB) & HITS Contractors.

Assessment Objective: CM-5 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Configuration management policy
* Procedures addressing access restrictions for changes to the information system
* Configuration management plan
* Information system design documentation
* Information system architecture and configuration documentation
* Information system configuration settings and associated documentation
* Logical access approvals
* Physical access approvals
* Access credentials
* Change control records
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with logical access control responsibilities
* Organizational personnel with physical access control responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Organizational processes for managing access restrictions to change
* Automated mechanisms supporting/implementing/enforcing access restrictions associated with changes to the information system

Determine If Statement: CM-05 - The organization

* defines physical access restrictions associated with changes to the information system;
* documents physical access restrictions associated with changes to the information system;
* approves physical access restrictions associated with changes to the information system;
* enforces physical access restrictions associated with changes to the information system;
* defines logical access restrictions associated with changes to the information system;
* documents logical access restrictions associated with changes to the information system;
* approves logical access restrictions associated with changes to the information system; and
* enforces logical access restrictions associated with changes to the information system.

Result: Not Assessed

Control Title: CM-06 -Configuration Settings

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using [%Assignment: organization-defined security configuration checklists%] that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for [%Assignment: organization-defined information system components%] based on [%Assignment: organization-defined operational requirements%]; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Office of IT Security

Assessment Objective: CM-6 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Configuration management policy
* Procedures addressing configuration settings for the information system
* Configuration management plan
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Security configuration checklists
* Evidence supporting approved deviations from established configuration settings
* Change control records
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with security configuration management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Organizational processes for managing configuration settings
* Automated mechanisms that implement, monitor, and/or control information system configuration settings
* Automated mechanisms that identify and/or document deviations from established configuration settings

Determine If Statement: CM-06 (a) - The organization
* defines security configuration checklists to be used to establish and document configuration settings for the information technology products employed;
* ensures the defined security configuration checklists reflect the most restrictive mode consistent with operational requirements;
* establishes and documents configuration settings for information technology products employed within the information system using organization-defined security configuration checklists.

Result: Not Assessed

Determine If Statement: CM-06 (b) - The organization implements the configuration settings established/documented in CM-6(a).

Result: Not Assessed

Determine If Statement: CM-06 (c) - The organization
* defines information system components for which any deviations from established configuration settings must be identified; documented; approved;
* defines operational requirements to support the identification of any deviations from established configuration settings; the documentation of any deviations from established configuration settings; the approval of any deviations from established configuration settings;
* identifies any deviations from established configuration settings for organization-defined information system components based on organizational-defined operational requirements;
* documents any deviations from established configuration settings for organization-defined information system components based on organizational-defined operational requirements;
* approves any deviations from established configuration settings for organization-defined information system components based on organizational-defined operational requirements.

Result: Not Assessed

Determine If Statement: CM-06 (d) - The organization
* monitors changes to the configuration settings in accordance with organizational policies and procedures; and
* controls changes to the configuration settings in accordance with organizational policies and procedures.

Result: Not Assessed

Control Title: CM-07 -Least Functionality

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Configures the information system to provide only essential capabilities; and
b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [%Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services%].

Implementation Statement: This is a common hybrid control, the implementation of which is the responsibility of HITS Contractors & HUD Office of IT Security.

Assessment Objective: CM-7 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Configuration management policy
* Configuration management plan
* Procedures addressing least functionality in the information system
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Security configuration checklists
* Other relevant documents or records

Interview
* Organizational personnel with security configuration management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes prohibiting or restricting functions, ports, protocols, and/or services
* Automated mechanisms implementing restrictions or prohibition of functions, ports, protocols, and/or services

Determine If Statement: CM-07 (a) - The organization configures the information system to provide only essential capabilities.

Result: Not Assessed

Determine If Statement: CM-07 (b)[01] - The organization defines prohibited or restricted:
* functions;
* ports;
* protocols; and/or
* services.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Determine If Statement: CM-07 (b)[02] - The organization prohibits or restricts the use of organization-defined:
* functions;
* ports;
* protocols; and/or
* services.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Control Title: CM-07(1) -Periodic Review
Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
(a) Reviews the information system [%Assignment: organization-defined frequency%] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
(b) Disables [%Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure%].

Implementation Statement: This control is not applicable. CM-07 is the responsibility of the HITS contractors and IT Security.

Assessment Objective: CM-7(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Configuration management policy
* Procedures addressing least functionality in the information system
* Configuration management plan
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Security configuration checklists
* Documented reviews of functions, ports, protocols, and/or services
* Change control records
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for reviewing functions, ports, protocols, and services on the information system
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for reviewing/disabling nonsecure functions, ports, protocols, and/or services
* Automated mechanisms implementing review and disabling of nonsecure functions, ports, protocols, and/or services

Determine If Statement: CM-07(01) (a)[01] - The organization defines the frequency to review the information system to identify unnecessary and/or nonsecure:
* functions;
* ports;
* protocols; and/or
* services.

Result: Not Assessed

Determine If Statement: CM-07(01) (a)[02] - The organization reviews the information system with the organization-defined frequency to identify unnecessary and/or nonsecure:
* functions;
* ports;
* protocols; and/or
* services.

Result: Not Assessed

Determine If Statement: CM-07(01) (b)[01] - The organization defines, within the information system, unnecessary and/or nonsecure:
* functions;
* ports;
* protocols; and/or
* services.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CM-07(01) (b)[02] - The organization disables organization-defined unnecessary and/or nonsecure:
* functions;
* ports;
* protocols; and/or
* services.

Result: Not Assessed

Control Title: CM-07(2) -Prevent Program Execution

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system prevents program execution in accordance with [%Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage%].

Assessment Objective: CM-7(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Configuration management policy
* Procedures addressing least functionality in the information system
* Configuration management plan
* Security plan
* Information system design documentation
* Specifications for preventing software program execution
* Information system configuration settings and associated documentation
* Change control records
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test
* Organizational processes preventing program execution on the information system
* Organizational processes for software program usage and restrictions
* Automated mechanisms preventing program execution on the information system
* Automated mechanisms supporting and/or implementing software program usage and restrictions

Determine If Statement: CM-07(02) [01] - The organization defines policies regarding software program usage and restrictions.

Result: Not Assessed

Determine If Statement: CM-07(02) [02] - The information system prevents program execution in accordance with one or more of the following:
* organization-defined policies regarding program usage and restrictions; and/or
* rules authorizing the terms and conditions of software program usage.

Result: Not Assessed

Control Title: CM-07(4) -Unauthorized Software / Blacklisting

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
(a) Identifies [%Assignment: organization-defined software programs not authorized to execute on the information system%];
(b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and
(c) Reviews and updates the list of unauthorized software programs [%Assignment: organization-defined frequency%].

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Assessment Objective: CM-7(4) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Configuration management policy
* Procedures addressing least functionality in the information system
* Configuration management plan
* Information system design documentation
* Information system configuration settings and associated documentation
* List of software programs not authorized to execute on the information system
* Security configuration checklists
* Review and update records associated with list of unauthorized software programs
* Change control records
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for identifying software not authorized to execute on the information system
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Organizational process for identifying, reviewing, and updating programs not authorized to execute on the information system
* Organizational process for implementing blacklisting
* Automated mechanisms supporting and/or implementing blacklisting

Determine If Statement: CM-07(04) (a) - The organization identifies/defines software programs not authorized to execute on the information system.

Result: Not Assessed

Determine If Statement: CM-07(04) (b) - The organization employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.

Result: Not Assessed

Determine If Statement: CM-07(04) (c)[01] - The organization defines the frequency to review and update the list of unauthorized software programs on the information system.

Result: Not Assessed

Determine If Statement: CM-07(04) (c)[02] - The organization reviews and updates the list of unauthorized software programs with the organization-defined frequency.

Result: Not Assessed

Control Title: CM-08 -Information System Component Inventory

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:

a. Develops and documents an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Includes all components within the authorization boundary of the information system;
   3. Is at the level of granularity deemed necessary for tracking and reporting; and
   4. Includes [%Assignment: organization-defined information deemed necessary to achieve effective information system component accountability%]; and

b. Reviews and updates the information system component inventory [%Assignment: organization-defined frequency%].

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors & HUD Office of IT Security.

Assessment Objective: CM-8 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Configuration management policy
* Procedures addressing information system component inventory
* Configuration management plan
* Security plan
* Information system inventory records
* Inventory reviews and update records
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for information system component inventory
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Organizational processes for developing and documenting an inventory of information system components
* Automated mechanisms supporting and/or implementing the information system component inventory

Determine If Statement: CM-08 (a) - The organization
* develops and documents an inventory of information system components that accurately reflects the current information system;
* develops and documents an inventory of information system components that includes all components within the authorization boundary of the information system;
* develops and documents an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting;
* defines the information deemed necessary to achieve effective information system component accountability; develops and documents an inventory of information system components that includes organization-defined information deemed necessary to achieve effective information system component accountability.

Result: Not Assessed

Determine If Statement: CM-08 (b)[01] - The organization defines the frequency to review and update the information system component inventory.

Result: Not Assessed

Determine If Statement: CM-08 (b)[02] - The organization reviews and updates the information system component inventory with the organization-defined frequency.

Result: Not Assessed

Control Title: CM-08(1) -Updates During Installations / Removals

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors & HUD Office of IT Security.

Assessment Objective: CM-8(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Configuration management policy
* Procedures addressing information system component inventory
* Configuration management plan
* Security plan
* Information system inventory records
* Inventory reviews and update records
* Component installation records
* Component removal records
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for updating the information system component inventory
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Organizational processes for updating inventory of information system components
* Automated mechanisms implementing updating of the information system component inventory

Determine If Statement: CM-08(01) [01] - The organization updates the inventory of information system components as an integral part of component installations.

Result: Not Assessed

Determine If Statement: CM-08(01) [02] - The organization updates the inventory of information system components as an integral part of component removals.

Result: Not Assessed

Determine If Statement: CM-08(01) [03] - The organization updates the inventory of information system components as an integral part of information system updates.

Result: Not Assessed

Control Title: CM-08(3) -Automated Unauthorized Component Detection

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
(a) Employs automated mechanisms [%Assignment: organization-defined frequency%] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
(b) Takes the following actions when unauthorized components are detected: [%Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]%].

Assessment Objective: CM-8(3) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Configuration management policy
* Procedures addressing information system component inventory
* Configuration management plan
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system inventory records
* Alerts/notifications of unauthorized components within the information system
* Information system monitoring records
* Change control records
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for managing the automated mechanisms implementing unauthorized information system component detection
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test

* Organizational processes for detection of unauthorized information system components
* Automated mechanisms implementing the detection of unauthorized information system components

Determine If Statement: CM-08(03) (a)[01] - The organization defines the frequency to employ automated mechanisms to detect the presence of unauthorized:
* hardware components within the information system;
* software components within the information system;
* firmware components within the information system.

Result: Not Assessed

Determine If Statement: CM-08(03) (a)[02][a] - The organization employs automated mechanisms with the organization-defined frequency to detect the presence of unauthorized hardware components within the information system.

Result: Not Assessed

Determine If Statement: CM-08(03) (a)[02][b] - The organization employs automated mechanisms with the organization-defined frequency to detect the presence of unauthorized software components within the information system.

Result: Not Assessed

Determine If Statement: CM-08(03) (a)[02][c] - The organization employs automated mechanisms with the organization-defined frequency to detect the presence of unauthorized firmware components within the information system.

Result: Not Assessed

Determine If Statement: CM-08(03) (b)[01] - The organization defines personnel or roles to be notified when unauthorized components are detected.

Result: Not Assessed

Determine If Statement: CM-08(03) (b)[02] - The organization takes one or more of the following actions when unauthorized components are detected:
* disables network access by such components;
* isolates the components; and/or
* notifies organization-defined personnel or roles.

Result: Not Assessed

Control Title: CM-08(5) -No Duplicate Accounting Of Components

Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

Implementation Statement: All components of the information system are inventoried as a part of the system or recognized as a component by another system.

Assessment Objective: CM-8(5) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Configuration management policy
* Procedures addressing information system component inventory
* Configuration management plan
* Security plan
* Information system inventory records
* Other relevant documents or records

Interview
* Organizational personnel with information system inventory responsibilities
* Organizational personnel with responsibilities for defining information system components within the authorization boundary of the system
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for maintaining the inventory of information system components
* Automated mechanisms implementing the information system component inventory

Determine If Statement: CM-08(05) - The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

Result: Not Assessed

Control Title: CM-09 -Configuration Management Plan

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization develops, documents, and implements a configuration management plan for the information system that:
a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the information system and places the configuration items under configuration management; and
d. Protects the configuration management plan from unauthorized disclosure and modification.

Implementation Statement: The information system develops, documents and implements a configuration management plan that addresses roles, responsibilities, configuration management processes and procedures; defines configuration items; and establishes a means for identifying configuration items throughout the development life cycle.

Implementation Statement for **P207 - Mainframe (IBM)**
HPES developed and documented the Configuration Management Plan, dated Nov 22, 2011. The Configuration Management Plan is updated on an annual basis or as needed. Additionally, the configuration management plan addresses the roles and responsibilities pertaining to the configuration management process and procedures. Furthermore, the configuration items for the information system are defined and when in the system development life cycle the configuration items are placed under configuration management. Lastly, the configuration management plan documents a means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

Assessment Objective: CM-9 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* Configuration management policy
* Procedures addressing configuration management planning
* Configuration management plan
* Security plan
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for developing the configuration management plan
* Organizational personnel with responsibilities for implementing and managing processes defined in the configuration management plan
* Organizational personnel with responsibilities for protecting the configuration management plan
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for developing and documenting the configuration management plan
* Organizational processes for identifying and managing configuration items
* Organizational processes for protecting the configuration management plan
* Automated mechanisms implementing the configuration management plan
* Automated mechanisms for managing configuration items
* Automated mechanisms for protecting the configuration management plan

Determine If Statement: CM-09 (a) - The organization develops, documents, and implements a configuration management plan for the information system that:
* addresses roles;
* addresses responsibilities;
* addresses configuration management processes and procedures.

Result: Not Assessed

Determine If Statement: CM-09 (b)[01] - The organization develops, documents, and implements a configuration management plan for the information system that establishes a process for identifying configuration items throughout the SDLC.

Result: Not Assessed

Determine If Statement: CM-09 (b)[02] - The organization develops, documents, and implements a configuration management plan for the information system that establishes a process for managing the configuration of the configuration items.

Result: Not Assessed

Determine If Statement: CM-09 (c)[01] - The organization develops, documents, and implements a configuration management plan for the information system that defines the configuration items for the information system.

Result: Not Assessed

Determine If Statement: CM-09 (c)[02] - The organization develops, documents, and implements a configuration management plan for the information system that places the configuration items under configuration management.

Result: Not Assessed

Determine If Statement: CM-09 (d)[01] - The organization develops, documents, and implements a configuration management plan for the information system that protects the configuration management plan from unauthorized disclosure.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CM-09 (d)[02] - The organization develops, documents, and implements a configuration management plan for the information system that protects the configuration management plan from unauthorized modification.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: CM-10 -Software Usage Restrictions

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Implementation Statement: The organization:
a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution

Assessment Objective: CM-10 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Configuration management policy
* Procedures addressing software usage restrictions
* Configuration management plan
* Security plan
* Software contract agreements and copyright laws
* Site license documentation
* List of software usage restrictions
* Software license tracking reports
* Other relevant documents or records

Interview
* Organizational personnel with information security responsibilities
* System/network administrators
* Organizational personnel operating, using, and/or maintaining the information system
* Organizational personnel with software license management responsibilities

Test
* Organizational process for tracking the use of software protected by quantity licenses
* Organization process for controlling/documenting the use of peer-to-peer file sharing technology
* Automated mechanisms implementing software license tracking
* Automated mechanisms implementing and controlling the use of peer-to-peer files sharing technology

Determine If Statement: CM-10 (a) - The organization uses software and associated documentation in accordance with contract agreements and copyright laws.

Result: Not Assessed

Determine If Statement: CM-10 (b) - The organization tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution.

Result: Not Assessed

Determine If Statement: CM-10 (c) - The organization controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: CM-11 -User-Installed Software
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Establishes [%Assignment: organization-defined policies%] governing the installation of software by users;
b. Enforces software installation policies through [%Assignment: organization-defined methods%]; and
c. Monitors policy compliance at [%Assignment: organization-defined frequency%].

Implementation Statement: The organization, HUD IT and remote site:
a. Establish policies governing the installation of software by users, such a IE11 push or remote installation;
b. Enforces software installation policies, such as no software that is non-related to work.

Assessment Objective: CM-11 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Configuration management policy
* Procedures addressing user installed software
* Configuration management plan
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* List of rules governing user installed software
* Information system monitoring records
* Information system audit records
* Other relevant documents or records
* Continuous monitoring strategy

Interview
* Organizational personnel with responsibilities for governing user-installed software
* Organizational personnel operating, using, and/or maintaining the information system
* Organizational personnel monitoring compliance with user-installed software policy
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes governing user-installed software on the information system
* Automated mechanisms enforcing rules/methods for governing the installation of software by users
* Automated mechanisms monitoring policy compliance

Determine If Statement: CM-11 (a) - The organization
* defines policies to govern the installation of software by users;
* establishes organization-defined policies governing the installation of software by users.

Result: Not Assessed

Determine If Statement: CM-11 (b)[01] - The organization defines methods to enforce software installation policies.
Result: Not Assessed

Determine If Statement: CM-11 (b)[02] - The organization enforces software installation policies through organization-defined methods.
Result: Not Assessed

Determine If Statement: CM-11 (c)[01] - The organization defines frequency to monitor policy compliance.
Result: Not Assessed

Determine If Statement: CM-11 (c)[02] - The organization monitors policy compliance at organization-defined frequency.
Result: Not Assessed

Control Title: CP-01 -Contingency Planning Policy And Procedures
Applicability: Hybrid **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:
1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
b. Reviews and updates the current:
1. Contingency planning policy [%Assignment: organization-defined frequency (b)(1)%]; and
2. Contingency planning procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: HUD IT security policy (inclusive of contingency planning) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Contingency planning compliance policy is specifically addressed in Sections 3.6 and 4.7.3 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 4.3 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy, Handbook 2400.2500 Rev. 2 documents, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance. Section 3.6. This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.

Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented configuration management policy within Section 4.3. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to configuration management.
The configuration management policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The configuration management procedures to facilitate the implementation of the configuration management policy and associated configuration management security controls are documented within the Section 4.3 of the Information Technology Security Procedures, dated November 1, 2013.
The configuration management procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: CP-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with contingency planning responsibilities
* Organizational personnel with information security responsibilities

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CP-01 (a)(01)[01] - The organization develops and documents a contingency planning policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CP-01 (a)(01)[02] - The organization defines personnel or roles to whom the contingency planning policy is to be disseminated.

Result: Not Assessed

Determine If Statement: CP-01 (a)(01)[03] - The organization disseminates the contingency planning policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CP-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CP-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CP-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Result: Not Assessed

Determine If Statement: CP-01 (b)(01)[01] - The organization defines the frequency to review and update the current contingency planning policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CP-01 (b)(01)[02] - The organization reviews and updates the current contingency planning with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CP-01 (b)(02)[01] - The organization defines the frequency to review and update the current contingency planning procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: CP-01 (b)(02)[02] - The organization reviews and updates the current contingency planning procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: CP-02 -Contingency Plan
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Develops a contingency plan for the information system that:
1. Identifies essential missions and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
6. Is reviewed and approved by [%Assignment: organization-defined personnel or roles%];
b. Distributes copies of the contingency plan to [%Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements (b)%];
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for the information system [%Assignment: organization-defined frequency%];
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes to [%Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements (f)%]; and
g. Protects the contingency plan from unauthorized disclosure and modification.

Implementation Statement: The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

Assessment Objective: CP-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy
* Procedures addressing contingency operations for the information system
* Contingency plan
* Security plan
* Evidence of contingency plan reviews and updates
* Other relevant documents or records
Interview
* Organizational personnel with contingency planning and plan implementation responsibilities
* Organizational personnel with incident handling responsibilities
* Organizational personnel with information security responsibilities
Test
* Organizational processes for contingency plan development, review, update, and protection
* Automated mechanisms for developing, reviewing, updating and/or protecting the contingency plan

Determine If Statement: CP-02 (a)(01) - The organization develops and documents a contingency plan for the information system that identifies essential missions and business functions and associated contingency requirements.
Result: Not Assessed

Determine If Statement: CP-02 (a)(02) - The organization develops and documents a contingency plan for the information system that:
* provides recovery objectives;
* provides restoration priorities;
* provides metrics.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CP-02 (a)(03) - The organization develops and documents a contingency plan for the information system that:
* addresses contingency roles;
* addresses contingency responsibilities;
* addresses assigned individuals with contact information.

Result: Not Assessed

Determine If Statement: CP-02 (a)(04) - The organization develops and documents a contingency plan for the information system that addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure.

Result: Not Assessed

Determine If Statement: CP-02 (a)(05) - The organization develops and documents a contingency plan for the information system that addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.

Result: Not Assessed

Determine If Statement: CP-02 (a)(06)[01] - The organization develops and documents a contingency plan for the information system that defines personnel or roles to review and approve the contingency plan for the information system.

Result: Not Assessed

Determine If Statement: CP-02 (a)(06)[02] - The organization develops and documents a contingency plan for the information system that is reviewed and approved by organization-defined personnel or roles.

Result: Not Assessed

Determine If Statement: CP-02 (b)[01] - The organization defines key contingency personnel (identified by name and/or by role) and organizational elements to whom copies of the contingency plan are to be distributed.

Result: Not Assessed

Determine If Statement: CP-02 (b)[02] - The organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.

Result: Not Assessed

Determine If Statement: CP-02 (c) - The organization coordinates contingency planning activities with incident handling activities.

Result: Not Assessed

Determine If Statement: CP-02 (d)[01] - The organization defines a frequency to review the contingency plan for the information system.

Result: Not Assessed

Determine If Statement: CP-02 (d)[02] - The organization reviews the contingency plan with the organization-defined frequency.

Result: Not Assessed

Determine If Statement: CP-02 (e)[01] - The organization updates the contingency plan to address changes to the organization, information system, or environment of operation.

Result: Not Assessed

Determine If Statement: CP-02 (e)[02] - The organization updates the contingency plan to address problems encountered during plan implementation, execution, and testing.

Result: Not Assessed

Determine If Statement: CP-02 (f)[01] - The organization defines key contingency personnel (identified by name and/or by role) and organizational elements to whom contingency plan changes are to be communicated.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CP-02 (f)[02] - The organization communicates contingency plan changes to organization-defined key contingency personnel and organizational elements.

Result: Not Assessed

Determine If Statement: CP-02 (g) - The organization protects the contingency plan from unauthorized disclosure and modification.

Result: Not Assessed

Control Title: CP-02(1) -Coordinate With Related Plans

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization coordinates contingency plan development with organizational elements responsible for related plans.

Implementation Statement: The organization coordinates contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).

Assessment Objective: CP-2(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Contingency planning policy
* Procedures addressing contingency operations for the information system
* Contingency plan
* Business contingency plans
* Disaster recovery plans
* Continuity of operations plans
* Crisis communications plans
* Critical infrastructure plans
* Cyber incident response plan
* Insider threat implementation plans
* Occupant emergency plans
* Security plan
* Other relevant documents or records

Interview

* Organizational personnel with contingency planning and plan implementation responsibilities
* Organizational personnel with information security responsibilities
* Personnel with responsibility for related plans

Determine If Statement: CP-02(01) - The organization coordinates contingency plan development with organizational elements responsible for related plans.

Result: Not Assessed

Control Title: CP-02(3) -Resume Essential Missions / Business Functions

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization plans for the resumption of essential missions and business functions within [%Assignment: organization-defined time period%] of contingency plan activation.

Implementation Statement: TRACS has a Contingency Plan with a Contingency Log and Action Item Checklist. Disruptions can be minor and the Contingency team meets with HP to determine when service can be restored. Refer to April 2013 DR Test Results in CSAM.

Assessment Objective: CP-2(3) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy
* Procedures addressing contingency operations for the information system
* Contingency plan
* Security plan
* Business impact assessment
* Other related plans
* Other relevant documents or records

Interview
* Organizational personnel with contingency planning and plan implementation responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for resumption of missions and business functions

Determine If Statement: CP-02(03) [01] - The organization defines the time period to plan for the resumption of essential missions and business functions as a result of contingency plan activation.

Result: Not Assessed

Determine If Statement: CP-02(03) [02] - The organization plans for the resumption of essential missions and business functions within organization-defined time period of contingency plan activation.

Result: Not Assessed

Control Title: CP-02(8) -Identify Critical Assets

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization identifies critical information system assets supporting essential missions and business functions.

Implementation Statement: The organization identifies critical information system assets supporting essential missions and business functions. The TRACS system Contingency Plan has a check list for testing various components. The team also notifies users about expected timing

Assessment Objective: CP-2(8) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy
* Procedures addressing contingency operations for the information system
* Contingency plan
* Business impact assessment
* Security plan
* Other relevant documents or records

Interview
* Organizational personnel with contingency planning and plan implementation responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: CP-02(08) - The organization identifies critical information system assets supporting essential missions and business functions.

Result: Not Assessed

Control Title: CP-03 -Contingency Training

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:
a. Within [%Assignment: organization-defined time period%] of assuming a contingency role or responsibility;
b. When required by information system changes; and
c. [%Assignment: organization-defined frequency%] thereafter.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Implementation Statement: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training annually.

Assessment Objective: CP-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Contingency planning policy
* Procedures addressing contingency training
* Contingency plan
* Contingency training curriculum
* Contingency training material
* Security plan
* Contingency training records
* Other relevant documents or records

Interview
* Organizational personnel with contingency planning, plan implementation, and training responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for contingency training

Determine If Statement: CP-03 (a)[01] - The organization defines a time period within which contingency training is to be provided to information system users assuming a contingency role or responsibility.

Result: Not Assessed

Determine If Statement: CP-03 (a)[02] - The organization provides contingency training to information system users consistent with assigned roles and responsibilities within the organization-defined time period of assuming a contingency role or responsibility.

Result: Not Assessed

Determine If Statement: CP-03 (b) - The organization provides contingency training to information system users consistent with assigned roles and responsibilities when required by information system changes.

Result: Not Assessed

Determine If Statement: CP-03 (c)[01] - The organization defines the frequency for contingency training thereafter.

Result: Not Assessed

Determine If Statement: CP-03 (c)[02] - The organization provides contingency training to information system users consistent with assigned roles and responsibilities with the organization-defined frequency thereafter.

Result: Not Assessed

Control Title: CP-04 -Contingency Plan Testing

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Tests the contingency plan for the information system [%Assignment: organization-defined frequency%] using [%Assignment: organization-defined tests%] to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

Implementation Statement: The CP Plan testing is conducted annually for TRACS with the F87 Contingency Plan team and OITS Security.

Assessment Objective: CP-4 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Contingency planning policy
* Procedures addressing contingency plan testing
* Contingency plan
* Security plan
* Contingency plan test documentation
* Contingency plan test results
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for contingency plan testing, reviewing or responding to contingency plan tests
* Organizational personnel with information security responsibilities

Test

* Organizational processes for contingency plan testing
* Automated mechanisms supporting the contingency plan and/or contingency plan testing

Determine If Statement: CP-04 (a)[01] - The organization defines tests to determine the effectiveness of the contingency plan and the organizational readiness to execute the plan.

Result: Not Assessed

Determine If Statement: CP-04 (a)[02] - The organization defines a frequency to test the contingency plan for the information system.

Result: Not Assessed

Determine If Statement: CP-04 (a)[03] - The organization tests the contingency plan for the information system with the organization-defined frequency, using organization-defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan.

Result: Not Assessed

Determine If Statement: CP-04 (b) - The organization reviews the contingency plan test results.

Result: Not Assessed

Determine If Statement: CP-04 (c) - The organization initiates corrective actions, if needed.

Result: Not Assessed

Control Title: CP-04(1) -Coordinate With Related Plans

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Implementation Statement: The organization does test the contingency plan for the information system at least annually.

Assessment Objective: CP-4(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Contingency planning policy
* Incident response policy
* Procedures addressing contingency plan testing
* Contingency plan testing documentation
* Contingency plan
* Business continuity plans
* Disaster recovery plans
* Continuity of operations plans
* Crisis communications plans
* Critical infrastructure plans
* Cyber incident response plans
* Occupant emergency plans
* Security plan
* Other relevant documents or records

Interview

* Organizational personnel with contingency plan testing responsibilities
* Organizational personnel
* Personnel with responsibilities for related plans
* Organizational personnel with information security responsibilities

Determine If Statement: CP-04(01) - The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Result: Not Assessed

Control Title: CP-06 -Alternate Storage Site

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization:
a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
(a)HPES has established an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.
(b)The alternate tape storage facility (NOVA) is located in South Charleston WV and provides equivalent security safeguards.
Implementation Statement for **P210 - Intranet Server**
HPES has established an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. The alternate backup of information is located in Philadelphia, PA. Sungard facility for Production and in South Charleston Datacenter Facility in West Virginia for Development and Test.

Assessment Objective: CP-6 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Contingency planning policy
* Procedures addressing alternate storage sites
* Contingency plan
* Alternate storage site agreements
* Primary storage site agreements
* Other relevant documents or records

Interview

* Organizational personnel with contingency plan alternate storage site responsibilities
* Organizational personnel with information system recovery responsibilities
* Organizational personnel with information security responsibilities

Test

* Organizational processes for storing and retrieving information system backup information at the alternate storage site
* Automated mechanisms supporting and/or implementing storage and retrieval of information system backup information at the alternate storage site

Determine If Statement: CP-06 [01] - The organization establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-06 [01] - The organization establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-06 [02] - The organization ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-06 [02] - The organization ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: CP-06(1) -Separation From Primary Site

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**

HPES has an agreement in place with an alternate tape storage facility. HPES has established an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. The alternate tape storage facility (Iron Mountain) is located in Charleston WV, in addition to the alternate tape storage facility, critical data are replicated to the DRF.

Implementation Statement for **P210 - Intranet Server**

HPES has an agreement in place with an alternate virtual tape storage facility to house the TCP/IP replicated virtual volumes of information system backup information. The alternate facility for Production is in Philadelphia, PA. Sungard where critical data are replicated to. The alternate facility for Development and Test and configuration management release tapes is in South Charleston Datacenter Facility in West Virginia.

Assessment Objective: CP-6(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy
* Procedures addressing alternate storage sites
* Contingency plan
* Alternate storage site
* Alternate storage site agreements
* Primary storage site agreements
* Other relevant documents or records

Interview
* Organizational personnel with contingency plan alternate storage site responsibilities
* Organizational personnel with information system recovery responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: CP-06(01) - The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-06(01) - The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: CP-06(3) -Accessibility

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
HPES identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions within the HPES DRP for service continuity and availability management.
Implementation Statement for **P210 - Intranet Server**
HPES identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions within the HPES DRP for service continuity and availability management.

Assessment Objective: CP-6(3) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy
* Procedures addressing alternate storage sites
* Contingency plan
* Alternate storage site
* List of potential accessibility problems to alternate storage site
* Mitigation actions for accessibility problems to alternate storage site
* Organizational risk assessments
* Other relevant documents or records

Interview
* Organizational personnel with contingency plan alternate storage site responsibilities
* Organizational personnel with information system recovery responsibilities
* Organizational personnel with information security responsibilities

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CP-06(03) [01] - The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-06(03) [01] - The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-06(03) [02] - The organization outlines explicit mitigation actions for such potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-06(03) [02] - The organization outlines explicit mitigation actions for such potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: CP-07 -Alternate Processing Site

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [%Assignment: organization-defined information system operations%] for essential missions/business functions within [%Assignment: organization-defined time period consistent with recovery time and recovery point objectives%] when the primary processing capabilities are unavailable;
b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors.

Implementation Statement for **P207 - Mainframe (IBM)**
(a)HPES established an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the contracted time frames when the primary processing capabilities are unavailable.
(b) HPES ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the HUD defined time period for resumption which is outlined in the contingency plan.
(c)HPES ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.
Implementation Statement for **P210 - Intranet Server**
HPES established an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within contracted timeframes when the primary processing capabilities are unavailable. HPES ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the HUD defined time period for resumption which is outlined in appendix F of the contingency plan.

Assessment Objective: CP-7 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Contingency planning policy
* Procedures addressing alternate processing sites
* Contingency plan
* Alternate processing site agreements
* Primary processing site agreements
* Spare equipment and supplies inventory at alternate processing site
* Equipment and supply contracts
* Service-level agreements
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for contingency planning and/or alternate site arrangements
* Organizational personnel with information security responsibilities

Test

* Organizational processes for recovery at the alternate site
* Automated mechanisms supporting and/or implementing recovery at the alternate processing site

Determine If Statement: CP-07 (a)[01] - The organization defines information system operations requiring an alternate processing site to be established to permit the transfer and resumption of such operations.

Result: Not Assessed

Determine If Statement: CP-07 (a)[02] - The organization defines the time period consistent with recovery time objectives and recovery point objectives (as specified in the information system contingency plan) for transfer/resumption of organization-defined information system operations for essential missions/business functions.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-07 (a)[02] - The organization defines the time period consistent with recovery time objectives and recovery point objectives (as specified in the information system contingency plan) for transfer/resumption of organization-defined information system operations for essential missions/business functions.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-07 (a)[03] - The organization establishes an alternate processing site including necessary agreements to permit the transfer and resumption of organization-defined information system operations for essential missions/business functions, within the organization-defined time period, when the primary processing capabilities are unavailable.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-07 (a)[03] - The organization establishes an alternate processing site including necessary agreements to permit the transfer and resumption of organization-defined information system operations for essential missions/business functions, within the organization-defined time period, when the primary processing capabilities are unavailable.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CP-07 (b) - The organization
* ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site; or
* ensures that contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-07 (b) - The organization
* ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site; or
* ensures that contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-07 (c) - The organization ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-07 (c) - The organization ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: CP-07(1) -Separation From Primary Site

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
HPES identifies within the DRP an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards. The Disaster Recovery Facility is over 250 miles away from the HPES Data Center.
Implementation Statement for **P210 - Intranet Server**
HPES identifies within the DRP an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards. The Disaster Recovery Facility is over 250 miles away from the HPES Data Center.

Assessment Objective: CP-7(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy
* Procedures addressing alternate processing sites
* Contingency plan
* Alternate processing site
* Alternate processing site agreements
* Primary processing site agreements
* Other relevant documents or records

Interview
* Organizational personnel with contingency plan alternate processing site responsibilities
* Organizational personnel with information system recovery responsibilities
* Organizational personnel with information security responsibilities

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CP-07(01) - The organization identifies an alternate processing site that is separated from the primary storage site to reduce susceptibility to the same threats.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-07(01) - The organization identifies an alternate processing site that is separated from the primary storage site to reduce susceptibility to the same threats.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: CP-07(2) -Accessibility

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
HPES identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions within the HPES DRP for service continuity and availability management.
Implementation Statement for **P210 - Intranet Server**
HPES identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions within the HPES DRP for service continuity and availability management.

Assessment Objective: CP-7(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy
* Procedures addressing alternate processing sites
* Contingency plan
* Alternate processing site
* Alternate processing site agreements
* Primary processing site agreements
* Other relevant documents or records

Interview
* Organizational personnel with contingency plan alternate processing site responsibilities
* Organizational personnel with information system recovery responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: CP-07(02) [01] - The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-07(02) [01] - The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-07(02) [02] - The organization outlines explicit mitigation actions for such potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CP-07(02) [02] - The organization outlines explicit mitigation actions for such potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: CP-07(3) -Priority Of Service

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
The alternate processing site does not offer priority of service provisions, however mission critical application data is replicated in real time to the alternate processing site and components of critical application are mirrored and run in real-time.
Implementation Statement for **P210 - Intranet Server**
The alternate processing site does not offer priority of service provisions, however mission critical application data is replicated in real time to the alternate processing site and components of critical application are mirrored and run in real-time.

Assessment Objective: CP-7(3) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy
* Procedures addressing alternate processing sites
* Contingency plan
* Alternate processing site agreements
* Service-level agreements
* Other relevant documents or records

Interview
* Organizational personnel with contingency plan alternate processing site responsibilities
* Organizational personnel with information system recovery responsibilities
* Organizational personnel with information security responsibilities
* Organizational personnel with responsibility for acquisitions/contractual agreements

Determine If Statement: CP-07(03) - The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives as specified in the information system contingency plan).

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-07(03) - The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives as specified in the information system contingency plan).

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: CP-08 -Telecommunications Services

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [%Assignment: organization-defined information system operations%] for essential missions and business functions within [%Assignment: organization-defined time period%] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Implementation Statement for **P207 - Mainframe (IBM)**
HPES employs an alternate telecom service that is available at all times and is load-balanced with the primary telecom service to permit the resumption of information system operations for essential missions and business functions within the time periods specified in the HITS-CS contract in the event of a failure of the primary service.
Implementation Statement for **P210 - Intranet Server**
HPES employs an alternate telecom service that is available at all times and is load-balanced with the primary telecom service to permit the resumption of information system operations for essential missions and business functions within the time periods specified in the HITS SLA in the event of a failure of the primary service.

Assessment Objective: CP-8 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy
* Procedures addressing alternate telecommunications services
* Contingency plan
* Primary and alternate telecommunications service agreements
* Other relevant documents or records
Interview
* Organizational personnel with contingency plan telecommunications responsibilities
* Organizational personnel with information system recovery responsibilities
* Organizational personnel with information security responsibilities
* Organizational personnel with responsibility for acquisitions/contractual agreements
Test
* Automated mechanisms supporting telecommunications

Determine If Statement: CP-08 [01] - The organization defines information system operations requiring alternate telecommunications services to be established to permit the resumption of such operations.

Result: Not Assessed

Determine If Statement: CP-08 [02] - The organization defines the time period to permit resumption of organization-defined information system operations for essential missions and business functions.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-08 [02] - The organization defines the time period to permit resumption of organization-defined information system operations for essential missions and business functions.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-08 [03] - The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of organization-defined information system operations for essential missions and business functions, within the organization-defined time period, when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-08 [03] - The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of organization-defined information system operations for essential missions and business functions, within the organization-defined time period, when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: CP-08(1) -Priority Of Service Provisions

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization:
(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
(a) Priority-of-service provisions are developed in accordance with HUD policy.
(b) Telecommunications Service Priority is requested by HUD OCIO as needed.
Implementation Statement for **P210 - Intranet Server**
Priority-of-service provisions are developed in accordance with HUD policy. Telecommunications Service Priority is requested by HUD OCIO as needed.

Assessment Objective: CP-8(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy
* Procedures addressing primary and alternate telecommunications services
* Contingency plan
* Primary and alternate telecommunications service agreements
* Telecommunications Service Priority documentation
* Other relevant documents or records
Interview
* Organizational personnel with contingency plan telecommunications responsibilities
* Organizational personnel with information system recovery responsibilities
* Organizational personnel with information security responsibilities
* Organizational personnel with responsibility for acquisitions/contractual agreements
Test
* Automated mechanisms supporting telecommunications

Determine If Statement: CP-08(01) [01] - The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives as specified in the information system contingency plan).

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-08(01) [01] - The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives as specified in the information system contingency plan).

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-08(01) [02] - The organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-08(01) [02] - The organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: CP-08(2) -Single Points Of Failure
Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
HPES employs alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.
Implementation Statement for **P210 - Intranet Server**
HPES employs an alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

Assessment Objective: CP-8(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy
* Procedures addressing primary and alternate telecommunications services
* Contingency plan
* Primary and alternate telecommunications service agreements
* Other relevant documents or records
Interview
* Organizational personnel with contingency plan telecommunications responsibilities
* Organizational personnel with information system recovery responsibilities
* Primary and alternate telecommunications service providers
* Organizational personnel with information security responsibilities

Determine If Statement: CP-08(02) - The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed

Determine If Statement: CP-08(02) - The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.
Inherited From: P210 - Intranet Server
Result: Not Assessed

Control Title: CP-09 -Information System Backup
Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Conducts backups of user-level information contained in the information system [%Assignment: organization-defined frequency consistent with recovery time and recovery point objectives (a)%];
b. Conducts backups of system-level information contained in the information system [%Assignment: organization-defined frequency consistent with recovery time and recovery point objectives (b)%];
c. Conducts backups of information system documentation including security-related documentation [%Assignment: organization-defined frequency consistent with recovery time and recovery point objectives (c)%]; and
d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors and System Owners of Major Applications.

Implementation Statement for **P207 - Mainframe (IBM)**
(a/b/c)HPES conducts daily backup of all data stored within HPES. This backup includes SAN storage, backup tapes, and real time vaulting and load balancing to SunGard for clustered Web-enabled applications and all operationally required documentation including security. (d) HPES ensures the confidentiality, integrity and availability of backup information at the storage location are protected.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Implementation Statement for **P210 - Intranet Server**

HPES conducts daily backup of all data stored within HPES. This backup includes SAN storage, backup tapes, and real time vaulting and load balancing to SunGard for clustered Web-enabled applications. HPES ensures the confidentiality and integrity of backup information at the storage location are protected.

Assessment Objective: CP-9 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Contingency planning policy
* Procedures addressing information system backup
* Contingency plan
* Backup storage location(s)
* Information system backup logs or records
* Other relevant documents or records

Interview
* Organizational personnel with information system backup responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for conducting information system backups
* Automated mechanisms supporting and/or implementing information system backups

Determine If Statement: CP-09 (a)[01] - The organization defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of user-level information contained in the information system.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-09 (a)[01] - The organization defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of user-level information contained in the information system.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-09 (a)[02] - The organization conducts backups of user-level information contained in the information system with the organization-defined frequency.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-09 (a)[02] - The organization conducts backups of user-level information contained in the information system with the organization-defined frequency.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-09 (b)[01] - The organization defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of system-level information contained in the information system.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-09 (b)[01] - The organization defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of system-level information contained in the information system.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CP-09 (b)[02] - The organization conducts backups of system-level information contained in the information system with the organization-defined frequency.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-09 (b)[02] - The organization conducts backups of system-level information contained in the information system with the organization-defined frequency.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-09 (c)[01] - The organization defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of information system documentation including security-related documentation.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-09 (c)[01] - The organization defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of information system documentation including security-related documentation.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-09 (c)[02] - The organization conducts backups of information system documentation, including security-related documentation, with the organization-defined frequency.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-09 (c)[02] - The organization conducts backups of information system documentation, including security-related documentation, with the organization-defined frequency.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-09 (d) - The organization protects the confidentiality, integrity, and availability of backup information at storage locations.

Result: Not Assessed

Control Title: CP-09(1) -Testing For Reliability / Integrity

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization tests backup information [%Assignment: organization-defined frequency%] to verify media reliability and information integrity.

Implementation Statement: Implementation Statement for **P210 - Intranet Server**

Monthly volume of actual successful restores from backup media functions as verification of media reliability and integrity. SAN and vaulting are available in real time.

Assessment Objective: CP-9(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Contingency planning policy
* Procedures addressing information system backup
* Contingency plan
* Information system backup test results
* Contingency plan test documentation
* Contingency plan test results
* Other relevant documents or records

Interview

* Organizational personnel with information system backup responsibilities
* Organizational personnel with information security responsibilities

Test

* Organizational processes for conducting information system backups
* Automated mechanisms supporting and/or implementing information system backups

Determine If Statement: CP-09(01) [01] - The organization defines the frequency to test backup information to verify media reliability and information integrity.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-09(01) [02] - The organization tests backup information with the organization-defined frequency to verify media reliability and information integrity.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: CP-10 -Information System Recovery And Reconstitution

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**

HPES Data Center relies on data backups (in all forms) to allow reconstitution of the information system to a known state after a disruption, compromise, or failure. The DRP would be deployed should equipment be affected.

Implementation Statement for **P210 - Intranet Server**

HPES Data Center relies on data backups (in all forms) to allow reconstitution of the information system to a known state after a disruption, compromise, or failure. The DRP would be deployed should equipment be affected.

Assessment Objective: CP-10 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Contingency planning policy
* Procedures addressing information system backup
* Contingency plan
* Information system backup test results
* Contingency plan test results
* Contingency plan test documentation
* Redundant secondary system for information system backups
* Location(s) of redundant secondary backup system(s)
* Other relevant documents or records

Interview

* Organizational personnel with contingency planning, recovery, and/or reconstitution responsibilities
* Organizational personnel with information security responsibilities

Test

* Organizational processes implementing information system recovery and reconstitution operations
* Automated mechanisms supporting and/or implementing information system recovery and reconstitution operations

Determine If Statement: CP-10 [01][a] - The organization provides for the recovery of the information system to a known state after a disruption.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-10 [01][a] - The organization provides for the recovery of the information system to a known state after a disruption.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-10 [01][b] - The organization provides for the recovery of the information system to a known state after a compromise.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-10 [01][b] - The organization provides for the recovery of the information system to a known state after a compromise.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-10 [01][c] - The organization provides for the recovery of the information system to a known state after a failure.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-10 [01][c] - The organization provides for the recovery of the information system to a known state after a failure.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-10 [02][a] - The organization provides for the reconstitution of the information system to a known state after a disruption.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CP-10 [02][a] - The organization provides for the reconstitution of the information system to a known state after a disruption.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-10 [02][b] - The organization provides for the reconstitution of the information system to a known state after a compromise.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-10 [02][b] - The organization provides for the reconstitution of the information system to a known state after a compromise.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: CP-10 [02][c] - The organization provides for the reconstitution of the information system to a known state after a failure.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: CP-10 [02][c] - The organization provides for the reconstitution of the information system to a known state after a failure.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: CP-10(2) -Transaction Recovery

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The information system implements transaction recovery for systems that are transaction-based.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
The IBM mainframe utilizes CICS (Customer Information Control System), a family of application servers and connectors that provides industrial-strength, online transaction management and connectivity.

Assessment Objective: CP-10(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Contingency planning policy
* Procedures addressing information system recovery and reconstitution
* Contingency plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Contingency plan test documentation
* Contingency plan test results
* Information system transaction recovery records
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with responsibility for transaction recovery
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms supporting and/or implementing transaction recovery capability

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: CP-10(02) - The information system implements transaction recovery for systems that are transaction-based.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: DI-01 -Data Quality

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;
b. Collects PII directly from the individual to the greatest extent practicable;
c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [%Assignment: organization-defined frequency%]; and
d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Implementation Statement: The organization:
a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information, using TRACS system edit checks;
b. Collects PII directly from the business partner or individual to the greatest extent practicable;
c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems such as tenant move outs or transfers and annual re-certifications; and
d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of data, such as income and SSN verification.

Assessment Objective: DI-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Information systems to ensure PII that is collected is accurate, relevant, timely, and complete to the greatest extent practicable.
* Information systems to ensure PII that is collected is collected directly from the individual to the greatest extent practicable.
* Programs and information systems to correct as necessary any PII that is inaccurate or outdated.
* Guidelines that ensure and maximize the quality, utility, objectivity, and integrity of disseminated information
Interview
* Organizational personnel with privacy review responsibilities. [note: interview component system owners/managers].
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and OPCL].

Determine If Statement: DI-01 (a) - The organization confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information.

Result: Not Assessed

Determine If Statement: DI-01 (b) - The organization collects PII directly from the individual to the greatest extent practicable.

Result: Not Assessed

Determine If Statement: DI-01 (c) - The organization (1) Defines frequency for checking accuracy of PII; (2) Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems with organization-defined frequency.

Result: Not Assessed

Determine If Statement: DI-01 (d) - The organization issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Result: Not Assessed

Control Title: DI-02 -Data Integrity And Data Integrity Board

Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and
b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

Implementation Statement: HUD documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and oversees organizational Computer Matching Agreements with Social Security Administration to ensure that those agreements comply with the computer matching provisions of the Privacy Act. TRACS displays a 4-digit partial social security number for individuals receiving subsidy assistance.

Assessment Objective: DI-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Procedures and processes to ensure the integrity of personally identifiable information (PII) through existing security controls.
* Department policy and procedures for establishing Board.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and system owners/managers and OPCL].
* Organizational personnel with privacy review responsibilities. [note: interview CPCLO/OPCL].

Determine If Statement: DI-02 (a) - The organization documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls.

Result: Not Assessed

Determine If Statement: DI-02 (b) - The organization establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

Result: Not Assessed

Control Title: DM-01 -Minimization Of Personally Identifiable Information
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and
c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [%Assignment: organization-defined frequency, at least annually%] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Implementation Statement: HUD:
a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and
c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings and creating archives of data older than 2 years to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Assessment Objective: DM-1 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Privacy compliance process and information systems to ensure that PII is relevant and necessary to accomplish the legally authorized purpose of collection.
* Privacy compliance process and information systems to ensure that PII collected and retained is limited to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.
* PII holdings in information systems to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Interview

* Organizational personnel with privacy review responsibilities. [note: interview component system owners/managers and OPCL].
* Organizational personnel with privacy review responsibilities. [note: interview component system owners/managers].

Determine If Statement: DM-01 (a) - The organization identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection.

Result: Not Assessed

Determine If Statement: DM-01 (b) - The organization limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.

Result: Not Assessed

Determine If Statement: DM-01 (c) - The organization (1) Defines frequency for reviewing evaluation of PII holdings (at least annually); (2) Conducts an initial evaluation of PII holdings; (3) Regularly reviews PII holdings with organization-defined frequency to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Result: Not Assessed

Control Title: DM-02 -Data Retention And Disposal

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:

a. Retains each collection of personally identifiable information (PII) for [%Assignment: organization-defined time period%] to fulfill the purpose(s) identified in the notice or as required by law;

b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

c. Uses [%Assignment: organization-defined techniques or methods%] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Implementation Statement: HUD:

a. Retains each collection of personally identifiable information (PII) for five years to fulfill the purpose(s) identified in the notice or as required by law;

b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and annually secures 5 years of historic data.

Assessment Objective: DM-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* PII holdings in information systems to ensure that PII is collected and retained only for a defined time-period to fulfill the purpose(s) identified in the notice or as required by law.
* PII holdings in information systems to ensure that PII is disposed, destroyed, erased, and/or anonymized, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.
* Techniques or methods to ensure secure deletion or destruction of PII, and procedures to use such techniques and methods.

Interview

* Organizational personnel with privacy review responsibilities. [note: interview component system owners/managers].

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: DM-02 (a) - The organization (1) Defines frequency for retaining personally identifiable information (PII) to fulfill purpose(s) identified in notice; (2) Retains each collection of personally identifiable information (PII) with organization-defined frequency to fulfill the purpose(s) identified in the notice or as required by law.

Result: Not Assessed

Determine If Statement: DM-02 (b) - The organization disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

Result: Not Assessed

Determine If Statement: DM-02 (c) - The organization (1) Defines techniques and methods to delete or destroy PII; (2) Uses organization-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Result: Not Assessed

Control Title: DM-03 -Minimization Of PII Used In Testing, Training, And Research

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and
b. Implements controls to protect PII used for testing, training, and research.

Implementation Statement: HUD:
a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and
b. Implements controls to protect PII used for testing and training, such as partial SSN display and download.

Assessment Objective: DM-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research.
* Information systems to ensure that controls are being used to protect PII that is used for testing, training, and research.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs, OCIO, and OPCL].
* Organizational personnel with privacy review responsibilities. [note: interview component system owners/managers].

Determine If Statement: DM-03 (a) - The organization develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research.

Result: Not Assessed

Determine If Statement: DM-03 (b) - The organization implements controls to protect PII used for testing, training, and research.

Result: Not Assessed

Control Title: IA-01 -Identification And Authentication Policy And Procedures

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:
1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
b. Reviews and updates the current:
1. Identification and authentication policy [%Assignment: organization-defined frequency (b)(1)%]; and
2. Identification and authentication procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: HUD IT security policy (inclusive of identification and authentication) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Identification and authentication compliance policy is specifically addressed in Sections 5.1, 5.1.1, 5.1.2, and 5.1.3 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 5.1 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 contains the policy for Identification and Authentication. Section 5.1

Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented identification and authentication policy within Section 5.1. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to identification and authentication.
The identification and authentication policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The identification and authentication procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication security controls are documented within the Section 5.1 of the Information Technology Security Procedures, dated November 1, 2013.
The identification and authentication procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: IA-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Identification and authentication policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with identification and authentication responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: IA-01 (a)(01)[01] - The organization develops and documents an identification and authentication policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IA-01 (a)(01)[02] - The organization defines personnel or roles to whom the identification and authentication policy is to be disseminated.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IA-01 (a)(01)[03] - The organization disseminates the identification and authentication policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IA-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IA-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Not Assessed

Determine If Statement: IA-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IA-01 (b)(01)[01] - The organization defines the frequency to review and update the current identification and authentication policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IA-01 (b)(01)[02] - The organization reviews and updates the current identification and authentication policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IA-01 (b)(02)[01] - The organization defines the frequency to review and update the current identification and authentication procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IA-01 (b)(02)[02] - The organization reviews and updates the current identification and authentication procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: IA-02 -Identification And Authentication (Organizational Users)

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Implementation Statement: The information system uniquely identifies and authenticates users (or processes acting on behalf of users). Users are required to login in using authorized IDs and are locked out after 90 days if not used. Passwords must be reset per HUD security guidelines as well (at least every 90 days.) Please also refer to page 4 regarding WASS. Remote access for users is provided with VPN.

Assessment Objective: IA-2 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Identification and authentication policy
* Procedures addressing user identification and authentication
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* List of information system accounts
* Other relevant documents or records

Interview

* Organizational personnel with information system operations responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* Organizational personnel with account management responsibilities
* System developers

Test

* Organizational processes for uniquely identifying and authenticating users
* Automated mechanisms supporting and/or implementing identification and authentication capability

Determine If Statement: IA-02 - The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Result: Not Assessed

Control Title: IA-02(1) -Network Access To Privileged Accounts

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system implements multifactor authentication for network access to privileged accounts.

Implementation Statement: Remote access for users is provided with VPN and secure tunnel. Authentication is by user id, role and action code.

Assessment Objective: IA-2(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Identification and authentication policy
* Procedures addressing user identification and authentication
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* List of information system accounts
* Other relevant documents or records

Interview

* Organizational personnel with information system operations responsibilities
* Organizational personnel with account management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test

* Automated mechanisms supporting and/or implementing multifactor authentication capability

Determine If Statement: IA-02(01) - The information system implements multifactor authentication for network access to privileged accounts.

Result: Not Assessed

Control Title: IA-02(2) -Network Access To Non-Privileged Accounts

Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The information system implements multifactor authentication for network access to non-privileged accounts.

Implementation Statement: The information system does use multifactor authentication for network access to non-privileged accounts.

Assessment Objective: IA-2(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Identification and authentication policy
* Procedures addressing user identification and authentication
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* List of information system accounts
* Other relevant documents or records

Interview
* Organizational personnel with information system operations responsibilities
* Organizational personnel with account management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test
* Automated mechanisms supporting and/or implementing multifactor authentication capability

Determine If Statement: IA-02(02) - The information system implements multifactor authentication for network access to non-privileged accounts.

Result: Not Assessed

Control Title: IA-02(3) -Local Access To Privileged Accounts

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system implements multifactor authentication for local access to privileged accounts.

Implementation Statement: The information system does use multifactor authentication for local access to privileged accounts.

Assessment Objective: IA-2(3) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Identification and authentication policy
* Procedures addressing user identification and authentication
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* List of information system accounts
* Other relevant documents or records

Interview
* Organizational personnel with information system operations responsibilities
* Organizational personnel with account management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test
* Automated mechanisms supporting and/or implementing multifactor authentication capability

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IA-02(03) - The information system implements multifactor authentication for local access to privileged accounts.

Result: Not Assessed

Control Title: IA-02(8) -Network Access To Privileged Accounts - Replay Resistant

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

Implementation Statement: This is a common control under the purview of the Wide Area Security System (WASS) that is the gatekeeper to the information system.

Assessment Objective: IA-2(8) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Identification and authentication policy
* Procedures addressing user identification and authentication
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* List of privileged information system accounts
* Other relevant documents or records

Interview
* Organizational personnel with information system operations responsibilities
* Organizational personnel with account management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test
* Automated mechanisms supporting and/or implementing identification and authentication capability
* Automated mechanisms supporting and/or implementing replay resistant authentication mechanisms

Determine If Statement: IA-02(08) - The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

Result: Not Assessed

Control Title: IA-02(11) -Remote Access - Separate Device

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [%Assignment: organization-defined strength of mechanism requirements%].

Implementation Statement: TRACS contractors are off-site and remote into HUD systems through a secure tunnel. This level of security is the prevue of HITS contractors.

Assessment Objective: IA-2(11) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Identification and authentication policy
* Procedures addressing user identification and authentication
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* List of privileged and non-privileged information system accounts
* Other relevant documents or records

Interview

* Organizational personnel with information system operations responsibilities
* Organizational personnel with account management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test

* Automated mechanisms supporting and/or implementing identification and authentication capability

Determine If Statement: IA-02(11) [01] - The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

Result: Not Assessed

Determine If Statement: IA-02(11) [02] - The information system implements multifactor authentication for remote access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

Result: Not Assessed

Determine If Statement: IA-02(11) [03] - The organization defines strength of mechanism requirements to be enforced by a device separate from the system gaining remote access to privileged accounts.

Result: Not Assessed

Determine If Statement: IA-02(11) [04] - The organization defines strength of mechanism requirements to be enforced by a device separate from the system gaining remote access to non-privileged accounts.

Result: Not Assessed

Determine If Statement: IA-02(11) [05] - The information system implements multifactor authentication for remote access to privileged accounts such that a device, separate from the system gaining access, meets organization-defined strength of mechanism requirements.

Result: Not Assessed

Determine If Statement: IA-02(11) [06] - The information system implements multifactor authentication for remote access to non-privileged accounts such that a device, separate from the system gaining access, meets organization-defined strength of mechanism requirements.

Result: Not Assessed

Control Title: IA-02(12) -Acceptance Of Piv Credentials

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

Assessment Objective: IA-2(12) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Identification and authentication policy
* Procedures addressing user identification and authentication
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* PIV verification records
* Evidence of PIV credentials
* PIV credential authorizations
* Other relevant documents or records

Interview

* Organizational personnel with information system operations responsibilities
* Organizational personnel with account management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test

* Automated mechanisms supporting and/or implementing acceptance and verification of PIV credentials

Determine If Statement: IA-02(12) [01] - The information system accepts Personal Identity Verification (PIV) credentials.
Result: Not Assessed

Determine If Statement: IA-02(12) [02] - The information system electronically verifies Personal Identity Verification (PIV) credentials.
Result: Not Assessed

Control Title: IA-03 -Device Identification And Authentication
Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The information system uniquely identifies and authenticates [%Assignment: organization-defined specific and/or types of devices%] before establishing a [%Selection (one or more): local; remote; network%] connection.

Implementation Statement: The information system identifies and authenticates specific devices before establishing a connection.

Assessment Objective: IA-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Identification and authentication policy
* Procedures addressing device identification and authentication
* Information system design documentation
* List of devices requiring unique identification and authentication
* Device connection reports
* Information system configuration settings and associated documentation
* Other relevant documents or records

Interview

* Organizational personnel with operational responsibilities for device identification and authentication
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test

* Automated mechanisms supporting and/or implementing device identification and authentication capability

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IA-03 [01] - The organization defines specific and/or types of devices that the information system uniquely identifies and authenticates before establishing one or more of the following:
* a local connection;
* a remote connection; and/or
* a network connection.

Result: Not Assessed

Determine If Statement: IA-03 [02] - The information system uniquely identifies and authenticates organization-defined devices before establishing one or more of the following:
* a local connection;
* a remote connection; and/or
* a network connection.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Control Title: IA-04 -Identifier Management

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization manages information system identifiers by:
a. Receiving authorization from [%Assignment: organization-defined personnel or roles%] to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group, role, or device;
d. Preventing reuse of identifiers for [%Assignment: organization-defined time period%]; and
e. Disabling the identifier after [%Assignment: organization-defined time period of inactivity%].

Implementation Statement: This control is inherited from WASS, which performs user authentication, disables user access after 90 days of inactivity, and prevents password reuse for 8 generations. HUD manages user identifiers by: (i) uniquely identifying each user with a user H-ID, business partner M-ID, or contractor C-ID ; (ii) verifying the identity of each user with partial SSN; (iii) receiving authorization to issue a user identifier from an appropriate security official after a background check; (iv) ensuring that the user identifier is issued to the intended party via email notification and user initiated telephone assignment; (v) disabling user identifier after 90 days of inactivity; and (vi) archiving user identifiers. WASS prevents password reuse for 8 generations. Please see page 4 for additional details in the SSP re: access via WASS.HUD manages user identifiers by: (i) uniquely identifying each user with a user H-ID, business partner M-ID, or contractor C-ID ; (ii) verifying the identity of each user with partial SSN; (iii) receiving authorization to issue a user identifier from an appropriate security official after a background check; (iv) ensuring that the user identifier is issued to the intended party via email notification and user initiated telephone assignment; (v) disabling user identifier after 90 days of inactivity; and (vi) archiving user identifiers. WASS prevents password reuse for 8 generations. Please see page 4 for additional details in the SSP re: access via WASS.

Assessment Objective: IA-4 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* Identification and authentication policy
* Procedures addressing identifier management
* Procedures addressing account management
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* List of information system accounts
* List of identifiers generated from physical access control devices
* Other relevant documents or records

Interview
* Organizational personnel with identifier management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test
* Automated mechanisms supporting and/or implementing identifier management

Determine If Statement: IA-04 (a)[01] - The organization manages information system identifiers by defining personnel or roles from whom authorization must be received to assign:
* an individual identifier;
* a group identifier;
* a role identifier; and/or
* a device identifier.

Result: Not Assessed

Determine If Statement: IA-04 (a)[02] - The organization manages information system identifiers by receiving authorization from organization-defined personnel or roles to assign:
* an individual identifier;
* a group identifier;
* a role identifier; and/or
* a device identifier.

Result: Not Assessed

Determine If Statement: IA-04 (b) - The organization manages information system identifiers by selecting an identifier that identifies:
* an individual;
* a group;
* a role; and/or
* a device.

Result: Not Assessed

Determine If Statement: IA-04 (c) - The organization manages information system identifiers by assigning the identifier to the intended:
* individual;
* group;
* role; and/or
* device.

Result: Not Assessed

Determine If Statement: IA-04 (d)[01] - The organization manages information system identifiers by defining a time period for preventing reuse of identifiers.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IA-04 (d)[02] - The organization manages information system identifiers by preventing reuse of identifiers for the organization-defined time period.

Result: Not Assessed

Determine If Statement: IA-04 (e)[01] - The organization manages information system identifiers by defining a time period of inactivity to disable the identifier.

Result: Not Assessed

Determine If Statement: IA-04 (e)[02] - The organization manages information system identifiers by disabling the identifier after the organization-defined time period of inactivity.

Result: Not Assessed

Control Title: IA-05 -Authenticator Management

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization manages information system authenticators by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators [%Assignment: organization-defined time period by authenticator type%];
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts changes.

Implementation Statement: HUD manages information system authenticators (e.g., user ids, passwords, key cards) by: (i) defining initial authenticator content as a request from the user's supervisor; (ii) establishing administrative procedures for initial authenticator distribution by HUD's entry in CHAMPS and final approval by ADP Security, for lost/compromised, or damaged authenticators via the help desk after verification, and for revoking authenticators via HUD gone action; and (iii) changing default authenticators upon information system installation. Authentication occurs via ldap for webservices, and WASS for the online. Users are required to login in using authorized H, M and C-IDs and are locked out after 90 days if not used. Passwords must be reset per HUD security guidelines as well (at least every 90 days.)

Assessment Objective: IA-5 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Identification and authentication policy
* Procedures addressing authenticator management
* Information system design documentation
* Information system configuration settings and associated documentation
* List of information system authenticator types
* Change control records associated with managing information system authenticators
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with authenticator management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Automated mechanisms supporting and/or implementing authenticator management capability

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IA-05 (a) - The organization manages information system authenticators by verifying, as part of the initial authenticator distribution, the identity of:
* the individual receiving the authenticator;
* the group receiving the authenticator;
* the role receiving the authenticator; and/or
* the device receiving the authenticator.

Result: Not Assessed

Determine If Statement: IA-05 (a) - The organization manages information system authenticators by verifying, as part of the initial authenticator distribution, the identity of:
* the individual receiving the authenticator;
* the group receiving the authenticator;
* the role receiving the authenticator; and/or
* the device receiving the authenticator.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (b) - The organization manages information system authenticators by establishing initial authenticator content for authenticators defined by the organization.

Result: Not Assessed

Determine If Statement: IA-05 (b) - The organization manages information system authenticators by establishing initial authenticator content for authenticators defined by the organization.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (c) - The organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use.

Result: Not Assessed

Determine If Statement: IA-05 (c) - The organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (d)[01] - The organization manages information system authenticators by establishing and implementing administrative procedures for initial authenticator distribution.

Result: Not Assessed

Determine If Statement: IA-05 (d)[01] - The organization manages information system authenticators by establishing and implementing administrative procedures for initial authenticator distribution.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (d)[02] - The organization manages information system authenticators by establishing and implementing administrative procedures for lost/compromised or damaged authenticators.

Result: Not Assessed

Determine If Statement: IA-05 (d)[02] - The organization manages information system authenticators by establishing and implementing administrative procedures for lost/compromised or damaged authenticators.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (d)[03] - The organization manages information system authenticators by establishing and implementing administrative procedures for revoking authenticators.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IA-05 (d)[03] - The organization manages information system authenticators by establishing and implementing administrative procedures for revoking authenticators.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (e) - The organization manages information system authenticators by changing default content of authenticators prior to information system installation.

Result: Not Assessed

Determine If Statement: IA-05 (e) - The organization manages information system authenticators by changing default content of authenticators prior to information system installation.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (f)[01] - The organization manages information system authenticators by establishing minimum lifetime restrictions for authenticators.

Result: Not Assessed

Determine If Statement: IA-05 (f)[01] - The organization manages information system authenticators by establishing minimum lifetime restrictions for authenticators.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (f)[02] - The organization manages information system authenticators by establishing maximum lifetime restrictions for authenticators.

Result: Not Assessed

Determine If Statement: IA-05 (f)[02] - The organization manages information system authenticators by establishing maximum lifetime restrictions for authenticators.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (f)[03] - The organization manages information system authenticators by establishing reuse conditions for authenticators.

Result: Not Assessed

Determine If Statement: IA-05 (g)[01] - The organization manages information system authenticators by defining a time period (by authenticator type) for changing/refreshing authenticators.

Result: Not Assessed

Determine If Statement: IA-05 (g)[01] - The organization manages information system authenticators by defining a time period (by authenticator type) for changing/refreshing authenticators.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (g)[02] - The organization manages information system authenticators by changing/refreshing authenticators with the organization-defined time period by authenticator type.

Result: Not Assessed

Determine If Statement: IA-05 (g)[02] - The organization manages information system authenticators by changing/refreshing authenticators with the organization-defined time period by authenticator type.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (h)[01] - The organization manages information system authenticators by protecting authenticator content from unauthorized disclosure.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IA-05 (h)[01] - The organization manages information system authenticators by protecting authenticator content from unauthorized disclosure.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (h)[02] - The organization manages information system authenticators by protecting authenticator content from unauthorized modification.

Result: Not Assessed

Determine If Statement: IA-05 (h)[02] - The organization manages information system authenticators by protecting authenticator content from unauthorized modification.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05 (i)[01] - The organization manages information system authenticators by requiring individuals to take specific security safeguards to protect authenticators.

Result: Not Assessed

Determine If Statement: IA-05 (i)[02] - The organization manages information system authenticators by having devices implement specific security safeguards to protect authenticators.

Result: Not Assessed

Determine If Statement: IA-05 (j) - The organization manages information system authenticators by changing authenticators for group/role accounts when membership to those accounts changes.

Result: Not Assessed

Control Title: IA-05(1) -Password-Based Authentication

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The information system, for password-based authentication:
(a) Enforces minimum password complexity of [%Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type%];
(b) Enforces at least the following number of changed characters when new passwords are created: [%Assignment: organization-defined number (b)%];
(c) Stores and transmits only cryptographically-protected passwords;
(d) Enforces password minimum and maximum lifetime restrictions of [%Assignment: organization-defined numbers for lifetime minimum, lifetime maximum%];
(e) Prohibits password reuse for [%Assignment: organization-defined number (e)%] generations; and
(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Implementation Statement: This is a common control under the purview of the Web Access Security System (WASS).

Assessment Objective: IA-5(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Identification and authentication policy
* Password policy
* Procedures addressing authenticator management
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Password configurations and associated documentation
* Other relevant documents or records

Interview

* Organizational personnel with authenticator management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test

* Automated mechanisms supporting and/or implementing password-based authenticator management capability

Determine If Statement: IA-05(01) (a)[01,02,03,04] - For password-based authentication:
* the organization defines requirements for case sensitivity;
* the organization defines requirements for number of characters;
* the organization defines requirements for the mix of upper-case letters, lower-case letters, numbers and special characters;
* the organization defines minimum requirements for each type of character.

Result: Not Assessed

Determine If Statement: IA-05(01) (a)[01,02,03,04] - For password-based authentication:
* the organization defines requirements for case sensitivity;
* the organization defines requirements for number of characters;
* the organization defines requirements for the mix of upper-case letters, lower-case letters, numbers and special characters;
* the organization defines minimum requirements for each type of character.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(01) (a)[05] - For password-based authentication the information system enforces minimum password complexity of organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type.

Result: Not Assessed

Determine If Statement: IA-05(01) (a)[05] - For password-based authentication the information system enforces minimum password complexity of organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(01) (b)[01] - For password-based authentication the organization defines a minimum number of changed characters to be enforced when new passwords are created.

Result: Not Assessed

Determine If Statement: IA-05(01) (b)[01] - For password-based authentication the organization defines a minimum number of changed characters to be enforced when new passwords are created.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IA-05(01) (b)[02] - For password-based authentication the information system enforces at least the organization-defined minimum number of characters that must be changed when new passwords are created.
Result: Not Assessed

Determine If Statement: IA-05(01) (b)[02] - For password-based authentication the information system enforces at least the organization-defined minimum number of characters that must be changed when new passwords are created.
Inherited From: [Externally Inherited] F87TRACS
Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(01) (c) - For password-based authentication the information system stores and transmits only encrypted representations of passwords.
Result: Not Assessed

Determine If Statement: IA-05(01) (c) - For password-based authentication the information system stores and transmits only encrypted representations of passwords.
Inherited From: [Externally Inherited] F87TRACS
Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(01) (d)[01] - For password-based authentication the organization defines numbers for password minimum lifetime restrictions to be enforced for passwords.
Result: Not Assessed

Determine If Statement: IA-05(01) (d)[01] - For password-based authentication the organization defines numbers for password minimum lifetime restrictions to be enforced for passwords.
Inherited From: [Externally Inherited] F87TRACS
Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(01) (d)[02] - For password-based authentication the organization defines numbers for password maximum lifetime restrictions to be enforced for passwords.
Result: Not Assessed

Determine If Statement: IA-05(01) (d)[02] - For password-based authentication the organization defines numbers for password maximum lifetime restrictions to be enforced for passwords.
Inherited From: [Externally Inherited] F87TRACS
Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(01) (d)[03] - For password-based authentication the information system enforces password minimum lifetime restrictions of organization-defined numbers for lifetime minimum.
Result: Not Assessed

Determine If Statement: IA-05(01) (d)[03] - For password-based authentication the information system enforces password minimum lifetime restrictions of organization-defined numbers for lifetime minimum.
Inherited From: [Externally Inherited] F87TRACS
Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(01) (d)[04] - For password-based authentication the information system enforces password maximum lifetime restrictions of organization-defined numbers for lifetime maximum.
Result: Not Assessed

Determine If Statement: IA-05(01) (d)[04] - For password-based authentication the information system enforces password maximum lifetime restrictions of organization-defined numbers for lifetime maximum.
Inherited From: [Externally Inherited] F87TRACS
Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(01) (e)[01] - For password-based authentication the organization defines the number of password generations to be prohibited from password reuse.
Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IA-05(01) (e)[01] - For password-based authentication the organization defines the number of password generations to be prohibited from password reuse.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(01) (e)[02] - For password-based authentication the information system prohibits password reuse for the organization-defined number of generations.

Result: Not Assessed

Determine If Statement: IA-05(01) (f) - For password-based authentication the information system allows the use of a temporary password for system logons with an immediate change to a permanent password.

Result: Not Assessed

Control Title: IA-05(2) -Pki-Based Authentication

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The information system, for PKI-based authentication:
(a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
(b) Enforces authorized access to the corresponding private key;
(c) Maps the authenticated identity to the account of the individual or group; and
(d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Implementation Statement: This is a common control under the Web Access Security System (WASS).

Assessment Objective: IA-5(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Identification and authentication policy
* Procedures addressing authenticator management
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* PKI certification validation records
* PKI certification revocation lists
* Other relevant documents or records

Interview
* Organizational personnel with PKI-based, authenticator management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test
* Automated mechanisms supporting and/or implementing PKI-based, authenticator management capability

Determine If Statement: IA-05(02) (a)[01] - The information system, for PKI-based authentication validates certifications by constructing a certification path to an accepted trust.

Result: Not Assessed

Determine If Statement: IA-05(02) (a)[01] - The information system, for PKI-based authentication validates certifications by constructing a certification path to an accepted trust.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(02) (a)[02] - The information system, for PKI-based authentication validates certifications by verifying a certification path to an accepted trust.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IA-05(02) (a)[02] - The information system, for PKI-based authentication validates certifications by verifying a certification path to an accepted trust.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(02) (a)[03] - The information system, for PKI-based authentication includes checking certificate status information when constructing and verifying the certification path.

Result: Not Assessed

Determine If Statement: IA-05(02) (a)[03] - The information system, for PKI-based authentication includes checking certificate status information when constructing and verifying the certification path.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(02) (b) - The information system, for PKI-based authentication enforces authorized access to the corresponding private key.

Result: Not Assessed

Determine If Statement: IA-05(02) (b) - The information system, for PKI-based authentication enforces authorized access to the corresponding private key.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(02) (c) - The information system, for PKI-based authentication maps the authenticated identity to the account of the individual or group.

Result: Not Assessed

Determine If Statement: IA-05(02) (c) - The information system, for PKI-based authentication maps the authenticated identity to the account of the individual or group.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(02) (d) - The information system, for PKI-based authentication implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Result: Not Assessed

Control Title: IA-05(3) -In-Person Or Trusted Third-Party Registration

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization requires that the registration process to receive [%Assignment: organization-defined types of and/or specific authenticators%] be conducted [%Selection: in person; by a trusted third party%] before [%Assignment: organization-defined registration authority%] with authorization by [%Assignment: organization-defined personnel or roles%].

Implementation Statement: This is a common control under the purview of the Web Access Security System (WASS).

Assessment Objective: IA-5(3) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Identification and authentication policy
* Procedures addressing authenticator management
* Registration process for receiving information system authenticators
* List of authenticators requiring in-person registration
* List of authenticators requiring trusted third party registration
* Authenticator registration documentation
* Other relevant documents or records

Interview

* Organizational personnel with authenticator management responsibilities
* Registration authority
* Organizational personnel with information security responsibilities

Determine If Statement: IA-05(03) [01] - The organization defines types of and/or specific authenticators to be received in person or by a trusted third party.

Result: Not Assessed

Determine If Statement: IA-05(03) [01] - The organization defines types of and/or specific authenticators to be received in person or by a trusted third party.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(03) [02] - The organization defines the registration authority with oversight of the registration process for receipt of organization-defined types of and/or specific authenticators.

Result: Not Assessed

Determine If Statement: IA-05(03) [02] - The organization defines the registration authority with oversight of the registration process for receipt of organization-defined types of and/or specific authenticators.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(03) [03] - The organization defines personnel or roles responsible for authorizing organization-defined registration authority.

Result: Not Assessed

Determine If Statement: IA-05(03) [03] - The organization defines personnel or roles responsible for authorizing organization-defined registration authority.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: IA-05(03) [04] - The organization defines if the registration process is to be conducted:

* in person; or
* by a trusted third party.

Result: Not Assessed

Determine If Statement: IA-05(03) [05] - The organization requires that the registration process to receive organization-defined types of and/or specific authenticators be conducted in person or by a trusted third party before organization-defined registration authority with authorization by organization-defined personnel or roles.

Result: Not Assessed

Determine If Statement: IA-05(03) [05] - The organization requires that the registration process to receive organization-defined types of and/or specific authenticators be conducted in person or by a trusted third party before organization-defined registration authority with authorization by organization-defined personnel or roles.

Inherited From: [Externally Inherited] F87TRACS

Result: **Assessed by:** **Date:**

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: IA-05(11) -Hardware Token-Based Authentication

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system, for hardware token-based authentication, employs mechanisms that satisfy [%Assignment: organization-defined token quality requirements%].

Assessment Objective: IA-5(11) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Identification and authentication policy
* Procedures addressing authenticator management
* Security plan
* Information system design documentation
* Automated mechanisms employing hardware token-based authentication for the information system
* List of token quality requirements
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with authenticator management responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test
* Automated mechanisms supporting and/or implementing hardware token-based authenticator management capability

Determine If Statement: IA-05(11) [01] - For hardware token-based authentication the organization defines token quality requirements to be satisfied.

Result: Not Assessed

Determine If Statement: IA-05(11) [02] - For hardware token-based authentication the information system employs mechanisms that satisfy organization-defined token quality requirements.

Result: Not Assessed

Control Title: IA-06 -Authenticator Feedback

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Implementation Statement: The information system provides feedback to a user during an attempted authentication and that feedback does not compromise the authentication mechanism.

Assessment Objective: IA-6 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Identification and authentication policy
* Procedures addressing authenticator feedback
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test

* Automated mechanisms supporting and/or implementing the obscuring of feedback of authentication information during authentication

Determine If Statement: IA-06 - The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Result: Not Assessed

Control Title: IA-07 -Cryptographic Module Authentication

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Implementation Statement: System does not use cryptographic modules.

Assessment Objective: IA-7 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Identification and authentication policy
* Procedures addressing cryptographic module authentication
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibility for cryptographic module authentication
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers

Test

* Automated mechanisms supporting and/or implementing cryptographic module authentication

Determine If Statement: IA-07 - The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Result: Not Assessed

Control Title: IA-08 -Identification And Authentication (Non-Organizational Users)

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Implementation Statement: The information system does uniquely identify and authenticate non-organizational users. This control is inherited from WASS. All users – even those outside of HUD – are industry partners that must have a valid

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

WASS ID.

Assessment Objective: IA-8 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Identification and authentication policy
* Procedures addressing user identification and authentication
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* List of information system accounts
* Other relevant documents or records

Interview
* Organizational personnel with information system operations responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* Organizational personnel with account management responsibilities

Test
* Automated mechanisms supporting and/or implementing identification and authentication capability

Determine If Statement: IA-08 - The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Result: Not Assessed

Control Title: IA-08(1) -Acceptance Of Piv Credentials From Other Agencies

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

Assessment Objective: IA-8(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Identification and authentication policy
* Procedures addressing user identification and authentication
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* PIV verification records
* Evidence of PIV credentials
* PIV credential authorizations
* Other relevant documents or records

Interview
* Organizational personnel with information system operations responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers
* Organizational personnel with account management responsibilities

Test
* Automated mechanisms supporting and/or implementing identification and authentication capability
* Automated mechanisms that accept and verify PIV credentials

Determine If Statement: IA-08(01) [01] - The information system accepts Personal Identity Verification (PIV) credentials from other agencies.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IA-08(01) [02] - The information system electronically verifies Personal Identity Verification (PIV) credentials from other agencies.
Result: Not Assessed

Control Title: IA-08(2) -Acceptance Of Third-Party Credentials
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system accepts only FICAM-approved third-party credentials.

Assessment Objective: IA-8(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Identification and authentication policy
* Procedures addressing user identification and authentication
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* List of FICAM-approved, third-party credentialing products, components, or services procured and implemented by organization
* Third-party credential verification records
* Evidence of FICAM-approved third-party credentials
* Third-party credential authorizations
* Other relevant documents or records

Interview
* Organizational personnel with information system operations responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers
* Organizational personnel with account management responsibilities

Test
* Automated mechanisms supporting and/or implementing identification and authentication capability
* Automated mechanisms that accept FICAM-approved credentials

Determine If Statement: IA-08(02) - The information system accepts only FICAM-approved third-party credentials.
Result: Not Assessed

Control Title: IA-08(3) -Use Of Ficam-Approved Products
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization employs only FICAM-approved information system components in [%Assignment: organization-defined information systems%] to accept third-party credentials.

Assessment Objective: IA-8(3) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Identification and authentication policy
* System and services acquisition policy
* Procedures addressing user identification and authentication
* Procedures addressing the integration of security requirements into the acquisition process
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Third-party credential validations
* Third-party credential authorizations
* Third-party credential records
* List of FICAM-approved information system components procured and implemented by organization
* Acquisition documentation
* Acquisition contracts for information system procurements or services
* Other relevant documents or records

Interview

* Organizational personnel with information system operations responsibilities
* System/network administrators
* Organizational personnel with account management responsibilities
* Organizational personnel with information system security, acquisition, and contracting responsibilities

Test

* Automated mechanisms supporting and/or implementing identification and authentication capability

Determine If Statement: IA-08(03) [01] - The organization defines information systems in which only FICAM-approved information system components are to be employed to accept third-party credentials.

Result: Not Assessed

Determine If Statement: IA-08(03) [02] - The organization employs only FICAM-approved information system components in organization-defined information systems to accept third-party credentials.

Result: Not Assessed

Control Title: IA-08(4) -Use Of Ficam-Issued Profiles

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system conforms to FICAM-issued profiles.

Assessment Objective: IA-8(4) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Identification and authentication policy
* System and services acquisition policy
* Procedures addressing user identification and authentication
* Procedures addressing the integration of security requirements into the acquisition process
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* List of FICAM-issued profiles and associated, approved protocols
* Acquisition documentation
* Acquisition contracts for information system procurements or services
* Other relevant documents or records

Interview

* Organizational personnel with information system operations responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* System developers
* Organizational personnel with account management responsibilities

Test

* Automated mechanisms supporting and/or implementing identification and authentication capability
* Automated mechanisms supporting and/or implementing conformance with FICAM-issued profiles

Determine If Statement: IA-08(04) - The information system conforms to FICAM-issued profiles.
Result: Not Assessed

Control Title: IP-01 -Consent
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;
b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and
d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Implementation Statement: HUD:
a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;
b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and
d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Assessment Objective: IP-1 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Privacy compliance process and documentation to ensure that individuals are provided with a means, if necessary and appropriate, to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection.
* Privacy compliance process and documentation to ensure that individuals are provided with a means, if necessary and appropriate, to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.
* Privacy compliance process and documentation to ensure that system owners consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.
* Privacy compliance process and documentation to ensure that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Interview

* Organizational personnel with privacy review responsibilities. [note: interview component system owners/managers and OPCL].

Determine If Statement: IP-01 (a) - The organization provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection.

Result: Not Assessed

Determine If Statement: IP-01 (b) - The organization provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.

Result: Not Assessed

Determine If Statement: IP-01 (c) - The organization obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

Result: Not Assessed

Determine If Statement: IP-01 (d) - The organization ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Result: Not Assessed

Control Title: IP-02 -Individual Access

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:

a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;
b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;
c. Publishes access procedures in System of Records Notices (SORNs); and
d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Implementation Statement: The organization:

a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;
b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;
c. Publishes access procedures in System of Records Notices (SORNs); and
d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Assessment Objective: IP-2 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Privacy compliance process and documentation to ensure that access procedures in System of Records Notices (SORNs) are published.
* Privacy compliance process and documentation to ensure that individuals are provided with the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records, if necessary and appropriate.
* Privacy compliance process and documentation to ensure that rules and regulations are published which govern how individuals may request access to records maintained in a Privacy Act system of records.
* Privacy compliance process, documentation, and department policy to ensure that Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests are met.

Interview

* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs/record managers/system owners and managers, and OPCL].
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and OPCL].
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and record managers, and OPCL].

Determine If Statement: IP-02 (a) - The organization provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records.

Result: Not Assessed

Determine If Statement: IP-02 (b) - The organization publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records.

Result: Not Assessed

Determine If Statement: IP-02 (c) - The organization publishes access procedures in System of Records Notices (SORNs).

Result: Not Assessed

Determine If Statement: IP-02 (d) - The organization adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Result: Not Assessed

Control Title: IP-03 -Redress

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and
b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

Implementation Statement: The organization:
a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and
b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

Assessment Objective: IP-3 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Privacy compliance process and documentation to ensure that individuals have the ability to correct or amend, as appropriate, inaccurate personally identifiable information (PII) maintained by the organization.
* Privacy compliance process to ensure that a process exists that provides for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, and notifies affected individuals that their information has been corrected or amended.

Interview

* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and record and system managers, and OPCL].
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and record managers, and OPCL].

Determine If Statement: IP-03 (a) - The organization provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate.

Result: Not Assessed

Determine If Statement: IP-03 (b) - The organization establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

Result: Not Assessed

Control Title: IP-04 -Complaint Management

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Implementation Statement: The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Assessment Objective: IP-4 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Privacy compliance process and documentation to ensure that the Department receives and responds to complaints, concerns, or questions from individuals about the organizational privacy practices.

Interview

* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and OPCL].

Determine If Statement: IP-04 - The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Result: Not Assessed

Control Title: IR-01 -Incident Response Policy And Procedures

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:

a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:
   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

b. Reviews and updates the current:
   1. Incident response policy [%Assignment: organization-defined frequency (b)(1)%]; and
   2. Incident response procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: HUD IT security policy (inclusive of incident response) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Incident response compliance policy is specifically addressed in Section 4.7.1 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 4.8 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.

Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented incident response policy within Section 4.8. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to incident response.
The incident response policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The incident response procedures to facilitate the implementation of the incident response policy and associated incident response security controls are documented within the Section 4.8 of the Information Technology Security Procedures, dated November 1, 2013.
The incident response procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: IR-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Incident response policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with incident response responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: IR-01 (a)(01)[01] - The organization develops and documents an incident response policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IR-01 (a)(01)[02] - The organization defines personnel or roles to whom the incident response policy is to be disseminated.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IR-01 (a)(01)[03] - The organization disseminates the incident response policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IR-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IR-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Not Assessed

Determine If Statement: IR-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IR-01 (b)(01)[01] - The organization defines the frequency to review and update the current incident response policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IR-01 (b)(01)[02] - The organization reviews and updates the current incident response policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IR-01 (b)(02)[01] - The organization defines the frequency to review and update the current incident response procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: IR-01 (b)(02)[02] - The organization reviews and updates the current incident response procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: IR-02 -Incident Response Training

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:
a. Within [%Assignment: organization-defined time period%] of assuming an incident response role or responsibility;
b. When required by information system changes; and
c. [%Assignment: organization-defined frequency%] thereafter.

Implementation Statement: Incident response roles and responsibilities are incorporated into the security awareness training, which all HUD employees and contractors are required to take annually.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.Incident response roles and responsibilities are incorporated into the security awareness training, which all HUD employees and contractors are required to take annually. This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.

Assessment Objective: IR-2 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Incident response policy
* Procedures addressing incident response training
* Incident response training curriculum
* Incident response training materials
* Security plan
* Incident response plan
* Security plan
* Incident response training records
* Other relevant documents or records

Interview

* Organizational personnel with incident response training and operational responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: IR-02 (a)[01] - The organization defines a time period within which incident response training is to be provided to information system users assuming an incident response role or responsibility.

Result: Not Assessed

Determine If Statement: IR-02 (a)[02] - The organization provides incident response training to information system users consistent with assigned roles and responsibilities within the organization-defined time period of assuming an incident response role or responsibility.

Result: Not Assessed

Determine If Statement: IR-02 (b) - The organization provides incident response training to information system users consistent with assigned roles and responsibilities when required by information system changes.

Result: Not Assessed

Determine If Statement: IR-02 (c)[01] - The organization defines the frequency to provide refresher incident response training to information system users consistent with assigned roles or responsibilities.

Result: Not Assessed

Determine If Statement: IR-02 (c)[02] - The organization after the initial incident response training, provides refresher incident response training to information system users consistent with assigned roles and responsibilities in accordance with the organization-defined frequency to provide refresher training.

Result: Not Assessed

Control Title: IR-03 -Incident Response Testing

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization tests the incident response capability for the information system [%Assignment: organization-defined frequency%] using [%Assignment: organization-defined tests%] to determine the incident response effectiveness and documents the results.

Implementation Statement: This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HUD CSIRC/IRT.
This control is not currently implemented within HUD. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HUD Computer Security Incident Response Center and Incident Response Team (CSIRC/IRT).

Assessment Objective: IR-3 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Incident response policy
* Contingency planning policy
* Procedures addressing incident response testing
* Procedures addressing contingency plan testing
* Incident response testing material
* Incident response test results
* Incident response test plan
* Incident response plan
* Contingency plan
* Security plan
* Other relevant documents or records

Interview

* Organizational personnel with incident response testing responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: IR-03 [01] - The organization defines incident response tests to test the incident response capability for the information system.

Result: Not Assessed

Determine If Statement: IR-03 [02] - The organization defines the frequency to test the incident response capability for the information system.

Result: Not Assessed

Determine If Statement: IR-03 [03] - The organization tests the incident response capability for the information system with the organization-defined frequency, using organization-defined tests to determine the incident response effectiveness and documents the results.

Result: Not Assessed

Control Title: IR-03(2) -Coordination With Related Plans

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization coordinates incident response testing with organizational elements responsible for related plans.

Implementation Statement: The organization coordinates incident response testing with organizational elements responsible for related plans.

Assessment Objective: IR-3(2) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Incident response policy
* Contingency planning policy
* Procedures addressing incident response testing
* Incident response testing documentation
* Incident response plan
* Business continuity plans
* Contingency plans
* Disaster recovery plans
* Continuity of operations plans
* Crisis communications plans
* Critical infrastructure plans
* Occupant emergency plans
* Security plan
* Other relevant documents or records

Interview

* Organizational personnel with incident response testing responsibilities
* Organizational personnel with responsibilities for testing organizational plans related to incident response testing
* Organizational personnel with information security responsibilities

Determine If Statement: IR-03(02) - The organization coordinates incident response testing with organizational elements responsible for related plans.

Result: Not Assessed

Control Title: IR-04 -Incident Handling

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Implementation Statement: The HUD Incident Reporting Procedures outlines the process for incident handling. The HUD CSIRC/IRT executes regular vulnerability scans on IT infrastructure components looking for potential security incidents. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HUD CSIRC/IRT.

Assessment Objective: IR-4 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Incident response policy
* Contingency planning policy
* Procedures addressing incident handling
* Incident response plan
* Contingency plan
* Security plan
* Other relevant documents or records

Interview

* Organizational personnel with incident handling responsibilities
* Organizational personnel with contingency planning responsibilities
* Organizational personnel with information security responsibilities

Test

* Incident handling capability for the organization

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IR-04 (a)[01] - The organization implements an incident handling capability for security incidents that includes preparation.
Result: Not Assessed

Determine If Statement: IR-04 (a)[02] - The organization implements an incident handling capability for security incidents that includes detection and analysis.
Result: Not Assessed

Determine If Statement: IR-04 (a)[03] - The organization implements an incident handling capability for security incidents that includes containment.
Result: Not Assessed

Determine If Statement: IR-04 (a)[04] - The organization implements an incident handling capability for security incidents that includes eradication.
Result: Not Assessed

Determine If Statement: IR-04 (a)[05] - The organization implements an incident handling capability for security incidents that includes recovery.
Result: Not Assessed

Determine If Statement: IR-04 (b) - The organization coordinates incident handling activities with contingency planning activities.
Result: Not Assessed

Determine If Statement: IR-04 (c)[01][a] - The organization incorporates lessons learned from ongoing incident handling activities into incident response procedures.
Result: Not Assessed

Determine If Statement: IR-04 (c)[01][b] - The organization incorporates lessons learned from ongoing incident handling activities into training.
Result: Not Assessed

Determine If Statement: IR-04 (c)[01][c] - The organization incorporates lessons learned from ongoing incident handling activities into testing/exercises.
Result: Not Assessed

Determine If Statement: IR-04 (c)[02][a] - The organization implements the resulting changes accordingly to incident response procedures.
Result: Not Assessed

Determine If Statement: IR-04 (c)[02][b] - The organization implements the resulting changes accordingly to training.
Result: Not Assessed

Determine If Statement: IR-04 (c)[02][c] - The organization implements the resulting changes accordingly to testing/exercises.

Result: Not Assessed

Control Title: IR-04(1) -Automated Incident Handling Processes
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization employs automated mechanisms to support the incident handling process.

Implementation Statement: The HUD on-line ticket tracking system, ServiceDesk, is used to document and track security incidents reported by HUD employees and contractors through the HUD National Help Desk. In addition, IDS sensors constantly monitor, collect data, and alert on (potential) network intrusion attempts. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HUD CSIRC/IRT.

Assessment Objective: IR-4(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Incident response policy
* Procedures addressing incident handling
* Automated mechanisms supporting incident handling
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Incident response plan
* Security plan
* Other relevant documents or records

Interview

* Organizational personnel with incident handling responsibilities
* Organizational personnel with information security responsibilities

Test

* Automated mechanisms that support and/or implement the incident handling process

Determine If Statement: IR-04(01) - The organization employs automated mechanisms to support the incident handling process.

Result: Not Assessed

Control Title: IR-05 -Incident Monitoring

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization tracks and documents information system security incidents.

Implementation Statement: Security incidents are tracked and documented on an ongoing basis using the HUD on-line ticket tracking system, ServiceDesk. In addition, IDS sensor reports are generated and provided to the HUD CSIRC/IRT on a weekly basis by the IDS administrators. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HUD CSIRC/IRT.

Assessment Objective: IR-5 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Incident response policy
* Procedures addressing incident monitoring
* Incident response records and documentation
* Incident response plan
* Security plan
* Other relevant documents or records

Interview

* Organizational personnel with incident monitoring responsibilities
* Organizational personnel with information security responsibilities

Test

* Incident monitoring capability for the organization
* Automated mechanisms supporting and/or implementing tracking and documenting of system security incidents

Determine If Statement: IR-05 [01] - The organization tracks information system security incidents.

Result: Not Assessed

Determine If Statement: IR-05 [02] - The organization documents information system security incidents.

Result: Not Assessed

Control Title: IR-06 -Incident Reporting

Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Requires personnel to report suspected security incidents to the organizational incident response capability within [%Assignment: organization-defined time period%]; and
b. Reports security incident information to [%Assignment: organization-defined authorities%].

Implementation Statement: Actual and suspected security incidents are reported by HUD employees and contractors via a call to the HUD National Help Desk. The HUD Incident Reporting Procedures describes the reporting process flow and provides reporting timeframes for security event categories in accordance with U.S. CERT federal incident reporting guidelines, inclusive of notification, as required, to appropriate authorities at all levels.
This is a common control, the implementation of which is the combined responsibility of the HUD Office of IT Security, the HITS Contractors, the System Owners of Major Applications, and the HUD CSIRC/IRT.

Assessment Objective: IR-6 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Incident response policy
* Procedures addressing incident reporting
* Incident reporting records and documentation
* Incident response plan
* Security plan
* Other relevant documents or records

Interview
* Organizational personnel with incident reporting responsibilities
* Organizational personnel with information security responsibilities
* Personnel who have/should have reported incidents
* Personnel (authorities) to whom incident information is to be reported

Test
* Organizational processes for incident reporting
* Automated mechanisms supporting and/or implementing incident reporting

Determine If Statement: IR-06 (a)[01] - The organization defines the time period within which personnel report suspected security incidents to the organizational incident response capability.
Result: Not Assessed

Determine If Statement: IR-06 (a)[02] - The organization requires personnel to report suspected security incidents to the organizational incident response capability within the organization-defined time period.
Result: Not Assessed

Determine If Statement: IR-06 (b)[01] - The organization defines authorities to whom security incident information is to be reported.
Result: Not Assessed

Determine If Statement: IR-06 (b)[02] - The organization reports security incident information to organization-defined authorities.
Result: Not Assessed

Control Title: IR-06(1) -Automated Reporting
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization employs automated mechanisms to assist in the reporting of security incidents.

Implementation Statement: The HUD on-line ticket tracking system, ServiceDesk, is used to document and track security incidents reported through the HUD National Help Desk. In addition, IDS sensors constantly monitor, collect data, and alert on potential network intrusion attempts. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HUD CSIRC/IRT.

Assessment Objective: IR-6(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Incident response policy
* Procedures addressing incident reporting
* Automated mechanisms supporting incident reporting
* Information system design documentation
* Information system configuration settings and associated documentation
* Incident response plan
* Security plan
* Other relevant documents or records

Interview

* Organizational personnel with incident reporting responsibilities
* Organizational personnel with information security responsibilities

Test

* Organizational processes for incident reporting
* Automated mechanisms supporting and/or implementing reporting of security incidents

Determine If Statement: IR-06(01) - The organization employs automated mechanisms to assist in the reporting of security incidents.

Result: Not Assessed

Control Title: IR-07 -Incident Response Assistance

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Implementation Statement: The HUD CSIRC/IRT serves as the support resource to all HUD users for incident handling and reporting assistance.
This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HUD CSIRC/IRT.
The HUD CSIRC/IRT serves as the support resource to all HUD users for incident handling and reporting assistance. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HUD CSIRC/IRT.

Assessment Objective: IR-7 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Incident response policy
* Procedures addressing incident response assistance
* Incident response plan
* Security plan
* Other relevant documents or records

Interview

* Organizational personnel with incident response assistance and support responsibilities
* Organizational personnel with access to incident response support and assistance capability
* Organizational personnel with information security responsibilities

Test

* Organizational processes for incident response assistance
* Automated mechanisms supporting and/or implementing incident response assistance

Determine If Statement: IR-07 [01] - The organization provides an incident response support resource that is integral to the organizational incident response capability.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IR-07 [02] - The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Result: Not Assessed

Control Title: IR-07(1) -Automation Support For Availability Of Information / Support

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Implementation Statement: IDS sensors constantly monitor, collect data, and alert on potential network intrusion attempts. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HUD CSIRC/IRTIDS sensors constantly monitor, collect data, and alert on potential network intrusion attempts. This is a common control, the implementation of which is the joint responsibility of the HUD Office of IT Security and the HUD CSIRC/IRT.

Assessment Objective: IR-7(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Incident response policy
* Procedures addressing incident response assistance
* Automated mechanisms supporting incident response support and assistance
* Information system design documentation
* Information system configuration settings and associated documentation
* Incident response plan
* Security plan
* Other relevant documents or records

Interview
* Organizational personnel with incident response support and assistance responsibilities
* Organizational personnel with access to incident response support and assistance capability
* Organizational personnel with information security responsibilities

Test
* Organizational processes for incident response assistance
* Automated mechanisms supporting and/or implementing an increase in the availability of incident response information and support

Determine If Statement: IR-07(01) - The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Result: Not Assessed

Control Title: IR-08 -Incident Response Plan

Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Develops an incident response plan that:
1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
8. Is reviewed and approved by [%Assignment: organization-defined personnel or roles%];
b. Distributes copies of the incident response plan to [%Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements (b)%];
c. Reviews the incident response plan [%Assignment: organization-defined frequency%];
d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
e. Communicates incident response plan changes to [%Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements (e)%]; and
f. Protects the incident response plan from unauthorized disclosure and modification.

Implementation Statement: HUD incorporates NIST standards:
1. Develop and maintain HUD's Incident Response Plan as part of OCIO's responsibility as the common control provider for the Department. (HUD-CIRT, OCIO)
2. Ensure the plan is distributed upon request and on an as-needed basis to incident response personnel. HUD-CIRT maintains the list of incident response personnel. (HUD-CIRT, OCIO)
3. Update and revise HUD's Incident Response Plan to address system/organizational changes or problems. At a minimum, the Plan is reviewed annually. (HUD-CIRT, OCIO)

Assessment Objective: IR-8 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Incident response policy
* Procedures addressing incident response planning
* Incident response plan
* Records of incident response plan reviews and approvals
* Other relevant documents or records
Interview
* Organizational personnel with incident response planning responsibilities
* Organizational personnel with information security responsibilities
Test
* Organizational incident response plan and related organizational processes

Determine If Statement: IR-08 (a)(01) - The organization develops an incident response plan that provides the organization with a roadmap for implementing its incident response capability.
Result: Not Assessed

Determine If Statement: IR-08 (a)(02) - The organization develops an incident response plan that describes the structure and organization of the incident response capability.
Result: Not Assessed

Determine If Statement: IR-08 (a)(03) - The organization develops an incident response plan that provides a high-level approach for how the incident response capability fits into the overall organization.
Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IR-08 (a)(04) - The organization develops an incident response plan that meets the unique requirements of the organization, which relate to:
* mission;
* size;
* structure;
* functions.

Result: Not Assessed

Determine If Statement: IR-08 (a)(05) - The organization develops an incident response plan that defines reportable incidents.

Result: Not Assessed

Determine If Statement: IR-08 (a)(06) - The organization develops an incident response plan that provides metrics for measuring the incident response capability within the organization.

Result: Not Assessed

Determine If Statement: IR-08 (a)(07) - The organization develops an incident response plan that defines the resources and management support needed to effectively maintain and mature an incident response capability.

Result: Not Assessed

Determine If Statement: IR-08 (a)(08)[01] - The organization develops an incident response plan that defines personnel or roles to review and approve the incident response plan.

Result: Not Assessed

Determine If Statement: IR-08 (a)(08)[02] - The organization develops an incident response plan that is reviewed and approved by organization-defined personnel or roles.

Result: Not Assessed

Determine If Statement: IR-08 (b)[01] - The organization
* defines incident response personnel (identified by name and/or by role) to whom copies of the incident response plan are to be distributed;
* defines organizational elements to whom copies of the incident response plan are to be distributed.

Result: Not Assessed

Determine If Statement: IR-08 (b)[02] - The organization distributes copies of the incident response plan to organization-defined incident response personnel (identified by name and/or by role) and organizational elements.

Result: Not Assessed

Determine If Statement: IR-08 (c)[01] - The organization defines the frequency to review the incident response plan.

Result: Not Assessed

Determine If Statement: IR-08 (c)[02] - The organization reviews the incident response plan with the organization-defined frequency.

Result: Not Assessed

Determine If Statement: IR-08 (d) - The organization updates the incident response plan to address system/organizational changes or problems encountered during plan:
* implementation;
* execution; or
* testing.

Result: Not Assessed

Determine If Statement: IR-08 (e)[01] - The organization
* defines incident response personnel (identified by name and/or by role) to whom incident response plan changes are to be communicated;
* defines organizational elements to whom incident response plan changes are to be communicated.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: IR-08 (e)[02] - The organization communicates incident response plan changes to organization-defined incident response personnel (identified by name and/or by role) and organizational elements.

Result: Not Assessed

Determine If Statement: IR-08 (f) - The organization protects the incident response plan from unauthorized disclosure and modification.

Result: Not Assessed

Control Title: MA-01 -System Maintenance Policy And Procedures

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:
1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
b. Reviews and updates the current:
1. System maintenance policy [%Assignment: organization-defined frequency (b)(1)%]; and
2. System maintenance procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: HUD IT security policy (inclusive of system maintenance) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. System maintenance compliance policy is specifically addressed in Section 4.6.5 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 4.5 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 contains the policy for Maintenance. Section 4.6.5

Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 1, 2013. The HUD Handbook 2400.25 contains a formal documented system maintenance policy within Section 4.5. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to system maintenance.
The system maintenance policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The system maintenance procedures to facilitate the implementation of the system maintenance policy and associated system maintenance security controls are documented within the Section 4.5 of the Information Technology Security Procedures, dated November 1, 2013.
The system maintenance procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: MA-1 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Maintenance policy and procedures
* Other relevant documents or records

Interview

* Organizational personnel with maintenance responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: MA-01 (a)(01)[01] - The organization develops and documents a system maintenance policy that addresses:

* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: MA-01 (a)(01)[02] - The organization defines personnel or roles to whom the system maintenance policy is to be disseminated.

Result: Not Assessed

Determine If Statement: MA-01 (a)(01)[03] - The organization disseminates the system maintenance policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: MA-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the maintenance policy and associated system maintenance controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: MA-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Not Assessed

Determine If Statement: MA-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: MA-01 (b)(01)[01] - The organization defines the frequency to review and update the current system maintenance policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: MA-01 (b)(01)[02] - The organization reviews and updates the current system maintenance policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: MA-01 (b)(02)[01] - The organization defines the frequency to review and update the current system maintenance procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: MA-01 (b)(02)[02] - The organization reviews and updates the current system maintenance procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: MA-02 -Controlled Maintenance

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
c. Requires that [%Assignment: organization-defined personnel or roles%] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
f. Includes [%Assignment: organization-defined maintenance-related information%] in organizational maintenance records.

Implementation Statement: Controlled Maintenance: The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
This is a common control, the implementation of which is the responsibility of HITS Contractors & System Owners of Major Applications.

Implementation Statement for **P207 - Mainframe (IBM)**
All maintenance/repair is strictly controlled, documented and scheduled through the Configuration/Change Management Program via Service Desk. All contractor maintenance/repair personnel are escorted during maintenance/repair activities. While there is no schedule routine maintenance, all severs are updated as patches are released and successfully tested. All mainframe maintenance is performed on-site. Following maintenance or repair actions all potentially impacted security controls are checked to verify that the controls are still functioning properly.

Assessment Objective: MA-2 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Information system maintenance policy
* Procedures addressing controlled information system maintenance
* Maintenance records
* Manufacturer/vendor maintenance specifications
* Equipment sanitization records
* Media sanitization records
* Other relevant documents or records

Interview

* Organizational personnel with information system maintenance responsibilities
* Organizational personnel with information security responsibilities
* Organizational personnel responsible for media sanitization
* System/network administrators

Test

* Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for the information system
* Organizational processes for sanitizing information system components
* Automated mechanisms supporting and/or implementing controlled maintenance
* Automated mechanisms implementing sanitization of information system components

Determine If Statement: MA-02 (a)[01] - The organization schedules maintenance and repairs on information system components in accordance with manufacture or vendor specifications; and/or organization requirements.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: MA-02 (a)[02] - The organization performs maintenance and repairs on information system components in accordance with manufacture or vendor specifications; and/or organization requirements.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: MA-02 (a)[03] - The organization documents maintenance and repairs on information system components in accordance with manufacture or vendor specifications; and/or organization requirements.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: MA-02 (a)[04] - The organization reviews records of maintenance and repairs on information system components in accordance with manufacture or vendor specifications; and/or organization requirements.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: MA-02 (b)[01] - The organization approves all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

Result: Not Assessed

Determine If Statement: MA-02 (b)[02] - The organization monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: MA-02 (c)[01] - The organization defines personnel or roles required to explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: MA-02 (c)[02] - The organization requires that organization-defined personnel or roles explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: MA-02 (d) - The organization sanitizesequipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: MA-02 (e) - The organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: MA-02 (f)[01] - The organization defines maintenance-related information to be included in organizational maintenance records.

Result: Not Assessed

Determine If Statement: MA-02 (f)[02] - The organization includes organization-defined maintenance-related information in organizational maintenance records.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: MA-03 -Maintenance Tools

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization approves, controls, and monitors information system maintenance tools.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**

All maintenance and repair tools are approved/ provided/maintained by the data center. External maintenance/repair tools are allowed into the computer room with accompanying contractor maintenance/repair personnel.

Assessment Objective: MA-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Information system maintenance policy
* Procedures addressing information system maintenance tools
* Information system maintenance tools and associated documentation
* Maintenance records
* Other relevant documents or records

Interview

* Organizational personnel with information system maintenance responsibilities
* Organizational personnel with information security responsibilities

Test

* Organizational processes for approving, controlling, and monitoring maintenance tools
* Automated mechanisms supporting and/or implementing approval, control, and/or monitoring of maintenance tools

Determine If Statement: MA-03 [01] - The organization approves information system maintenance tools.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: MA-03 [02] - The organization controls information system maintenance tools.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: MA-03 [03] - The organization monitors information system maintenance tools.
Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: MA-03(1) -Inspect Tools
Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

Assessment Objective: MA-3(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Information system maintenance policy
* Procedures addressing information system maintenance tools
* Information system maintenance tools and associated documentation
* Maintenance tool inspection records
* Maintenance records
* Other relevant documents or records

Interview
* Organizational personnel with information system maintenance responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for inspecting maintenance tools
* Automated mechanisms supporting and/or implementing inspection of maintenance tools

Determine If Statement: MA-03(01) - The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.
Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: MA-03(2) -Inspect Media
Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
All media containing diagnostic and test programs is scanned for malicious code before the media are used in the information system in accordance with HUD policy.

Assessment Objective: MA-3(2) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* Information system maintenance policy
* Procedures addressing information system maintenance tools
* Information system maintenance tools and associated documentation
* Maintenance records
* Other relevant documents or records

Interview
* Organizational personnel with information system maintenance responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational process for inspecting media for malicious code
* Automated mechanisms supporting and/or implementing inspection of media used for maintenance

Determine If Statement: MA-03(02) - The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: MA-04 -Nonlocal Maintenance

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Approves and monitors nonlocal maintenance and diagnostic activities;
b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintains records for nonlocal maintenance and diagnostic activities; and
e. Terminates session and network connections when nonlocal maintenance is completed.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors & System Owners of Major Applications.

Assessment Objective: MA-4 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Information system maintenance policy
* Procedures addressing nonlocal information system maintenance
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* Maintenance records
* Diagnostic records
* Other relevant documents or records

Interview
* Organizational personnel with information system maintenance responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for managing nonlocal maintenance
* Automated mechanisms implementing, supporting, and/or managing nonlocal maintenance
* Automated mechanisms for strong authentication of nonlocal maintenance diagnostic sessions
* Automated mechanisms for terminating nonlocal maintenance sessions and network connections

Determine If Statement: MA-04 (a)[01] - The organization approves nonlocal maintenance and diagnostic activities.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: MA-04 (a)[02] - The organization monitors nonlocal maintenance and diagnostic activities.
Result: Not Assessed

Determine If Statement: MA-04 (b)[01] - The organization allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy.
Result: Not Assessed

Determine If Statement: MA-04 (b)[02] - The organization allows the use of nonlocal maintenance and diagnostic tools only as documented in the security plan for the information system.
Result: Not Assessed

Determine If Statement: MA-04 (c) - The organization employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.
Result: Not Assessed

Determine If Statement: MA-04 (d) - The organization maintains records for nonlocal maintenance and diagnostic activities.

Result: Not Assessed

Determine If Statement: MA-04 (e)[01] - The organization terminates sessions when nonlocal maintenance or diagnostics is completed.
Result: Not Assessed

Determine If Statement: MA-04 (e)[02] - The organization terminates network connections when nonlocal maintenance or diagnostics is completed.
Result: Not Assessed

Control Title: MA-04(2) -Document Nonlocal Maintenance
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

Implementation Statement: The installation and use of non-local maintenance and diagnostic connections is documented in the security plan for the system.

Assessment Objective: MA-4(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Information system maintenance policy
* Procedures addressing non-local information system maintenance
* Security plan
* Maintenance records
* Diagnostic records
* Audit records
* Other relevant documents or records

Interview
* Organizational personnel with information system maintenance responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: MA-04(02) - The organization documents in the security plan for the information system, the:
* policies for the establishment and use of nonlocal maintenance and diagnostic connections; and
* procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

Result: Not Assessed

Control Title: MA-05 -Maintenance Personnel
Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors & System Owners of Major Applications

Assessment Objective: MA-5 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Information system maintenance policy
* Procedures addressing maintenance personnel
* Service provider contracts
* Service-level agreements
* List of authorized personnel
* Maintenance records
* Access control records
* Other relevant documents or records

Interview
* Organizational personnel with information system maintenance responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for authorizing and managing maintenance personnel
* Automated mechanisms supporting and/or implementing authorization of maintenance personnel

Determine If Statement: MA-05 (a)[01] - The organization establishes a process for maintenance personnel authorization.
Result: Not Assessed

Determine If Statement: MA-05 (a)[02] - The organization maintains a list of authorized maintenance organizations or personnel.
Result: Not Assessed

Determine If Statement: MA-05 (b) - The organization ensures that non-escorted personnel performing maintenance on the information system have required access authorizations.
Result: Not Assessed

Determine If Statement: MA-05 (c) - The organization designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
Result: Not Assessed

Control Title: MA-06 -Timely Maintenance
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization obtains maintenance support and/or spare parts for [%Assignment: organization-defined information system components%] within [%Assignment: organization-defined time period%] of failure.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors & System Owners of Major Applications.

Assessment Objective: MA-6 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Information system maintenance policy
* Procedures addressing information system maintenance
* Service provider contracts
* Service-level agreements
* Inventory and availability of spare parts
* Security plan
* Other relevant documents or records

Interview

* Organizational personnel with information system maintenance responsibilities
* Organizational personnel with acquisition responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Organizational processes for ensuring timely maintenance

Determine If Statement: MA-06 [01] - The organization defines information system components for which maintenance support and/or spare parts are to be obtained.

Result: Not Assessed

Determine If Statement: MA-06 [02] - The organization defines the time period within which maintenance support and/or spare parts are to be obtained after a failure.

Result: Not Assessed

Determine If Statement: MA-06 [03] - The organization

* obtains maintenance support for organization-defined information system components within the organization-defined time period of failure; and/or
* obtains spare parts for organization-defined information system components within the organization-defined time period of failure.

Result: Not Assessed

Control Title: MP-01 -Media Protection Policy And Procedures

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:

a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:
   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and

b. Reviews and updates the current:
   1. Media protection policy [%Assignment: organization-defined frequency (b)(1)%]; and
   2. Media protection procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: HUD IT security policy (inclusive of media protection) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Media protection compliance policy is specifically addressed in Section 4.3 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 4.7 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation. This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Implementation Statement for **Develop IT Security Standards and Policy**

HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented media protection policy within Section 4.7. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to media protection. The media protection policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The media protection procedures to facilitate the implementation of the media protection policy and associated media protection security controls are documented within the Section 4.7 of the Information Technology Security Procedures, dated November 1, 2013.
The media protection procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: MP-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Media protection policy and procedures
* Other relevant documents or records

Interview
* Organizational personnel with media protection responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: MP-01 (a)(01)[01] - The organization develops and documents a media protection policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: MP-01 (a)(01)[02] - The organization defines personnel or roles to whom the media protection policy is to be disseminated.

Result: Not Assessed

Determine If Statement: MP-01 (a)(01)[03] - The organization disseminates the media protection policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: MP-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: MP-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Not Assessed

Determine If Statement: MP-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: MP-01 (b)(01)[01] - The organization defines the frequency to review and update the current media protection policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: MP-01 (b)(01)[02] - The organization reviews and updates the current media protection policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: MP-01 (b)(02)[01] - The organization defines the frequency to review and update the current media protection procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: MP-01 (b)(02)[02] - The organization reviews and updates the current media protection procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: MP-02 -Media Access

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization restricts access to [%Assignment: organization-defined types of digital and/or non-digital media%] to [%Assignment: organization-defined personnel or roles%].

Implementation Statement: Implementation Statement for **P210 - Intranet Server**

All users are required to protect access to digital and non-digital media as per HUD policy. Multiple, redundant, layered management, operations and technical security measures are in place to control access to digital and non-digital media. Access to the computer room and console room are controlled by badge readers. Additionally, access to the entire floor is controlled by a badge reader.

Assessment Objective: MP-2 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Information system media protection policy
* Procedures addressing media access restrictions
* Access control policy and procedures
* Physical and environmental protection policy and procedures
* Media storage facilities
* Access control records
* Other relevant documents or records

Interview

* Organizational personnel with information system media protection responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Organizational processes for restricting information media
* Automated mechanisms supporting and/or implementing media access restrictions

Determine If Statement: MP-02 [01] - The organization defines types of digital and/or non-digital media requiring restricted access.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: MP-02 [02] - The organization defines personnel or roles authorized to access organization-defined types of digital and/or non-digital media.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: MP-02 [03] - The organization restricts access to organization-defined types of digital and/or non-digital media to organization-defined personnel or roles.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: MP-03 -Media Marking

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempts [%Assignment: organization-defined types of information system media%] from marking as long as the media remain within [%Assignment: organization-defined controlled areas%].

Implementation Statement: This is a common control implemented by HITS contractor security staff.

Assessment Objective: MP-3 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Information system media protection policy
* Procedures addressing media marking
* Physical and environmental protection policy and procedures
* Security plan
* List of information system media marking security attributes
* Designated controlled areas
* Other relevant documents or records

Interview

* Organizational personnel with information system media protection and marking responsibilities
* Organizational personnel with information security responsibilities

Test

* Organizational processes for marking information media
* Automated mechanisms supporting and/or implementing media marking

Determine If Statement: MP-03 (a)[01] - The organization marks information system media indicating the distribution limitations of the information.

Result: Not Assessed

Determine If Statement: MP-03 (a)[02] - The organization marks information system media indicating the handling caveats of the information.

Result: Not Assessed

Determine If Statement: MP-03 (a)[03] - The organization marks information system media indicating the applicable security markings (if any) of the information.

Result: Not Assessed

Determine If Statement: MP-03 (b)[01] - The organization defines types of information system media to be exempted from marking as long as the media remain in designated controlled areas.

Result: Not Assessed

Determine If Statement: MP-03 (b)[02] - The organization defines controlled areas where organization-defined types of information system media exempt from marking are to be retained.

Result: Not Assessed

Determine If Statement: MP-03 (b)[03] - The organization exempts organization-defined types of information system media from marking as long as the media remain within organization-defined controlled areas.

Result: Not Assessed

Control Title: MP-04 -Media Storage

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Physically controls and securely stores [%Assignment: organization-defined types of digital and/or non-digital media%] within [%Assignment: organization-defined controlled areas%]; and
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors & System Owners of Major Applications.
The organization secures digital and non-digital media within Contractor's locked controlled physical areas; protects information system media by encryption with password until the CD is physically destroyed; maintains on screen confidentiality for PII information by using only sanitized partial information.

Assessment Objective: MP-4 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Information system media protection policy
* Procedures addressing media storage
* Physical and environmental protection policy and procedures
* Access control policy and procedures
* Security plan
* Information system media
* Designated controlled areas
* Other relevant documents or records

Interview

* Organizational personnel with information system media protection and storage responsibilities
* Organizational personnel with information security responsibilities

Test

* Organizational processes for storing information media
* Automated mechanisms supporting and/or implementing secure media storage/media protection

Determine If Statement: MP-04 (a)[01] - The organization defines types of digital and/or non-digital media to be physically controlled and securely stored within designated controlled areas.

Result: Not Assessed

Determine If Statement: MP-04 (a)[02] - The organization defines controlled areas designated to physically control and securely store organization-defined types of digital and/or non-digital media.

Result: Not Assessed

Determine If Statement: MP-04 (a)[03] - The organization physically controls organization-defined types of digital and/or non-digital media within organization-defined controlled areas.

Result: Not Assessed

Determine If Statement: MP-04 (a)[04] - The organization securely stores organization-defined types of digital and/or non-digital media within organization-defined controlled areas.

Result: Not Assessed

Determine If Statement: MP-04 (b) - The organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Result: Not Assessed

Control Title: MP-04(2) -Automated Restricted Access

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**

[None Entered]

Implementation Statement for **P210 - Intranet Server**

[None Entered]

Assessment Objective: MP-4(2) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Information system media protection policy
* Procedures addressing media storage
* Access control policy and procedures
* Physical and environmental protection policy and procedures
* Information system design documentation
* Information system configuration settings and associated documentation
* Media storage facilities
* Access control devices
* Access control records
* Audit records
* Other relevant documents or records

Interview

* Organizational personnel with information system media protection and storage responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Automated mechanisms restricting access to media storage areas
* Automated mechanisms auditing access attempts and access granted to media storage areas

Determine If Statement: MP-04(02) [01] - The organization employs automated mechanisms to restrict access to media storage areas.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: MP-04(02) [01] - The organization employs automated mechanisms to restrict access to media storage areas.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: MP-04(02) [02] - The organization employs automated mechanisms to audit access attempts.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: MP-04(02) [02] - The organization employs automated mechanisms to audit access attempts.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: MP-04(02) [03] - The organization employs automated mechanisms to audit access granted.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: MP-04(02) [03] - The organization employs automated mechanisms to audit access granted.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: MP-05 -Media Transport

Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Protects and controls [%Assignment: organization-defined types of information system media%] during transport outside of controlled areas using [%Assignment: organization-defined security safeguards%];
b. Maintains accountability for information system media during transport outside of controlled areas;
c. Documents activities associated with the transport of information system media; and
d. Restricts the activities associated with the transport of information system media to authorized personnel.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors & System Owners of Major Applications.

Assessment Objective: MP-5 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Information system media protection policy
* Procedures addressing media storage
* Physical and environmental protection policy and procedures
* Access control policy and procedures
* Security plan
* Information system media
* Designated controlled areas
* Other relevant documents or records

Interview
* Organizational personnel with information system media protection and storage responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for storing information media
* Automated mechanisms supporting and/or implementing media storage/media protection

Determine If Statement: MP-05 (a)[01] - The organization defines types of information system media to be protected and controlled during transport outside of controlled areas.
Result: Not Assessed

Determine If Statement: MP-05 (a)[02] - The organization defines security safeguards to protect and control organization-defined information system media during transport outside of controlled areas.
Result: Not Assessed

Determine If Statement: MP-05 (a)[03] - The organization protects and controls organization-defined information system media during transport outside of controlled areas using organization-defined security safeguards.
Result: Not Assessed

Determine If Statement: MP-05 (b) - The organization maintains accountability for information system media during transport outside of controlled areas.
Result: Not Assessed

Determine If Statement: MP-05 (c) - The organization documents activities associated with the transport of information system media.
Result: Not Assessed

Determine If Statement: MP-05 (d) - The organization restricts the activities associated with transport of information system media to authorized personnel.
Result: Not Assessed

Control Title: MP-05(4) -Cryptographic Protection
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Contractors & System Owners of Major Applications.

Assessment Objective: MP-5(4) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Information system media protection policy
* Procedures addressing media transport
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system media transport records
* Audit records
* Other relevant documents or records

Interview
* Organizational personnel with information system media transport responsibilities
* Organizational personnel with information security responsibilities

Test
* Cryptographic mechanisms protecting information on digital media during transportation outside controlled areas

Determine If Statement: MP-05(04) - The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Result: Not Assessed

Control Title: MP-06 -Media Sanitization

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Sanitizes [%Assignment: organization-defined information system media%] prior to disposal, release out of organizational control, or release for reuse using [%Assignment: organization-defined sanitization techniques and procedures%] in accordance with applicable federal and organizational standards and policies; and
b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors & System Owners of Major Applications.

Assessment Objective: MP-6 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Information system media protection policy
* Procedures addressing media sanitization and disposal
* Applicable federal standards and policies addressing media sanitization
* Media sanitization records
* Audit records
* Information system design documentation
* Information system configuration settings and associated documentation
* Other relevant documents or records

Interview
* Organizational personnel with media sanitization responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for media sanitization
* Automated mechanisms supporting and/or implementing media sanitization

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: MP-06 (a)[01] - The organization defines information system media to be sanitized prior to:
* disposal;
* release out of organizational control; or
* release for reuse.

Result: Not Assessed

Determine If Statement: MP-06 (a)[02] - The organization defines sanitization techniques or procedures to be used for sanitizing organization-defined information system media prior to:
* disposal;
* release out of organizational control; or
* release for reuse.

Result: Not Assessed

Determine If Statement: MP-06 (a)[03] - The organization sanitizes organization-defined information system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques or procedures in accordance with applicable federal and organizational standards and policies.

Result: Not Assessed

Determine If Statement: MP-06 (b) - The organization employs sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information.

Result: Not Assessed

Control Title: MP-07 -Media Use

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization [%Selection: restricts; prohibits%] the use of [%Assignment: organization-defined types of information system media%] on [%Assignment: organization-defined information systems or system components%] using [%Assignment: organization-defined security safeguards%].

Implementation Statement: The organization prohibits the use of flash drives or external hard disk drives on HUD equipment. Authorized requests for data may be provided on a password-protected CD to senior staff members responsible for the multifamily program.

Assessment Objective: MP-7 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Information system media protection policy
* System use policy
* Procedures addressing media usage restrictions
* Security plan
* Rules of behavior
* Information system design documentation
* Information system configuration settings and associated documentation
* Audit records
* Other relevant documents or records

Interview
* Organizational personnel with information system media use responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for media use
* Automated mechanisms restricting or prohibiting use of information system media on information systems or system components

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: MP-07 [01] - The organization defines types of information system media to be:
* restricted on information systems or system components; or
* prohibited from use on information systems or system components.

Result: Not Assessed

Determine If Statement: MP-07 [02] - The organization defines information systems or system components on which the use of organization-defined types of information system media is to be one of the following:
* restricted; or
* prohibited.

Result: Not Assessed

Determine If Statement: MP-07 [03] - The organization defines security safeguards to be employed to restrict or prohibit the use of organization-defined types of information system media on organization-defined information systems or system components.

Result: Not Assessed

Determine If Statement: MP-07 [04] - The organization restricts or prohibits the use of organization-defined information system media on organization-defined information systems or system components using organization-defined security safeguards.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Control Title: MP-07(1) -Prohibit Use Without Owner

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Implementation Statement: The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner. The HITS team controls storage devices.

Assessment Objective: MP-7(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Information system media protection policy
* System use policy
* Procedures addressing media usage restrictions
* Security plan
* Rules of behavior
* Information system design documentation
* Information system configuration settings and associated documentation
* Audit records
* Other relevant documents or records

Interview
* Organizational personnel with information system media use responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for media use
* Automated mechanisms prohibiting use of media on information systems or system components

Determine If Statement: MP-07(01) - The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Result: Not Assessed

Control Title: PE-01 -Physical And Environmental Protection Policy And Procedures

Applicability: Fully Inherited **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:
1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
b. Reviews and updates the current:
1. Physical and environmental protection policy [%Assignment: organization-defined frequency (b)(1)%]; and
2. Physical and environmental protection procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 Information Technology Security Policy. The HUD Handbook 2400.25 contains a formal documented physical and environmental protection policy. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, the document contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to physical and environmental protection.
The physical and environmental protection policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The physical and environmental protection procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection security controls are documented within the Information Technology Security Procedures.
The physical and environmental protection procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: PE-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Physical and environmental protection policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with physical and environmental protection responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: PE-01 (a)(01)[01] - The organization develops and documents a physical and environmental protection policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PE-01 (a)(01)[02] - The organization defines personnel or roles to whom the physical and environmental protection policy is to be disseminated.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-01 (a)(01)[03] - The organization disseminates the physical and environmental protection policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PE-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PE-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PE-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PE-01 (b)(01)[01] - The organization defines the frequency to review and update the current physical and environmental protection policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PE-01 (b)(01)[02] - The organization reviews and updates the current physical and environmental protection policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PE-01 (b)(02)[01] - The organization defines the frequency to review and update the current physical and environmental protection procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PE-01 (b)(02)[02] - The organization reviews and updates the current physical and environmental protection procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: PE-02 -Physical Access Authorizations

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
b. Issues authorization credentials for facility access;
c. Reviews the access list detailing authorized facility access by individuals [%Assignment: organization-defined frequency%]; and
d. Removes individuals from the facility access list when access is no longer required.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Office of Security and Emergency Planning (OSEP) & HITS Contractors.

Implementation Statement for **P207 - Mainframe (IBM)**

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

The HPES Data Center is located in a open campus that is maintained by the State of West Virginia Higher Education Commission *HEPC) except for the 9 acres where the HPES Data Center is located which is owned and maintained by Alpha Technologies. The City of South Charleston maintains the main road thru the Tech Park. The City of South Charleston's Police and Fire departments respond to any alarms in the Tech Park. Every street was given a name and every building was given a street number for emergencies. Because of the government contract housed in Building 6000, HP hired Security Guards from Securitas for 24 X 7 X 365 coverage. They monitor the cameras and make rounds through the building and report any issues to the Facilities Manager.
Visitors enter into the facility lobby during normal work hours. Once inside the facility lobby, the visitor must be signed in and escorted by appropriate personnel at all times. If requested, required and authorized, the visitor may, once inside the facility, be given an access badge by the Facility Manager that provides access to common areas within the facility, such as the break room, bathrooms, the elevators, and the second floor hallway. At the end of the day, the facility visitor badge is retrieved from the visitor. All visitors are escorted when in sensitive areas. Once inside the facility, a card reader is present for authorized employees. All authorized employees have access badges with photo IDs. Entry into the computer room requires both an access badge, biometric hand geometry reader and corresponding PIN to enter.
Access badge control policies exist (reference HP HUD HITS Request for Employee Access Badge for B6000 V1.2) and are audited periodically (at least annually by the HP Data Center QMS Project Leader) or as required by changes to access needs. Access badges are controlled by HP Security which provides all physical security services for the facility. The Facility Manager requests the appropriate badge access for staff. New employees will have an ID photo taken and a badge created in accordance with physical access procedures. Badge access to certain parts of the facility is determined by the job role assigned to the individual. The Facility Manager determines the job role access level and provides HP Security with the proper badge form that identifies physical access requirements for setup within the Galaxy System. HP Security issues physical access credentials based on forms (with selected job roles determining access requirements) required as part of the badge request process. Reference Hire-In SLIP Badge Request Form (R-HTS-FAC-006 V1.0), Request for B6000 Access Badge (F-HTS-FAC-002 V1.2), Background and Drug Screen Verification Form (F-HTS-DCA-001), and Background Screen verification Form (R-HTS-FAC-007 V1.0). The Facility Manager maintains, reviews and approves the facility access list quarterly and removes access (per Removal\Termination form submitted to HP Security) when no longer required.
The Facility Manager maintains a list of all personnel and their physical access requirements/authorizations. This list is reviewed quarterly by the Facility Manager to verify and/or make access adjustments as needed i.e., leaving employment, termination, job transfer, new hire, etc. when required.
Access throughout the building is provided by access badges that are controlled by the Facility Manager in conjunction with HP Security which controls the building Galaxy System and provides badges/access as required/requested by the Facility Manager.
Implementation Statement for **P210 - Intranet Server**
The HPES Data Center is located in a open campus that is maintained by the State of West Virginia Higher Education Commission *HEPC) except for the 9 acres where the HPES Data Center is located which is owned and maintained by Alpha Technologies. The City of South Charleston maintains the main road thru the Tech Park. The City of South Charleston's Police and Fire departments respond to any alarms in the Tech Park. Every street was given a name and every building was given a street number for emergencies. Because of the government contract housed in Building 6000, HP hired Security Guards from Securitas for 24 X 7 X 365 coverage. They monitor the cameras and make rounds through the building and report any issues to the Facilities Manager.
Visitors enter into the facility lobby during normal work hours. Once inside the facility lobby, the visitor must be signed in and escorted by appropriate personnel at all times. If requested, required and authorized, the visitor may, once inside the facility, be given an access badge by the Facility Manager that provides access to common areas within the facility, such as the break room, bathrooms, the elevators, and the second floor hallway. At the end of the day, the facility visitor badge is retrieved from the visitor. All visitors are escorted when in sensitive areas. Once inside the facility, a card reader is present for authorized employees. All authorized employees have access badges with photo IDs. Entry into the computer room requires both an access badge, biometric hand geometry reader and corresponding PIN to enter. The visitor campus badge is retrieved by the gate guard from the visitor upon exit from the upper campus. Access badge control policies exist (reference HP HUD HITS Request for Employee Access Badge for B6000 V1.2) and are audited periodically (at least annually by the HP Data Center QMS Project Leader) or as required by changes to access HPES. Access badges are controlled by Dow Security which provides all physical security services for the technology park campus and the facility. The Facility Manager requests the appropriate badge access for staff. New employees are escorted by the Facility Manager to a

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Dow building at the Tech Center to have an ID photo taken and a badge created in accordance with physical access procedures. Badge access to certain parts of the facility is determined by the job role assigned to the individual. The Facility Manager determines the job role access level and provides Dow Security with the proper badge form that identifies physical access requirements for setup within the Honeywell PACS. Dow Security issues physical access credentials based on forms (with selected job roles determining access requirements) required as part of the badge request process. Reference Hire-In SLIP Badge Request Form (R-HTS-FAC-006 V1.0), Request for B6000 Access Badge (F-HTS-FAC-002 V1.2), Background and Drug Screen Verification Form (F-HTS-DCA-001), and Background Screen verification Form (R-HTS-FAC-007 V1.0). The Facility Manager maintains, reviews and approves the facility access list quarterly and removes access (per Removal\Termination form submitted to Dow Security) when no longer required. The Facility Manager maintains a list of all personnel and their physical access requirements/authorizations. This list is reviewed quarterly by the Facility Manager to verify and/or make access adjustments as needed i.e., leaving employment, termination, job transfer, new hire, etc. when required. Access badges and biometric hand scanning with PIN is necessary to access the computer room. However, once inside the computer room, individuals have unimpeded access to the tape room as there is no badge reader or lock on the door. Access to the tape room is not monitored, recorded or reviewed. Placing the tape room within the secure computer room acts as a compensating control as only a limited number of personnel (Operations staff, System administrators, and Network Team) have access to that area. Access throughout the building is provided by access badges that are controlled by the Facility Manager in conjunction with Dow Security which controls the building PACS and provides badges/access as required/requested by the Facility Manager. Access badges do not require an entry code. Entry code is only used with the geometric hand scanner to enter the computer room. This number is tied to an individual and does not change.

Assessment Objective: PE-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Physical and environmental protection policy
* Procedures addressing physical access authorizations
* Security plan
* Authorized personnel access list
* Authorization credentials
* Physical access list reviews
* Physical access termination records and associated documentation
* Other relevant documents or records

Interview
* Organizational personnel with physical access authorization responsibilities
* Organizational personnel with physical access to information system facility
* Organizational personnel with information security responsibilities

Test
* Organizational processes for physical access authorizations
* Automated mechanisms supporting and/or implementing physical access authorizations

Determine If Statement: PE-02 (a)[01] - The organization develops a list of individuals with authorized access to the facility where the information system resides.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-02 (a)[01] - The organization develops a list of individuals with authorized access to the facility where the information system resides.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-02 (a)[02] - The organization approves a list of individuals with authorized access to the facility where the information system resides.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-02 (a)[03] - The organization maintains a list of individuals with authorized access to the facility where the information system resides.

Result: Not Assessed

Determine If Statement: PE-02 (b) - The organization issues authorization credentials for facility access.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-02 (b) - The organization issues authorization credentials for facility access.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-02 (c)[01] - The organization defines the frequency to review the access list detailing authorized facility access by individuals.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-02 (c)[01] - The organization defines the frequency to review the access list detailing authorized facility access by individuals.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-02 (c)[02] - The organization reviews the access list detailing authorized facility access by individuals with the organization-defined frequency.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-02 (c)[02] - The organization reviews the access list detailing authorized facility access by individuals with the organization-defined frequency.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-02 (d) - The organization removes individuals from the facility access list when access is no longer required.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-02 (d) - The organization removes individuals from the facility access list when access is no longer required.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-03 -Physical Access Control

Applicability: Hybrid **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Enforces physical access authorizations at [%Assignment: organization-defined entry/exit points to the facility where the information system resides%] by;
1. Verifying individual access authorizations before granting access to the facility; and
2. Controlling ingress/egress to the facility using [%Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards%];
b. Maintains physical access audit logs for [%Assignment: organization-defined entry/exit points%];
c. Provides [%Assignment: organization-defined security safeguards%] to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity [%Assignment: organization-defined circumstances requiring visitor escorts and monitoring%];
e. Secures keys, combinations, and other physical access devices;
f. Inventories [%Assignment: organization-defined physical access devices%] every [%Assignment: organization-defined frequency (f)%]; and
g. Changes combinations and keys [%Assignment: organization-defined frequency (g)%] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Office of Security and Emergency Planning (OSEP) & HITS Contractors.

Implementation Statement for **P207 - Mainframe (IBM)**
All doors to the HPES Data Center have a card reader. The facility has CCTV cameras on all doors The HPES Data Center is located in a open campus that is maintained by the State of West Virginia Higher Education Commission *HEPC) except for the 9 acres where the HPES Data Center is located which is owned and maintained by Alpha Technology. The City of South Charleston maintains the main road thru the Tech Park. The City of South Charleston's Police and Fire departments respond to any alarms in the Tech Park. Every street was given a name and every building was given a street number for emergencies. Because of the government contract housed in Building 6000, HP hired Security Guards from Securitas for 24 X 7 X 365 coverage. They monitor the cameras and make rounds through the building and report any issues to the Facilities Manager. Visitors enter into the facility lobby during normal work hours. Once inside the facility lobby, the visitor must be signed in and escorted by appropriate personnel at all times. If requested, required and authorized, the visitor may, once inside the facility, be given an access badge by the Facility Manager that provides access to common areas within the facility, such as the break room, bathrooms, the elevators, and the second floor hallway. At the end of the day, the facility visitor badge is retrieved from the visitor. All visitors are escorted when in sensitive areas. Once inside the facility, a card reader is present for authorized employees. All authorized employees have access badges with photo IDs. Access badges are required for all entrances into the building. Additionally, an access badge is required to go beyond the lobby area at any time (and to get into the lobby area itself during non-business hours) and again prior to entering the office areas on the 2nd floor. From the 2nd floor elevator/stairs, one must badge in/out through a door or turnstile to gain access to the second floor offices. The Galaxy badge readers verify individual access to the facility. Badge readers are present on all facility entrances. There is no public accessible area. The Facility Manager secures office keys and other physical access devices and changes keys or terminates badge access when individuals are transferred or terminated. Access throughout the building is provided by access badges that are controlled by the Facility Manager in conjunction with Securitas Security which controls the building Galaxy and provides badges/access as required/requested by the Facility Manager. Emergency exit and re-entry procedures permit only authorized individuals to enter the building. After a fire drill, all doors are locked. Emergency exit doors to the facility are handle-less to prevent re-entry. Re-entry must occur through the main lobby. All staff must swipe their access badge as they re-enter the building. Any visitors, contractors or maintenance personnel must continue to be escorted while in the building. No openings other than doors or windows exists which are over 96 square inches. Other than in the lobby, all exterior doors are metal, metal/wood combination, or metal/wood combination with reinforced (metal mesh included) class in the top portion of the door. Access badges do not require an entry code. Personnel are educated on physical security and do not allow piggybacking or entrance of unauthorized individuals. All entry and selected exit points require the swiping of badge access cards at each entry and selected exits. All employees must read the HP Guidelines and Policies for Working in a Critical Environment (R-HTS-FAC-004) which prohibits tailgating (piggybacking). Exterior doors are metal except for building entrance doors to enter the main lobby. The lobby doors are made of non-bulllet-proof glass. Internal doors (within the lobby and throughout the facility) are mostly solid wood or wood/metal with some degree of

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

reinforced glass (metal mesh within the glass) in the top portion. Emergency doors have crash bars on the internal portion and no handles on the external portion to allow entry. They are accessible for access with no obstructions. External hinges on all external doors have been welded. Once out these doors, all personnel must re-enter through lobby doors where authorized personnel swipe their access badge and visitors, contractors and maintenance personnel continue to be escorted. Emergency doors are equipped with emergency bar openers (crash bars) located on the inside of the door. These doors comply with local safety codes. Building exterior doors have external hinges that have been welded closed to prevent removal of hinge pins. The computer room doors located on the second floor interior hallway have peened hinges on the outside that are fully encased/enclosed to prevent removal of hinge pins. Additionally, an alarm will sound if any badged facility door is opened without badge access or is left ajar for 45 seconds or less. Walls in the computer room and sensitive areas are true floor to ceiling concrete construction. Walls in the computer room are true floor to ceiling concrete construction which would reveal any attempt to enter without proper authorization. Ceilings in the computer room and sensitive areas are true floor to ceiling and floor and ceiling concrete construction. CCTV is in use externally and internally in the facility. Monitors are viewed 24X7X365 by HP Security staff. Activity is recorded to hard drive and maintained for at least 90 days. A Securitas security guard performs a walk-around outside the facility. This guard visually inspects the exterior of the facility and the surrounding area every 2 hours. Building access is managed and monitored. Securitas Security at the main security office monitors the Galaxy System which controls access to the facility and areas inside the building. The system is monitored by HP hired guards from Securitas 24X7X365. CCTV monitoring equipment (located outside/inside critical points for the facility including building perimeter entrances/exits, the computer room and loading dock area) is monitored in real time by HP Operations staff on site 24X7X365 from inside the command and control center located inside the computer room. Suspicious activity is immediately investigated as appropriate by Securitas security personnel. The Facility Manager is also notified as required. HP Operations staff notify Securitas Security and the Facility Manager of any suspicious activity viewed on the CCTV monitors. Security lighting is present on doors and throughout building, internally and externally. Lighting is also provided in the parking lot and around the perimeter of the facility. Laptops are used by managers and support staff. Help Desk personnel do not use laptops. All laptops contain BitLocker encryption of the hard drive. Users receive security awareness training which includes laptop protection. Unassigned equipment is stored in a locked storage area controlled by the Asset Team. Information system components reside within a secure facility with no general public accessible areas to prevent unauthorized access. An individual must have badge access in order to have access to an area that has system components.

Implementation Statement for **P210 - Intranet Server**

All doors to the HPES Data Center have either a card reader and/or a hand scanner. The facility has CCTV cameras on all doors The HPES Data Center is located in a open campus that is maintained by the State of West Virginia Higher Education Commission *HEPC) except for the 9 acres where the HPES Data Center is located which is owned and maintained by Alpha Technologies. The City of South Charleston maintains the main road thru the Tech Park. The City of South Charleston's Police and Fire departments respond to any alarms in the Tech Park. Every street was given a name and every building was given a street number for emergencies. Because of the government contract housed in Building 6000, HP hired Security Guards from Securitas for 24 X 7 X 365 coverage. They monitor the cameras and make rounds through the building and report any issues to the Facilities Manager.

Visitors enter into the facility lobby during normal work hours. Once inside the facility lobby, the visitor must be signed in and escorted by appropriate personnel at all times. If requested, required and authorized, the visitor may, once inside the facility, be given an access badge by the Facility Manager that provides access to common areas within the facility, such as the break room, bathrooms, the elevators, and the second floor hallway. At the end of the day, the facility visitor badge is retrieved from the visitor. All visitors are escorted when in sensitive areas. Once inside the facility, a card reader is present for authorized employees. All authorized employees have access badges with photo IDs. Entry into the computer room requires both an access badge, biometric hand geometry reader and corresponding PIN to enter. Access badges are required for all entrances into the building. Additionally, an access badge is required to go beyond the lobby area at any time (and to get into the lobby area itself during non-business hours) and again prior to entering the office areas on the 2nd floor. From the 2nd floor elevator/stairs, one must badge in/out through a door or turnstile to gain access to the second floor offices. Further entry into the computer room requires an access badge as well as biometric hand geometry and corresponding PIN. The PACS badge readers verify individual access to the facility. Badge readers are present on all facility entrances. There is no public accessible area. The Facility Manager secures office keys and other physical access devices and changes keys or terminates badge access when individuals are transferred or terminated. Access badges and biometric hand scanning with PIN is necessary to access the computer room. However, once inside the computer room, individuals

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

have unimpeded access to the tape room as there is no badge reader or lock on the door. Access to the tape room is not monitored, recorded or reviewed. Placing the tape room within the secure computer room acts as a compensating control as only a limited number of personnel (Operations staff, System administrators, and Network Team) have access to that area. Access throughout the building is provided by access badges that are controlled by the Facility Manager in conjunction with Securitas Security which controls the building PACS and provides badges/access as required/requested by the Facility Manager. Emergency exit and re-entry procedures permit only authorized individuals to enter the building. After a fire drill, all doors are locked. Emergency exit doors to the facility are handle-less to prevent re-entry. Re-entry must occur through the main lobby. All staff must swipe their access badge as they re-enter the building. Any visitors, contractors or maintenance personnel must continue to be escorted while in the building. No openings other than doors or windows exists which are over 96 square inches. Other than in the lobby, all exterior doors are metal, metal/wood combination, or metal/wood combination with reinforced (metal mesh included) class in the top portion of the door. Access badges do not require an entry code. Entry code is only used with the geometric hand scanner to enter the computer room. This number is tied to an individual and does not change. Personnel are educated on physical security and do not allow piggybacking or entrance of unauthorized individuals. All entry and selected exit points require the swiping of badge access cards at each entry and selected exits. All employees must read and sign the HP Guidelines and Policies for Working in a Critical Environment (R-HTS-FAC-004) which prohibits tailgating (piggybacking). Exterior doors are metal except for building entrance doors to enter the main lobby. The lobby doors are made of non-bulllet-proof glass. Internal doors (within the lobby and throughout the facility) are mostly solid wood or wood/metal with some degree of reinforced glass (metal mesh within the glass) in the top portion. Emergency doors have crash bars on the internal portion and no handles on the external portion to allow entry. They are accessible for access with no obstructions. External hinges on all external doors have been welded. Once out these doors, all personnel must re-enter through lobby doors where authorized personnel swipe their access badge and visitors, contractors and maintenance personnel continue to be escorted. Emergency doors are equipped with emergency bar openers (crash bars) located on the inside of the door. These doors comply with local safety codes. Building exterior doors have external hinges that have been welded closed to prevent removal of hinge pins. The computer room doors located on the second floor interior hallway have peened hinges on the outside that are fully encased/enclosed to prevent removal of hinge pins. Additionally, an alarm will sound if any badged facility door is opened without badge access or is left ajar for 45 seconds or less. Walls in the computer room and sensitive areas are true floor to ceiling concrete construction. Walls in the computer room are true floor to ceiling concrete construction which would reveal any attempt to enter without proper authorization. Ceilings in the computer room and sensitive areas are true floor to ceiling and floor and ceiling concrete construction. CCTV is in use externally and internally in the facility. Monitors are viewed 24X7X365 by HP operations staff in the command and control room inside the computer room. Activity is recorded to hard drive and maintained for at least 90 days. A Securitas security guard performs a walk-around outside the facility. This guard visually inspects the exterior of the facility and the surrounding area every 2 hours. Building access is managed and monitored. Securitas Security at the main security office monitors the Honeywell PACS which controls access to the facility and areas inside the building. The system is monitored by HP hired guards from Securitas 24X7X365. CCTV monitoring equipment (located outside/inside critical points for the facility including building perimeter entrances/exits, the computer room and loading dock area) is monitored in real time by HP Operations staff on site 24X7X365 from inside the command and control center located inside the computer room. Suspicious activity is immediately investigated as appropriate by Securitas security personnel. The Facility Manager is also notified as required. HP Operations staff notify Securitas Security and the Facility Manager of any suspicious activity viewed on the CCTV monitors. Securitas Security will instruct the Roving Guard to investigate any suspicious activity and take appropriate action. Security lighting is present on doors and throughout building, internally and externally. Lighting is also provided in the parking lot and around the perimeter of the facility. Laptops are used by managers and support staff. Help Desk personnel do not use laptops. All laptops contain PointSec encryption of the hard drive. Users receive security awareness training which includes laptop protection. Unassigned equipment is stored in a locked storage area controlled by the Asset Team. Information system components reside within a secure facility with no general public accessible areas to prevent unauthorized access. An individual must have badge access in order to have access to an area that has system components.

Assessment Objective: PE-3 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Physical and environmental protection policy
* Procedures addressing physical access control
* Security plan
* Physical access control logs or records
* Inventory records of physical access control devices
* Information system entry and exit points
* Records of key and lock combination changes
* Storage locations for physical access control devices
* Physical access control devices
* List of security safeguards controlling access to designated publicly accessible areas within facility
* Other relevant documents or records

Interview

* Organizational personnel with physical access control responsibilities
* Organizational personnel with information security responsibilities

Test

* Organizational processes for physical access control
* Automated mechanisms supporting and/or implementing physical access control
* Physical access control devices

Determine If Statement: PE-03 (a)[01] - The organization defines entry/exit points to the facility where the information system resides.

Result: Not Assessed

Determine If Statement: PE-03 (a)[02](01) - The organization enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides by verifying individual access authorizations before granting access to the facility.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-03 (a)[02](01) - The organization enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides by verifying individual access authorizations before granting access to the facility.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-03 (a)[02](02)[a] - The organization enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides by defining physical access control systems/devices to be employed to control ingress/egress to the facility where the information system resides.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-03 (a)[02](02)[a] - The organization enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides by defining physical access control systems/devices to be employed to control ingress/egress to the facility where the information system resides.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-03 (a)[02](02)[b] - The organization enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides by using one or more of the following ways to control ingress/egress to the facility:
* organization-defined physical access control systems/devices; and/or
* guards.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-03 (a)[02](02)[b] - The organization enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides by using one or more of the following ways to control ingress/egress to the facility:
* organization-defined physical access control systems/devices; and/or
* guards.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-03 (b)[01] - The organization defines entry/exit points for which physical access audit logs are to be maintained.

Result: Not Assessed

Determine If Statement: PE-03 (b)[02] - The organization maintains physical access audit logs for organization-defined entry/exit points.

Result: Not Assessed

Determine If Statement: PE-03 (c)[01] - The organization defines security safeguards to be employed to control access to areas within the facility officially designated as publicly accessible.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-03 (c)[01] - The organization defines security safeguards to be employed to control access to areas within the facility officially designated as publicly accessible.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-03 (c)[02] - The organization provides organization-defined security safeguards to control access to areas within the facility officially designated as publicly accessible.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-03 (c)[02] - The organization provides organization-defined security safeguards to control access to areas within the facility officially designated as publicly accessible.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-03 (d)[01] - The organization defines circumstances requiring visitor:
* escorts;
* monitoring.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-03 (d)[01] - The organization defines circumstances requiring visitor:
* escorts;
* monitoring.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-03 (d)[02][a] - The organization in accordance with organization-defined circumstances requiring visitor escorts and monitoring escorts visitors.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-03 (d)[02][a] - The organization in accordance with organization-defined circumstances requiring visitor escorts and monitoring escorts visitors.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-03 (d)[02][b] - The organization in accordance with organization-defined circumstances requiring visitor escorts and monitoring monitors visitor activities.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-03 (d)[02][b] - The organization in accordance with organization-defined circumstances requiring visitor escorts and monitoring monitors visitor activities.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-03 (e)[01] - The organization secures keys.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-03 (e)[01] - The organization secures keys.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-03 (e)[02] - The organization secures combinations.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-03 (e)[02] - The organization secures combinations.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-03 (e)[03] - The organization secures other physical access devices.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-03 (e)[03] - The organization secures other physical access devices.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-03 (f)[01] - The organization defines physical access devices to be inventoried.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-03 (f)[02] - The organization defines the frequency to inventory organization-defined physical access devices.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-03 (f)[02] - The organization defines the frequency to inventory organization-defined physical access devices.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-03 (f)[03] - The organization inventories the organization-defined physical access devices with the organization-defined frequency.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-03 (f)[03] - The organization inventories the organization-defined physical access devices with the organization-defined frequency.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-03 (g)[01] - The organization defines the frequency to change combinations and keys.

Result: Not Assessed

Determine If Statement: PE-03 (g)[02][a] - The organization changes combinations and keys with the organization-defined frequency and/or when keys are lost.

Result: Not Assessed

Determine If Statement: PE-03 (g)[02][b] - The organization changes combinations and keys with the organization-defined frequency and/or when combinations are compromised.

Result: Not Assessed

Determine If Statement: PE-03 (g)[02][c] - The organization changes combinations and keys with the organization-defined frequency and/or when individuals are transferred or terminated.

Result: Not Assessed

Control Title: PE-04 -Access Control For Transmission Medium

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization controls physical access to [%Assignment: organization-defined information system distribution and transmission lines%] within organizational facilities using [%Assignment: organization-defined security safeguards%].

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors & System Owners of Major Applications.

Implementation Statement for **P207 - Mainframe (IBM)**
Transmission lines are located in ceilings, floor panels in the computer room and route to a locked communications room. Only limited staff (Network Team and Facility Manager) have access to the communications room.
Implementation Statement for **P210 - Intranet Server**
Transmission lines are located in ceilings, floor panels in the computer room and route to a locked communications room. Only limited staff (Network Team and Facility Manager) have access to the communications room.

Assessment Objective: PE-4 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Physical and environmental protection policy
* Procedures addressing access control for transmission medium
* Information system design documentation
* Facility communications and wiring diagrams
* List of physical security safeguards applied to information system distribution and transmission lines
* Other relevant documents or records

Interview

* Organizational personnel with physical access control responsibilities
* Organizational personnel with information security responsibilities

Test

* Organizational processes for access control to distribution and transmission lines
* Automated mechanisms/security safeguards supporting and/or implementing access control to distribution and transmission lines

Determine If Statement: PE-04 [01] - The organization defines information system distribution and transmission lines requiring physical access controls.

Result: Not Assessed

Determine If Statement: PE-04 [02] - The organization defines security safeguards to be employed to control physical access to organization-defined information system distribution and transmission lines within organizational facilities.

Result: Not Assessed

Determine If Statement: PE-04 [03] - The organization controls physical access to organization-defined information system distribution and transmission lines within organizational facilities using organization-defined security safeguards.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-04 [03] - The organization controls physical access to organization-defined information system distribution and transmission lines within organizational facilities using organization-defined security safeguards.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-05 -Access Control For Output Devices

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Implementation Statement: The organization controls physical access to information system output devices like monitors and printers to prevent unauthorized individuals from obtaining the output. Authorized individuals have access to HUD or to contractor remote location with cards with an ID chip or key cards.

Assessment Objective: PE-5 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:
Examine
* Physical and environmental protection policy
* Procedures addressing access control for display medium
* Facility layout of information system components
* Actual displays from information system components
* Other relevant documents or records

Interview
* Organizational personnel with physical access control responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for access control to output devices
* Automated mechanisms supporting and/or implementing access control to output devices

Determine If Statement: PE-05 - The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Result: Not Assessed

Control Title: PE-05(1) -Access To Output By Authorized Individuals

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization:
(a) Controls physical access to output from [%Assignment: organization-defined output devices%]; and
(b) Ensures that only authorized individuals receive output from the device.

Assessment Objective: PE-5(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Physical and environmental protection policy
* Procedures addressing physical access control
* List of output devices and associated outputs requiring physical access controls
* Physical access control logs or records for areas containing output devices and related outputs
* Other relevant documents or records

Interview
* Organizational personnel with physical access control responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for access control to output devices
* Automated mechanisms supporting and/or implementing access control to output devices

Determine If Statement: PE-05(01) (a)[01] - The organization defines output devices whose output requires physical access controls.

Result: NA-RTM **Assessed by:** **Date:**

Determine If Statement: PE-05(01) (a)[02] - The organization controls physical access to output from organization-defined output devices.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-05(01) (a)[02] - The organization controls physical access to output from organization-defined output devices.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-05(01) (b) - The organization ensures that only authorized individuals receive output from the device.

Result: NA-RTM **Assessed by:** **Date:**

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: PE-06 -Monitoring Physical Access

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Reviews physical access logs [%Assignment: organization-defined frequency%] and upon occurrence of [%Assignment: organization-defined events or potential indications of events%]; and
c. Coordinates results of reviews and investigations with the organizational incident response capability.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Office of Security and Emergency Planning (OSEP) & HITS Contractors.

Implementation Statement for **P207 - Mainframe (IBM)**
The HPES Data Center is staffed 24 x 7. The facility has CCTV camera coverage on all perimeter doors and campus security guards make regular checks of the facility perimeter. The Facility Manager reviews the physical access list periodically (at least quarterly) and removes access as appropriate based upon this review and/or other changes to the needs of personnel for physical access. CCTV monitoring equipment (located outside/inside critical points for the facility including building perimeter entrances/exits, the computer room and loading dock area) are monitored in real time by HP Security staff on site 24X7X365. Building and computer room doors are alarmed and if left ajar/open for longer than 90 seconds or if there are multiple badge access attempt failures, the Galaxy System will issue an alert to HP Security.
HP security personnel are alerted to failed badge attempts etc. through the Galaxy System console located at the HP security office. Access violations are reported and investigated as needed by HP Security and the Facility Manager and appropriate remedial action is taken..
Implementation Statement for **P210 - Intranet Server**
The HPES Data Center is staffed 24 x 7. The facility has CCTV camera coverage on all perimeter doors and campus security guards make regular checks of the facility perimeter. The Facility Manager reviews the physical access list periodically (at least quarterly) and removes access as appropriate based upon this review and/or other changes to the HPES of personnel for physical access. CCTV monitoring equipment (located outside/inside critical points for the facility including building perimeter entrances/exits, the computer room and loading dock area) are monitored in real time by HP Operations staff on site 24X7X365. Building and computer room doors are alarmed and if left ajar/open for longer than 90 seconds or if there are multiple badge access attempt failures, the Honeywell Physical Access Control System (PACS) will issue an alert to Dow Security. Dow Security at the main office and/or the Guard duty hut will contact the Facility Manager and send a roving security guard to investigate. Dow security personnel are alerted to failed badge attempts etc. through the PACS console located at the Dow security office. Access violations are reported and investigated as needed by Dow Security and the Facility Manager and appropriate remedial action is taken.

Assessment Objective: PE-6 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* Physical and environmental protection policy
* Procedures addressing physical access monitoring
* Security plan
* Physical access logs or records
* Physical access monitoring records
* Physical access log reviews
* Other relevant documents or records

Interview
* Organizational personnel with physical access monitoring responsibilities
* Organizational personnel with incident response responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for monitoring physical access
* Automated mechanisms supporting and/or implementing physical access monitoring
* Automated mechanisms supporting and/or implementing reviewing of physical access logs

Determine If Statement: PE-06 (a) - The organization monitors physical access to the facility where the information system resides to detect and respond to physical security incidents.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-06 (a) - The organization monitors physical access to the facility where the information system resides to detect and respond to physical security incidents.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-06 (b)[01] - The organization defines the frequency to review physical access logs.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-06 (b)[01] - The organization defines the frequency to review physical access logs.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-06 (b)[02] - The organization defines events or potential indication of events requiring physical access logs to be reviewed.

Result: Not Assessed

Determine If Statement: PE-06 (b)[03] - The organization reviews physical access logs with the organization-defined frequency and upon occurrence of organization-defined events or potential indications of events.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-06 (b)[03] - The organization reviews physical access logs with the organization-defined frequency and upon occurrence of organization-defined events or potential indications of events.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-06 (c) - The organization coordinates results of reviews and investigations with the organizational incident response capability.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-06 (c) - The organization coordinates results of reviews and investigations with the organizational incident response capability.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-06(1) -Intrusion Alarms / Surveillance Equipment

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization monitors physical intrusion alarms and surveillance equipment.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
The HPES Data Center is staffed 24 x 7. The facility has CCTV camera coverage on all perimeter doors and HP security guards make regular checks of the facility perimeter.
Implementation Statement for **P210 - Intranet Server**
The HPES Data Center is staffed 24 x 7. The facility has CCTV camera c-overage on all perimeter doors and campus security guards make regular checks of the facility perimeter.

Assessment Objective: PE-6(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Physical and environmental protection policy
* Procedures addressing physical access monitoring
* Security plan
* Physical access logs or records
* Physical access monitoring records
* Physical access log reviews
* Other relevant documents or records

Interview
* Organizational personnel with physical access monitoring responsibilities
* Organizational personnel with incident response responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for monitoring physical intrusion alarms and surveillance equipment
* Automated mechanisms supporting and/or implementing physical access monitoring
* Automated mechanisms supporting and/or implementing physical intrusion alarms and surveillance equipment

Determine If Statement: PE-06(01) - The organization monitors physical intrusion alarms and surveillance equipment.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-06(01) - The organization monitors physical intrusion alarms and surveillance equipment.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-08 -Visitor Access Records

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Maintains visitor access records to the facility where the information system resides for [%Assignment: organization-defined time period%]; and
b. Reviews visitor access records [%Assignment: organization-defined frequency%].

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Office of Security and Emergency Planning (OSEP) & HITS Contractors.

Implementation Statement for **P207 - Mainframe (IBM)**
All visitors to the HPES Data Center must sign-in, be issued a temporary badge, and be met by and escorted by an HPES

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

representative. Badge readers maintain an audit log of all accesses and attempted accesses. Security violations are investigated by the HPES facility manager. Visitor logs are maintained at the building lobby entrance and the computer room. The visitor logs identify Date, Time in, Time Out, Visitors Full Name, Company Representing, Purpose of Visit, and Escort Name. For facility entrance, all visitors must sign in at the visitor log in the lobby. All visitors must sign out as well. All visitors are only allowed inside any badged areas if required and escorted. An authorized escort will sign them in and escort them to the appropriate location they need to visit. Some approved visitors are given visitor access badges for common areas within the facility. The Facility Manager determines access and controls the visitor process. The Facility Manager reviews the visitor log books weekly to ensure compliance. In addition, access records of physical entry from facility access points (external/internal) are recorded/maintained by HP Security and are made available for periodic review by the Facility Manager upon request. Visitor logs are retained by the Facility Manager for 3 years. Reference HP Charleston Data Center Security Review Process for B6000 Facilities V1.5 (P-HTS-FAC-007).

Implementation Statement for **P210 - Intranet Server**

All visitors to the HPES Data Center must sign-in, be issued a temporary badge, and be met by and escorted by an HPES representative. Badge readers maintain an audit log of all accesses and attempted accesses. Security violations are investigated by the HPES facility manager. Visitor logs are maintained at the building lobby entrance and the computer room. The visitor logs identify Date, Time in, Time Out, Visitors Full Name, Company Representing, Purpose of Visit, and Escort Name. For facility entrance, all visitors must sign in at the visitor log in the lobby. All visitors must sign out as well. All visitors are only allowed inside any badged areas if required and escorted. An authorized escort will sign them in and escort them to the appropriate location they need to visit. Some approved visitors are given visitor access badges for common areas within the facility. The Facility Manager determines access and controls the visitor process. The Facility Manager reviews the visitor log books weekly to ensure compliance. In addition, access records of physical entry from facility access points (external/internal) are recorded/maintained by Alpha Technologies and are made available for periodic review by the Facility Manager upon request. Visitor logs are retained by the Facility Manager for 3 years. Reference HP Charleston Data Center Security Review Process for B6000 Facilities V1.5 (P-HTS-FAC-007).

Assessment Objective: PE-8 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Physical and environmental protection policy
* Procedures addressing visitor access records
* Security plan
* Visitor access control logs or records
* Visitor access record or log reviews
* Other relevant documents or records

Interview
* Organizational personnel with visitor access records responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for maintaining and reviewing visitor access records
* Automated mechanisms supporting and/or implementing maintenance and review of visitor access records

Determine If Statement: PE-08 (a)[01] - The organization defines the time period to maintain visitor access records to the facility where the information system resides.

Result: Not Assessed

Determine If Statement: PE-08 (a)[02] - The organization maintains visitor access records to the facility where the information system resides for the organization-defined time period.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-08 (a)[02] - The organization maintains visitor access records to the facility where the information system resides for the organization-defined time period.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-08 (b)[01] - The organization defines the frequency to review visitor access records.
Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-08 (b)[01] - The organization defines the frequency to review visitor access records.
Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-08 (b)[02] - The organization reviews visitor access records with the organization-defined frequency.
Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-08 (b)[02] - The organization reviews visitor access records with the organization-defined frequency.
Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-09 -Power Equipment And Cabling
Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization protects power equipment and power cabling for the information system from damage and destruction.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
Only authorized personnel can access the rooms where power supplies and main power cables are located. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Nitro Mechanical periodically review equipment for risk of failure. Emergency Power Off (EPO) buttons are located inside the computer room for safety.
Implementation Statement for **P210 - Intranet Server**
Only authorized personnel can access the rooms where power supplies and main power cables are located. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Carrier periodically review equipment for risk of failure.

Assessment Objective: PE-9 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Physical and environmental protection policy
* Procedures addressing power equipment/cabling protection
* Facilities housing power equipment/cabling
* Other relevant documents or records
Interview
* Organizational personnel with responsibility for protecting power equipment/cabling
* Organizational personnel with information security responsibilities
Test
* Automated mechanisms supporting and/or implementing protection of power equipment/cabling

Determine If Statement: PE-09 - The organization protects power equipment and power cabling for the information system from damage and destruction.
Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-09 - The organization protects power equipment and power cabling for the information system from damage and destruction.
Inherited From: P210 - Intranet Server

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: PE-10 -Emergency Shutoff
Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization:
a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
b. Places emergency shutoff switches or devices in [%Assignment: organization-defined location by information system or system component%] to facilitate safe and easy access for personnel; and
c. Protects emergency power shutoff capability from unauthorized activation.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
Emergency shut-off switches are located throughout the HPES Data Center. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Nitro Mechanical periodically review equipment for risk of failure. Emergency Power Off (EPO) buttons are located inside the computer room for safety.
Implementation Statement for **P210 - Intranet Server**
Emergency shut-off switches are located throughout the HPES Data Center. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Carrier periodically review equipment for risk of failure.

Assessment Objective: PE-10 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Physical and environmental protection policy
* Procedures addressing power source emergency shutoff
* Security plan
* Emergency shutoff controls or switches
* Locations housing emergency shutoff switches and devices
* Security safeguards protecting emergency power shutoff capability from unauthorized activation
* Other relevant documents or records
Interview
* Organizational personnel with responsibility for emergency power shutoff capability (both implementing and using the capability)
* Organizational personnel with information security responsibilities
Test
* Automated mechanisms supporting and/or implementing emergency power shutoff

Determine If Statement: PE-10 (a) - The organization provides the capability of shutting off power to the information system or individual system components in emergency situations.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed

Determine If Statement: PE-10 (a) - The organization provides the capability of shutting off power to the information system or individual system components in emergency situations.
Inherited From: P210 - Intranet Server
Result: Not Assessed

Determine If Statement: PE-10 (b)[01] - The organization defines the location of emergency shutoff switches or devices by information system or system component.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-10 (b)[01] - The organization defines the location of emergency shutoff switches or devices by information system or system component.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-10 (b)[02] - The organization places emergency shutoff switches or devices in the organization-defined location by information system or system component to facilitate safe and easy access for personnel.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-10 (b)[02] - The organization places emergency shutoff switches or devices in the organization-defined location by information system or system component to facilitate safe and easy access for personnel.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-10 (c) - The organization protects emergency power shutoff capability from unauthorized activation.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-10 (c) - The organization protects emergency power shutoff capability from unauthorized activation.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-11 -Emergency Power

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization provides a short-term uninterruptible power supply to facilitate [%Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power%] in the event of a primary power source loss.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
In addition to UPS, the HPES Data Center has redundant diesel generators to allow the Data Center to remain operational during extended power outages. Four UPSs are present and in working condition. The UPSs consist of (2) 300 KVA and (2) 225 KVA units. Maintenance schedule has at least annual inspection. Alpha, as owner of the building, is responsible for maintenance of the 4 Liebert units.
4 Uninterruptible Power Supplies (UPS) act as voltage regulators keeping electrical power within acceptable levels and preventing spikes or drops from damaging equipment.
The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Nitro Mechanical periodically review equipment for risk of failure.
Implementation Statement for **P210 - Intranet Server**
In addition to UPS, the HPES Data Center has redundant diesel generators to allow the Data Center to remain operational during extended power outages. Four UPSs are present and in working condition. The UPSs consist of (2) 300 KVA and (2) 225 KVA units. Maintenance schedule has at least annual inspection. Alpha Technologies, as owner of the building, is responsible for maintenance of the 4 Liebert units. 4 Uninterruptible Power Supplies (UPS) act as voltage regulators keeping electrical power within acceptable levels and preventing spikes or drops from damaging equipment. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Carrier periodically review equipment for risk of failure.

Assessment Objective: PE-11 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Physical and environmental protection policy
* Procedures addressing emergency power
* Uninterruptible power supply
* Uninterruptible power supply documentation
* Uninterruptible power supply test records
* Other relevant documents or records

Interview

* Organizational personnel with responsibility for emergency power and/or planning
* Organizational personnel with information security responsibilities

Test

* Automated mechanisms supporting and/or implementing uninterruptible power supply
* The uninterruptable power supply

Determine If Statement: PE-11 - The organization provides a short-term uninterruptible power supply to facilitate one or more of the following in the event of a primary power source loss:
* an orderly shutdown of the information system; and/or
* transition of the information system to long-term alternate power.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-11 - The organization provides a short-term uninterruptible power supply to facilitate one or more of the following in the event of a primary power source loss:
* an orderly shutdown of the information system; and/or
* transition of the information system to long-term alternate power.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-12 -Emergency Lighting

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**

The HPES Data Center is equipped with emergency lighting in case of power failure. In that event, the building also has backup generators and UPSs systems. Security lighting is present on doors and throughout building, internally and externally. Lighting is also provided in the parking lot and around the perimeter of the facility.

Emergency lighting is a present throughout the facility to illuminate the emergency exit corridors and exit points internally and externally. If the power to the facility is lost the redundant UPS systems will power the emergency lighting system throughout the facility.

The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Nitro Mechanical periodically review equipment for risk of failure.

Implementation Statement for **P210 - Intranet Server**

The HPES Data Center is equipped with emergency lighting in case of power failure. In that event, the building also has backup generators and UPSs systems. Security lighting is present on doors and throughout building, internally and externally. Lighting is also provided in the parking lot and around the perimeter of the facility. Emergency lighting is a present throughout the facility to illuminate the emergency exit corridors and exit points internally and externally. If the power to the facility is lost the redundant UPS systems will power the emergency lighting system throughout the facility. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Carrier periodically review equipment for risk of failure.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Assessment Objective: PE-12 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Physical and environmental protection policy
* Procedures addressing emergency lighting
* Emergency lighting documentation
* Emergency lighting test records
* Emergency exits and evacuation routes
* Other relevant documents or records

Interview
* Organizational personnel with responsibility for emergency lighting and/or planning
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms supporting and/or implementing emergency lighting capability

Determine If Statement: PE-12 [01] - The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-12 [01] - The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-12 [02] - The organization employs and maintains automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-12 [02] - The organization employs and maintains automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-13 -Fire Protection

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**

The HPES Data Center is equipped with fire sprinkler systems throughout the facility that are activated in the event of a fire. Hand held fire extinguishers are present throughout the building and are maintained and inspected as required. Hand held fire extinguishers have up-to-date inspection information and are periodically checked by the Facility Manager. Fire suppression is present in the Data Center in the form of dry pipe/halon and hand held fire extinguishers. The facility fire suppression/prevention system (Simplex 4120 Fire Alarm Control System) is completely automated and alerts HP security personnel who immediately contact the South Charleston Fire Department. The Data Center does not contain any wet pipe fire suppression systems. The fire prevention/suppression system is serviced/tested regularly but at least annually. Smoke detectors are located throughout the building (1st and 2nd floor) and tested annually. The entire building has a dry pipe system. Additionally, the computer room has an AFP Notifier system for Halon. Heat and smoke sensors are present and in working condition. The sensors are maintained/serviced at least annually. The Facility Manager conducts physical inspections of the facility periodically and verifies proper storage of materials, device functionality and that potential fire hazards are not in place. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Nitro Mechanical

periodically review equipment for risk of failure.

Implementation Statement for **P210 - Intranet Server**

The HPES Data Center is equipped with fire sprinkler systems throughout the facility that are activated in the event of a fire. Hand held fire extinguishers are present throughout the building and are maintained and inspected as required. Hand held fire extinguishers have up-to-date inspection information and are periodically checked by the Facility Manager. Fire suppression is present in the Data Center in the form of dry pipe/halon and hand held fire extinguishers. The facility fire suppression/prevention system (Simplex 4120 Fire Alarm Control System) is completely automated and alerts Dow security personnel who immediately contact the South Charleston Fire Department. The Data Center does not contain any wet pipe fire suppression systems. The fire prevention/suppression system is serviced/tested regularly but at least annually. Smoke detectors are located throughout the building (1st and 2nd floor) and tested annually. The entire building has a dry pipe system. Additionally, the computer room has an AFP Notifier system for Halon. Heat and smoke sensors are present and in working condition. The sensors are maintained/serviced at least annually. The Facility Manager conducts physical inspections of the facility periodically and verifies proper storage of materials, device functionality and that potential fire hazards are not in place. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP Carrier periodically review equipment for risk of failure.

Assessment Objective: PE-13 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Physical and environmental protection policy
* Procedures addressing fire protection
* Fire suppression and detection devices/systems
* Fire suppression and detection devices/systems documentation
* Test records of fire suppression and detection devices/systems
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for fire detection and suppression devices/systems
* Organizational personnel with information security responsibilities

Test

* Automated mechanisms supporting and/or implementing fire suppression/detection devices/systems

Determine If Statement: PE-13 [01] - The organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-13 [01] - The organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-13 [02] - The organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-13 [02] - The organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-13(1) -Detection Devices / Systems

Applicability: Fully Inherited **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization employs fire detection devices/systems for the information system that activate automatically and notify [%Assignment: organization-defined personnel or roles%] and [%Assignment: organization-defined emergency responders%] in the event of a fire.

Assessment Objective: PE-13(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Physical and environmental protection policy
* Procedures addressing fire protection
* Facility housing the information system
* Alarm service-level agreements
* Test records of fire suppression and detection devices/systems
* Fire suppression and detection devices/systems documentation
* Alerts/notifications of fire events
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for fire detection and suppression devices/systems
* Organizational personnel with responsibilities for notifying appropriate personnel, roles, and emergency responders of fires
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms supporting and/or implementing fire detection devices/systems
* Activation of fire detection devices/systems (simulated)
* Automated notifications

Determine If Statement: PE-13(01) [01] - The organization defines personnel or roles to be notified in the event of a fire.

Result: NA-RTM **Assessed by:** **Date:**

Determine If Statement: PE-13(01) [02] - The organization defines emergency responders to be notified in the event of a fire.

Result: NA-RTM **Assessed by:** **Date:**

Determine If Statement: PE-13(01) [03][a] - The organization employs fire detection devices/systems for the information system that, in the event of a fire, activate automatically.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-13(01) [03][a] - The organization employs fire detection devices/systems for the information system that, in the event of a fire, activate automatically.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-13(01) [03][b] - The organization employs fire detection devices/systems for the information system that, in the event of a fire, notify organization-defined personnel or roles.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-13(01) [03][b] - The organization employs fire detection devices/systems for the information system that, in the event of a fire, notify organization-defined personnel or roles.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-13(01) [03][c] - The organization employs fire detection devices/systems for the information system that, in the event of a fire, notify organization-defined emergency responders.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-13(01) [03][c] - The organization employs fire detection devices/systems for the information system that, in the event of a fire, notify organization-defined emergency responders.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-13(2) -Suppression Devices / Systems

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to [%Assignment: organization-defined personnel or roles%] and [%Assignment: organization-defined emergency responders%].

Assessment Objective: PE-13(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Physical and environmental protection policy
* Procedures addressing fire protection
* Fire suppression and detection devices/systems documentation
* Facility housing the information system
* Alarm service-level agreements
* Test records of fire suppression and detection devices/systems
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for fire detection and suppression devices/systems
* Organizational personnel with responsibilities for providing automatic notifications of any activation of fire suppression devices/systems to appropriate personnel, roles, and emergency responders
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms supporting and/or implementing fire suppression devices/systems
* Activation of fire suppression devices/systems (simulated)
* Automated notifications

Determine If Statement: PE-13(02) [01] - The organization defines personnel or roles to be provided automatic notification of any activation of fire suppression devices/systems for the information system.

Result: NA-RTM **Assessed by:** **Date:**

Determine If Statement: PE-13(02) [02] - The organization defines emergency responders to be provided automatic notification of any activation of fire suppression devices/systems for the information system.

Result: NA-RTM **Assessed by:** **Date:**

Determine If Statement: PE-13(02) [03][a] - The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to organization-defined personnel or roles.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-13(02) [03][a] - The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to organization-defined personnel or roles.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-13(02) [03][b] - The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to organization-defined emergency responders.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-13(02) [03][b] - The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to organization-defined emergency responders.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-13(3) -Automatic Fire Suppression

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
The HPES Data Center is staffed 24 x 7. The HPES Data Center is equipped with fire sprinkler systems throughout the facility. Automatic fire suppression systems are in place (dry pipe and halon) for the facility. Hand held fire extinguishers are installed and maintained.
Implementation Statement for **P210 - Intranet Server**
The HPES Data Center is staffed 24 x 7. The HPES Data Center is equipped with fire sprinkler systems throughout the facility. Automatic fire suppression systems are in place (dry pipe and halon) for the facility. Hand held fire extinguishers are installed and maintained.

Assessment Objective: PE-13(3) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Physical and environmental protection policy
* Procedures addressing fire protection
* Fire suppression and detection devices/systems documentation
* Facility housing the information system
* Alarm service-level agreements
* Test records of fire suppression and detection devices/systems
* Other relevant documents or records

Interview
* Organizational personnel with responsibilities for fire detection and suppression devices/systems
* Organizational personnel with responsibilities for providing automatic notifications of any activation of fire suppression devices/systems to appropriate personnel, roles, and emergency responders
* Organizational personnel with information security responsibilities

Test
* Automated mechanisms supporting and/or implementing fire suppression devices/systems
* Activation of fire suppression devices/systems (simulated)

Determine If Statement: PE-13(03) - The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-13(03) - The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-14 -Temperature And Humidity Controls

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Maintains temperature and humidity levels within the facility where the information system resides at [%Assignment: organization-defined acceptable levels%]; and
b. Monitors temperature and humidity levels [%Assignment: organization-defined frequency%].

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Office of Security and Emergency Planning (OSEP) & HITS Contractors.

Implementation Statement for **P207 - Mainframe (IBM)**

The facility has three 300 ton Carrier chiller units to provide HVAC. Two chiller units run with one as backup. The system is present, working and maintained/serviced at least annually by Nitro Mechanical through a maintenance contract in place. Temperature and humidity controls are strategically located throughout the computer room.

There are 13 Liebert air handlers present within the computer room with humidity controls. Back-up air conditioning is present and in working condition. Two chiller units run with one as backup. The facility also has 3 redundant cooling towers. Functions are tested/serviced at least annually. Twenty-four hour temperature monitoring is present and working and tested/serviced at least annually. Temperature controls are strategically located throughout the computer room.

WVRTP checks temperature and humidity control units located inside the mechanical room every 6 hours for malfunction,., temperatures are logged. T

he Data Center is located where the risk from natural disasters: tornadoes, hurricanes, earthquakes, floods, etc is low to negligible. Although there is a river by the city, the Data Center is located on a hill well above the flood plain. Humidifiers located in the mechanical room feed the Liebert air handlers in the building and computer roomand control moisture levels. HP security personnel, HP Operations staff, and the Facility Manager have contact information for vendors responsible for servicing environmental control equipment. HP Operations staff or the Facility Manager contact HP security personnel or the vendor directly in the event of environmental control problems. Alpha is responsible for maintaining environmental controls for the facility.

The Facility Manager routinely checks environmental control equipment in the Mechanical Room and computer room to ensure they are functioning properly. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Nitro Mechanical periodically review equipment for risk of failure.

Implementation Statement for **P210 - Intranet Server**

The facility has three 300 ton Carrier chiller units to provide HVAC. Two chiller units run with one as backup. The system is present, working and maintained/serviced at least annually by Carrier through a maintenance contract in place. Temperature and humidity controls are strategically located throughout the computer room. There are 13 Liebert air handlers present within the computer room with humidity controls. Back-up air conditioning is present and in working condition. Two chiller units run with one as backup. The facility also has 3 redundant cooling towers. Functions are tested/serviced at least annually. Twenty-four hour temperature monitoring is present and working and tested/serviced at least annually. Temperature controls are strategically located throughout the computer room. WVRTP checks temperature and humidity control units located inside the mechanical room every 6 hours for malfunction. Temperatures are logged. The Data Center is located where the risk from natural disasters: tornadoes, hurricanes, earthquakes, floods, etc is low to negligible. Although there is a river by the city, the Data Center is located on a hill well above the flood plain. Humidifiers located in the mechanical room feed the Liebert air handlers in the building and computer room and control moisture levels. Dow security personnel, HP Operations staff, and the Facility Manager have contact information for vendors responsible for servicing environmental control equipment. HP Operations staff or the Facility Manager contact Dow security personnel or the vendor directly in the event of environmental control problems. Alpha Technologies is responsible for maintaining environmental controls for the facility. The Facility Manager routinely checks environmental control equipment in the Mechanical Room and computer room to ensure they are functioning properly. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Carrier periodically review equipment for risk of failure.

Assessment Objective: PE-14 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Physical and environmental protection policy
* Procedures addressing temperature and humidity control
* Security plan
* Temperature and humidity controls
* Facility housing the information system
* Temperature and humidity controls documentation
* Temperature and humidity records
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for information system environmental controls
* Organizational personnel with information security responsibilities

Test

* Automated mechanisms supporting and/or implementing maintenance and monitoring of temperature and humidity levels

Determine If Statement: PE-14 (a)[01] - The organization defines acceptable temperature levels to be maintained within the facility where the information system resides.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-14 (a)[01] - The organization defines acceptable temperature levels to be maintained within the facility where the information system resides.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-14 (a)[02] - The organization defines acceptable humidity levels to be maintained within the facility where the information system resides.

Result: Not Assessed

Determine If Statement: PE-14 (a)[03] - The organization maintains temperature levels within the facility where the information system resides at the organization-defined levels.

Result: Not Assessed

Determine If Statement: PE-14 (a)[04] - The organization maintains humidity levels within the facility where the information system resides at the organization-defined levels.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-14 (a)[04] - The organization maintains humidity levels within the facility where the information system resides at the organization-defined levels.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-14 (b)[01] - The organization defines the frequency to monitor temperature levels.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-14 (b)[01] - The organization defines the frequency to monitor temperature levels.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-14 (b)[02] - The organization defines the frequency to monitor humidity levels.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-14 (b)[02] - The organization defines the frequency to monitor humidity levels.
Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-14 (b)[03] - The organization monitors temperature levels with the organization-defined frequency.
Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-14 (b)[03] - The organization monitors temperature levels with the organization-defined frequency.
Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-14 (b)[04] - The organization monitors humidity levels with the organization-defined frequency.
Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-14 (b)[04] - The organization monitors humidity levels with the organization-defined frequency.
Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-15 -Water Damage Protection
Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
Water lines are located beneath the computer room floor. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Carrier periodically review equipment for risk of failure. Emergency Power Off (EPO) buttons are located inside the computer room for safety.
Water detection sensors are located under the raised floor of the computer room which will alert data center personnel of any water in that area so that appropriate shutoff valves/master shutoff valves can be activated. Water shutoff valves are located on the 1st and 2nd floor. The water master shutoff valve for the building is located in the 1st floor Mechanical Room. Within the 2nd floor computer room, the water shutoff valve location is under the raised computer room floor and has been marked on the floor tile above it for easy identification. The Facility Manager and HP Operations staff have been trained on the location of the shutoff valve.
Implementation Statement for **P210 - Intranet Server**
Water lines are located beneath the computer room floor. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Carrier periodically review equipment for risk of failure. Water detection sensors are located under the raised floor of the computer room which will alert data center personnel of any water in that area so that appropriate shutoff valves/master shutoff valves can be activated. Water shutoff valves are located on the 1st and 2nd floor. The water master shutoff valve for the building is located in the 1st floor Mechanical Room. Within the 2nd floor computer room, the water shutoff valve location is under the raised computer room floor and has been marked on the floor tile above it for easy identification. The Facility Manager and HP Operations staff have been trained on the location of the shutoff valve.

Assessment Objective: PE-15 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Physical and environmental protection policy
* Procedures addressing water damage protection
* Facility housing the information system
* Master shutoff valves
* List of key personnel with knowledge of location and activation procedures for master shutoff valves for the plumbing system
* Master shutoff valve documentation
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for information system environmental controls
* Organizational personnel with information security responsibilities

Test

* Master water-shutoff valves
* Organizational process for activating master water-shutoff

Determine If Statement: PE-15 [01] - The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-15 [01] - The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-15 [02] - The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are working properly.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-15 [02] - The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are working properly.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-15 [03] - The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are known to key personnel.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-15 [03] - The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are known to key personnel.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-16 -Delivery And Removal

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization authorizes, monitors, and controls [%Assignment: organization-defined types of information system components%] entering and exiting the facility and maintains records of those items.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**

HPES Data Center procedures detail how all data materials are received by, sent from, and managed within the Data Center. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

as environmental controls located in the Mechanical Room. WVRTP & Nitro Mechanical periodically review equipment for risk of failure.
Emergency Power Off (EPO) buttons are located inside the computer room for safety. As part of the configuration/change management program, all information system components entering and leaving the data center are documented in CA Service Desk in order to keep a current, accurate baseline of the information system. Additionally, they are logged in by HP support staff. Reference HP B6000 Incoming Material Package Log (F-HTS-FAC-011 V1.1) 95301
Implementation Statement for **P210 - Intranet Server**
HPES Data Center procedures detail how all data materials are received by, sent from, and managed within the Data Center. The Facility Manager periodically reviews/tests/inspects critical facility safety and security functions and processes as well as environmental controls located in the Mechanical Room. WVRTP and Carrier periodically review equipment for risk of failure. As part of the configuration/change management program, all information system components entering and leaving the data center are documented in CA Service Desk in order to keep a current, accurate baseline of the information system. Additionally, they are logged in by HP support staff. Reference HP B6000 Incoming Material Package Log (F-HTS-FAC-011 V1.1).

Assessment Objective: PE-16 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Physical and environmental protection policy
* Procedures addressing delivery and removal of information system components from the facility
* Security plan
* Facility housing the information system
* Records of items entering and exiting the facility
* Other relevant documents or records
Interview
* Organizational personnel with responsibilities for controlling information system components entering and exiting the facility
* Organizational personnel with information security responsibilities
Test
* Organizational process for authorizing, monitoring, and controlling information system-related items entering and exiting the facility
* Automated mechanisms supporting and/or implementing authorizing, monitoring, and controlling information system-related items entering and exiting the facility

Determine If Statement: PE-16 [01] - The organization defines types of information system components to be authorized, monitored, and controlled as such components are entering and exiting the facility.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-16 [01] - The organization defines types of information system components to be authorized, monitored, and controlled as such components are entering and exiting the facility.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-16 [02] - The organization authorizes organization-defined information system components entering the facility.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-16 [02] - The organization authorizes organization-defined information system components entering the facility.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-16 [03] - The organization monitors organization-defined information system components entering the facility.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed
Determine If Statement: PE-16 [03] - The organization monitors organization-defined information system components entering the facility.
Inherited From: P210 - Intranet Server
Result: Not Assessed
Determine If Statement: PE-16 [04] - The organization controls organization-defined information system components entering the facility.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed
Determine If Statement: PE-16 [04] - The organization controls organization-defined information system components entering the facility.
Inherited From: P210 - Intranet Server
Result: Not Assessed
Determine If Statement: PE-16 [05] - The organization authorizes organization-defined information system components exiting the facility.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed
Determine If Statement: PE-16 [05] - The organization authorizes organization-defined information system components exiting the facility.
Inherited From: P210 - Intranet Server
Result: Not Assessed
Determine If Statement: PE-16 [06] - The organization monitors organization-defined information system components exiting the facility.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed
Determine If Statement: PE-16 [06] - The organization monitors organization-defined information system components exiting the facility.
Inherited From: P210 - Intranet Server
Result: Not Assessed
Determine If Statement: PE-16 [07] - The organization controls organization-defined information system components exiting the facility.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed
Determine If Statement: PE-16 [07] - The organization controls organization-defined information system components exiting the facility.
Inherited From: P210 - Intranet Server
Result: Not Assessed
Determine If Statement: PE-16 [08] - The organization maintains records of information system components entering the facility.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-16 [08] - The organization maintains records of information system components entering the facility.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-16 [09] - The organization maintains records of information system components exiting the facility.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-16 [09] - The organization maintains records of information system components exiting the facility.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PE-17 -Alternate Work Site

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization:
a. Employs [%Assignment: organization-defined security controls%] at alternate work sites;
b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
The HPES Disaster Recovery Plan, which is maintained electronically by HPES and is accessible by HPES personnel, contains contact numbers for communication with key HPES staff in the event of any system-related emergency. Reporting of security-related emergencies by HUD employees and contractors is executed through a call to the HUD National Help Desk.
Implementation Statement for **P210 - Intranet Server**
The HPES Disaster Recovery Plan, which is maintained electronically by HPES and is accessible by HPES personnel, contains contact numbers for communication with key HPES staff in the event of any system-related emergency. Reporting of security-related emergencies by HUD employees and contractors is executed through a call to the HUD National Help Desk.

Assessment Objective: PE-17 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Physical and environmental protection policy
* Procedures addressing alternate work sites for organizational personnel
* Security plan
* List of security controls required for alternate work sites
* Assessments of security controls at alternate work sites
* Other relevant documents or records

Interview
* Organizational personnel approving use of alternate work sites
* Organizational personnel using alternate work sites
* Organizational personnel assessing controls at alternate work sites
* Organizational personnel with information security responsibilities

Test
* Organizational processes for security at alternate work sites
* Automated mechanisms supporting alternate work sites
* Security controls employed at alternate work sites
* Means of communications between personnel at alternate work sites and security personnel

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PE-17 (a)[01] - The organization defines security controls to be employed at alternate work sites.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed

Determine If Statement: PE-17 (a)[01] - The organization defines security controls to be employed at alternate work sites.
Inherited From: P210 - Intranet Server
Result: Not Assessed

Determine If Statement: PE-17 (a)[02] - The organization employs organization-defined security controls at alternate work sites.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed

Determine If Statement: PE-17 (a)[02] - The organization employs organization-defined security controls at alternate work sites.
Inherited From: P210 - Intranet Server
Result: Not Assessed

Determine If Statement: PE-17 (b) - The organization assesses, as feasible, the effectiveness of security controls at alternate work sites.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed

Determine If Statement: PE-17 (b) - The organization assesses, as feasible, the effectiveness of security controls at alternate work sites.
Inherited From: P210 - Intranet Server
Result: Not Assessed

Determine If Statement: PE-17 (c) - The organization provides a means for employees to communicate with information security personnel in case of security incidents or problems.
Inherited From: P207 - Mainframe (IBM)
Result: Not Assessed

Determine If Statement: PE-17 (c) - The organization provides a means for employees to communicate with information security personnel in case of security incidents or problems.
Inherited From: P210 - Intranet Server
Result: Not Assessed

Control Title: PE-18 -Location Of Information System Components
Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization positions information system components within the facility to minimize potential damage from [%Assignment: organization-defined physical and environmental hazards%] and to minimize the opportunity for unauthorized access.

Assessment Objective: PE-18 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Physical and environmental protection policy
* Procedures addressing positioning of information system components
* Documentation providing the location and position of information system components within the facility
* Locations housing information system components within the facility
* List of physical and environmental hazards with potential to damage information system components within the facility
* Other relevant documents or records

Interview

* Organizational personnel with responsibilities for positioning information system components
* Organizational personnel with information security responsibilities

Test

* Organizational processes for positioning information system components

Determine If Statement: PE-18 [01] - The organization defines physical hazards that could result in potential damage to information system components within the facility.

Result: NA-RTM **Assessed by:** **Date:**

Determine If Statement: PE-18 [02] - The organization defines environmental hazards that could result in potential damage to information system components within the facility.

Result: NA-RTM **Assessed by:** **Date:**

Determine If Statement: PE-18 [03] - The organization positions information system components within the facility to minimize potential damage from organization-defined physical and environmental hazards.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-18 [03] - The organization positions information system components within the facility to minimize potential damage from organization-defined physical and environmental hazards.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Determine If Statement: PE-18 [04] - The organization positions information system components within the facility to minimize the opportunity for unauthorized access.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: PE-18 [04] - The organization positions information system components within the facility to minimize the opportunity for unauthorized access.

Inherited From: P210 - Intranet Server

Result: Not Assessed

Control Title: PL-01 -Security Planning Policy And Procedures

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization:

a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:

1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and

b. Reviews and updates the current:

1. Security planning policy [%Assignment: organization-defined frequency (b)(1)%]; and

2. Security planning procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: Implementation Statement for **Develop IT Security Standards and Policy**

HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

HUD Handbook 2400.25 contains a formal documented security planning policy within Section 3.2. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to security planning.
The security planning policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The security planning procedures to facilitate the implementation of the security planning policy and associated security planning security controls are documented within the Section 3.2 of the Information Technology Security Procedures, dated November 1, 2013.
The security planning procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: PL-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Planning policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with planning responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: PL-01 (a)(01)[01] - The organization develops and documents a planning policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PL-01 (a)(01)[02] - The organization defines personnel or roles to whom the planning policy is to be disseminated.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PL-01 (a)(01)[03] - The organization disseminates the planning policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PL-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the planning policy and associated planning controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PL-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PL-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PL-01 (b)(01)[01] - The organization defines the frequency to review and update the current planning policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PL-01 (b)(01)[02] - The organization reviews and updates the current planning policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PL-01 (b)(02)[01] - The organization defines the frequency to review and update the current planning procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PL-01 (b)(02)[02] - The organization reviews and updates the current planning procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: PL-02 -System Security Plan

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Develops a security plan for the information system that:
1. Is consistent with the organization's enterprise architecture;
2. Explicitly defines the authorization boundary for the system;
3. Describes the operational context of the information system in terms of missions and business processes;
4. Provides the security categorization of the information system including supporting rationale;
5. Describes the operational environment for the information system and relationships with or connections to other information systems;
6. Provides an overview of the security requirements for the system;
7. Identifies any relevant overlays, if applicable;
8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
b. Distributes copies of the security plan and communicates subsequent changes to the plan to [%Assignment: organization-defined personnel or roles%];
c. Reviews the security plan for the information system [%Assignment: organization-defined frequency%];
d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
e. Protects the security plan from unauthorized disclosure and modification.

Implementation Statement: The TRACS team develops and implements a security plan for the F87 TRACS system that provides an overview of the security requirements for the various subsystems and a description of the security controls in

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

place or planned for meeting those requirements. HUD OCIO officials review and approve the plan every 3 years. The plan is reviewed and updated by TRACS staff for every major development effort, and at least yearly. Several updates were recommended and completed in 2012 after a CIRT vulnerability scan.

Assessment Objective: PL-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Security planning policy
* Procedures addressing security plan development and implementation
* Procedures addressing security plan reviews and updates
* Enterprise architecture documentation
* Security plan for the information system
* Records of security plan reviews and updates
* Other relevant documents or records

Interview
* Organizational personnel with security planning and plan implementation responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for security plan development/review/update/approval
* Automated mechanisms supporting the information system security plan

Determine If Statement: PL-02 (a)(01) - The organization develops a security plan for the information system that is consistent with the organization's enterprise architecture.

Result: Not Assessed

Determine If Statement: PL-02 (a)(02) - The organization develops a security plan for the information system that explicitly defines the authorization boundary for the system.

Result: Not Assessed

Determine If Statement: PL-02 (a)(03) - The organization develops a security plan for the information system that describes the operational context of the information system in terms of missions and business processes.

Result: Not Assessed

Determine If Statement: PL-02 (a)(04) - The organization develops a security plan for the information system that provides the security categorization of the information system including supporting rationale.

Result: Not Assessed

Determine If Statement: PL-02 (a)(05) - The organization develops a security plan for the information system that describes the operational environment for the information system and relationships with or connections to other information systems.

Result: Not Assessed

Determine If Statement: PL-02 (a)(06) - The organization develops a security plan for the information system that provides an overview of the security requirements for the system.

Result: Not Assessed

Determine If Statement: PL-02 (a)(07) - The organization develops a security plan for the information system that identifies any relevant overlays, if applicable.

Result: Not Assessed

Determine If Statement: PL-02 (a)(08) - The organization develops a security plan for the information system that describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplemental decisions.

Result: Not Assessed

Determine If Statement: PL-02 (a)(09) - The organization develops a security plan for the information system that is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PL-02 (b)[01] - The organization defines personnel or roles to whom copies of the security plan are to be distributed and subsequent changes to the plan are to be communicated.
Result: Not Assessed

Determine If Statement: PL-02 (b)[02] - The organization distributes copies of the security plan and communicates subsequent changes to the plan to organization-defined personnel or roles.
Result: Not Assessed

Determine If Statement: PL-02 (c)[01] - The organization defines the frequency to review the security plan for the information system.
Result: Not Assessed

Determine If Statement: PL-02 (c)[02] - The organization reviews the security plan for the information system with the organization-defined frequency.
Result: Not Assessed

Determine If Statement: PL-02 (d)[01] - The organization updates the plan to address changes to the information system/environment of operation.
Result: Not Assessed

Determine If Statement: PL-02 (d)[02] - The organization updates the plan to address problems identified during plan implementation.
Result: Not Assessed

Determine If Statement: PL-02 (d)[03] - The organization updates the plan to address problems identified during security control assessments.
Result: Not Assessed

Determine If Statement: PL-02 (e)[01] - The organization protects the security plan from unauthorized disclosure.
Result: Not Assessed

Determine If Statement: PL-02 (e)[02] - The organization protects the security plan from unauthorized modification.
Result: Not Assessed

Control Title: PL-02(3) -Plan / Coordinate With Other Organizational Entities
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization plans and coordinates security-related activities affecting the information system with [%Assignment: organization-defined individuals or groups%] before conducting such activities in order to reduce the impact on other organizational entities.

Implementation Statement: HUD OCIO plans and coordinates security-related activities affecting the information system with HUD intranet users before conducting such activities like replacing servers or upgrading Internet Explorer in order to reduce the impact on other organizational entities.

Assessment Objective: PL-2(3) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Security planning policy
* Access control policy
* Contingency planning policy
* Procedures addressing security-related activity planning for the information system
* Security plan for the information system
* Contingency plan for the information system
* Information system design documentation
* Other relevant documents or records

Interview
* Organizational personnel with security planning and plan implementation responsibilities
* Organizational individuals or groups with whom security-related activities are to be planned and coordinated
* Organizational personnel with information security responsibilities

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PL-02(03) [01] - The organization defines individuals or groups with whom security-related activities affecting the information system are to be planned and coordinated before conducting such activities in order to reduce the impact on other organizational entities.

Result: Not Assessed

Determine If Statement: PL-02(03) [02] - The organization plans and coordinates security-related activities affecting the information system with organization-defined individuals or groups before conducting such activities in order to reduce the impact on other organizational entities.

Result: Not Assessed

Control Title: PL-04 -Rules Of Behavior

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
c. Reviews and updates the rules of behavior [%Assignment: organization-defined frequency%]; and
d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

Implementation Statement: Rules of Behavior are included in this System Security Plan (SSP) as Appendix A. Rules of Behavior are also included in the annual security awareness training which all HUD employees and contractors are required to take. This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The ROB for TRACS is online, along with the HUD version. Annually, the system user is asked to read/print ROB before they can proceed to logon to the system.

Assessment Objective: PL-4 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Security planning policy
* Procedures addressing rules of behavior for information system users
* Rules of behavior
* Signed acknowledgements
* Records for rules of behavior reviews and updates
* Other relevant documents or records

Interview
* Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior
* Organizational personnel who are authorized users of the information system and have signed and resigned rules of behavior
* Organizational personnel with information security responsibilities

Test
* Organizational processes for establishing, reviewing, disseminating, and updating rules of behavior
* Automated mechanisms supporting and/or implementing the establishment, review, dissemination, and update of rules of behavior

Determine If Statement: PL-04 (a)[01] - The organization establishes, for individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.

Result: Not Assessed

Determine If Statement: PL-04 (a)[02] - The organization makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PL-04 (b) - The organization receives a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

Result: Not Assessed

Determine If Statement: PL-04 (c)[01] - The organization defines the frequency to review and update the rules of.

Result: Not Assessed

Determine If Statement: PL-04 (c)[02] - The organization reviews and updates the rules of behavior with the organization-defined frequency.

Result: Not Assessed

Determine If Statement: PL-04 (d) - The organization requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

Result: Not Assessed

Control Title: PL-04(1) -Social Media And Networking Restrictions

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Implementation Statement: The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Assessment Objective: PL-4(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Security planning policy
* Procedures addressing rules of behavior for information system users
* Rules of behavior
* Other relevant documents or records

Interview
* Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior
* Organizational personnel who are authorized users of the information system and have signed rules of behavior
* Organizational personnel with information security responsibilities

Test
* Organizational processes for establishing rules of behavior
* Automated mechanisms supporting and/or implementing the establishment of rules of behavior

Determine If Statement: PL-04(01) [01] - The organization includes the following in the rules of behavior explicit restrictions on the use of social media/networking sites.

Result: Not Assessed

Determine If Statement: PL-04(01) [02] - The organization includes the following in the rules of behavior posting organizational information on public websites.

Result: Not Assessed

Control Title: PL-08 -Information Security Architecture

Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Develops an information security architecture for the information system that:
1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
3. Describes any information security assumptions about, and dependencies on, external services;
b. Reviews and updates the information security architecture [%Assignment: organization-defined frequency%] to reflect updates in the enterprise architecture; and
c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

Implementation Statement: The organization:
a. Develops an information security architecture for the information system that:
1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
2. Describes how the information security architecture is integrated into and supports the enterprise architecture;
b. Reviews and updates the information security architecture annually to reflect updates in the enterprise architecture; and
c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions. HUD's approach described in this CONOPS is designed to ensurethat all HUD IT investments support the Department's mission, close performancegaps, or contribute to HUD's enterprise-wide IT infrastructure.

Assessment Objective: PL-8 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Security planning policy
* Procedures addressing information security architecture development
* Procedures addressing information security architecture reviews and updates
* Enterprise architecture documentation
* Information security architecture documentation
* Security plan for the information system
* Security CONOPS for the information system
* Records of information security architecture reviews and updates
* Other relevant documents or records

Interview
* Organizational personnel with security planning and plan implementation responsibilities
* Organizational personnel with information security architecture development responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for developing, reviewing, and updating the information security architecture
* Automated mechanisms supporting and/or implementing the development, review, and update of the information security architecture

Determine If Statement: PL-08 (a)(01) - The organization develops an information security architecture for the information system that describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.

Result: Not Assessed

Determine If Statement: PL-08 (a)(02) - The organization develops an information security architecture for the information system that describes how the information security architecture is integrated into and supports the enterprise architecture.

Result: Not Assessed

Determine If Statement: PL-08 (a)(03) - The organization develops an information security architecture for the information system that describes any information security assumptions about, and dependencies on, external services.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PL-08 (b)[01] - The organization defines the frequency to review and update the information security architecture.

Result: Not Assessed

Determine If Statement: PL-08 (b)[02] - The organization reviews and updates the information security architecture with the organization-defined frequency to reflect updates in the enterprise architecture.

Result: Not Assessed

Determine If Statement: PL-08 (c)[01] - The organization ensures that planned information security architecture changes are reflected in the security plan.

Result: Not Assessed

Determine If Statement: PL-08 (c)[02] - The organization ensures that planned information security architecture changes are reflected in the security Concept of Operations (CONOPS).

Result: Not Assessed

Determine If Statement: PL-08 (c)[03] - The organization ensures that planned information security architecture changes are reflected in the organizational procurements/acquisitions.

Result: Not Assessed

Control Title: PS-01 -Personnel Security Policy And Procedures

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:

a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:

1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and

b. Reviews and updates the current:

1. Personnel security policy [%Assignment: organization-defined frequency (b)(1)%]; and

2. Personnel security procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: HUD IT security policy (inclusive of personnel security) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. Personnel security compliance policy is specifically addressed in Sections 3.11 and 4.1 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 4.1 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 Section 4.1 documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance. This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.

Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented personnel security policy within Section 4.1. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to personnel security. The personnel security policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following link
http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Intranet portal.
The personnel security procedures to facilitate the implementation of the personnel security policy and associated personnel security controls are documented within the Section 4.1 of the Information Technology Security Procedures, dated November 1, 2013.
The personnel security procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: PS-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Personnel security policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with access control responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: PS-01 (a)(01)[01] - The organization develops and documents an personnel security policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PS-01 (a)(01)[02] - The organization defines personnel or roles to whom the personnel security policy is to be disseminated.

Result: Not Assessed

Determine If Statement: PS-01 (a)(01)[03] - The organization disseminates the personnel security policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PS-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PS-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Not Assessed

Determine If Statement: PS-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PS-01 (b)(01)[01] - The organization defines the frequency to review and update the current personnel security policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PS-01 (b)(01)[02] - The organization reviews and updates the current personnel security policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PS-01 (b)(02)[01] - The organization defines the frequency to review and update the current personnel security procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: PS-01 (b)(02)[02] - The organization reviews and updates the current personnel security procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: PS-02 -Position Risk Designation

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Assigns a risk designation to all organizational positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and updates position risk designations [%Assignment: organization-defined frequency%].

Implementation Statement: The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations annually.

Assessment Objective: PS-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Personnel security policy
* Procedures addressing position categorization
* Appropriate codes of federal regulations
* List of risk designations for organizational positions
* Security plan
* Records of position risk designation reviews and updates
* Other relevant documents or records

Interview
* Organizational personnel with personnel security responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for assigning, reviewing, and updating position risk designations
* Organizational processes for establishing screening criteria

Determine If Statement: PS-02 (a) - The organization assigns a risk designation to all organizational positions.

Result: Not Assessed

Determine If Statement: PS-02 (b) - The organization establishes screening criteria for individuals filling those positions.

Result: Not Assessed

Determine If Statement: PS-02 (c)[01] - The organization defines the frequency to review and update position risk designations.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PS-02 (c)[02] - The organization reviews and updates position risk designations with the organization-defined frequency.

Result: Not Assessed

Control Title: PS-03 -Personnel Screening

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization:
a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals according to [%Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening%].

Implementation Statement: Implementation Statement for **OSEP**

The mission of the Facility Services Branch is to develop, coordinate, and implement policies and procedures concerning the protection of HUD personnel and the security of property at all locations (field and satellite offices) under the charge and control of the Department. The Branch provides security related services for the HUD Headquarters Building, which include oversight of the guard contract, emergency evacuations procedures, threat assessment, building access control, and parking management. On August 27, 2004, the President signed HSPD-12 'Policy for a Common Identification Standard for Federal Employees and Contractors' (the Directive). The Directive requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. As required by the Directive, the Department of Commerce issued Federal Information Processing Standard 201 (the Standard).

Assessment Objective: PS-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Personnel security policy
* Procedures addressing personnel screening
* Records of screened personnel
* Security plan
* Other relevant documents or records

Interview
* Organizational personnel with personnel security responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for personnel screening

Determine If Statement: PS-03 (a) - The organization screens individuals prior to authorizing access to the information system.

Inherited From: OSEP

Result: Not Assessed

Determine If Statement: PS-03 (b)[01] - The organization defines conditions requiring re-screening.

Inherited From: OSEP

Result: Not Assessed

Determine If Statement: PS-03 (b)[02] - The organization defines the frequency of re-screening where it is so indicated.

Inherited From: OSEP

Result: Not Assessed

Determine If Statement: PS-03 (b)[03] - The organization re-screens individuals in accordance with organization-defined conditions requiring re-screening and, where re-screening is so indicated, with the organization-defined frequency of such re-screening.

Inherited From: OSEP

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: PS-04 -Personnel Termination
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization, upon termination of individual employment:
a. Disables information system access within [%Assignment: organization-defined time period (a)%];
b. Terminates/revokes any authenticators/credentials associated with the individual;
c. Conducts exit interviews that include a discussion of [%Assignment: organization-defined information security topics%];
d. Retrieves all security-related organizational information system-related property;
e. Retains access to organizational information and information systems formerly controlled by terminated individual; and
f. Notifies [%Assignment: organization-defined personnel or roles%] within [%Assignment: organization-defined time period (f)%].

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Human Resources, HUD IT Operations ISSO, & Program Area Sponsor/GTR.

Assessment Objective: PS-4 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Personnel security policy
* Procedures addressing personnel termination
* Records of personnel termination actions
* List of information system accounts
* Records of terminated or revoked authenticators/credentials
* Records of exit interviews
* Other relevant documents or records

Interview
* Organizational personnel with personnel security responsibilities
* Organizational personnel with account management responsibilities
* System/network administrators
* Organizational personnel with information security responsibilities

Test
* Organizational processes for personnel termination
* Automated mechanisms supporting and/or implementing personnel termination notifications
* Automated mechanisms for disabling information system access/revoking authenticators

Determine If Statement: PS-04 (a)[01] - The organization, upon termination of individual employment, defines a time period within which to disable information system access.
Result: Not Assessed

Determine If Statement: PS-04 (a)[02] - The organization, upon termination of individual employment, disables information system access within the organization-defined time period.
Result: Not Assessed

Determine If Statement: PS-04 (b) - The organization, upon termination of individual employment, terminates/revokes any authenticators/credentials associated with the individual.
Result: Not Assessed

Determine If Statement: PS-04 (c)[01] - The organization, upon termination of individual employment, defines information security topics to be discussed when conducting exit interviews.
Result: Not Assessed

Determine If Statement: PS-04 (c)[02] - The organization, upon termination of individual employment, conducts exit interviews that include a discussion of organization-defined information security topics.
Result: Not Assessed

Determine If Statement: PS-04 (d) - The organization, upon termination of individual employment, retrieves all security-related organizational information system-related property.
Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PS-04 (e) - The organization, upon termination of individual employment, retains access to organizational information and information systems formerly controlled by the terminated individual.

Result: Not Assessed

Determine If Statement: PS-04 (f)[01] - The organization, upon termination of individual employment, defines personnel or roles to be notified of the termination.

Result: Not Assessed

Determine If Statement: PS-04 (f)[02] - The organization, upon termination of individual employment, defines the time period within which to notify organization-defined personnel or roles.

Result: Not Assessed

Determine If Statement: PS-04 (f)[03] - The organization, upon termination of individual employment, notifies organization-defined personnel or roles within the organization-defined time period.

Result: Not Assessed

Control Title: PS-05 -Personnel Transfer

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiates [%Assignment: organization-defined transfer or reassignment actions%] within [%Assignment: organization-defined time period following the formal transfer action%];
c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notifies [%Assignment: organization-defined personnel or roles%] within [%Assignment: organization-defined time period%].

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Human Resources, HUD IT Operations ISSO, & Program Area Sponsor/GTR.

Assessment Objective: PS-5 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Personnel security policy
* Procedures addressing personnel transfer
* Security plan
* Records of personnel transfer actions
* List of information system and facility access authorizations
* Other relevant documents or records

Interview
* Organizational personnel with personnel security responsibilities organizational personnel with account management responsibilities
* System/network administrators
* Organizational personnel with information security responsibilities

Test
* Organizational processes for personnel transfer
* Automated mechanisms supporting and/or implementing personnel transfer notifications
* Automated mechanisms for disabling information system access/revoking authenticators

Determine If Statement: PS-05 (a)[01] - The organization when individuals are reassigned or transferred to other positions within the organization, reviews and confirms ongoing operational need for current logical access authorizations to information systems.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: PS-05 (a)[02] - The organization when individuals are reassigned or transferred to other positions within the organization, reviews and confirms ongoing operational need for current physical access authorizations to information systems and facilities.

Result: Not Assessed

Determine If Statement: PS-05 (b)[01] - The organization defines transfer or reassignment actions to be initiated following transfer or reassignment.

Result: Not Assessed

Determine If Statement: PS-05 (b)[02] - The organization defines the time period within which transfer or reassignment actions must occur following transfer or reassignment.

Result: Not Assessed

Determine If Statement: PS-05 (b)[03] - The organization initiates organization-defined transfer or reassignment actions within the organization-defined time period following transfer or reassignment.

Result: Not Assessed

Determine If Statement: PS-05 (c) - The organization modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.

Result: Not Assessed

Determine If Statement: PS-05 (d)[01] - The organization defines personnel or roles to be notified when individuals are reassigned or transferred to other positions within the organization.

Result: Not Assessed

Determine If Statement: PS-05 (d)[02] - The organization defines the time period within which to notify organization-defined personnel or roles when individuals are reassigned or transferred to other positions within the organization.

Result: Not Assessed

Determine If Statement: PS-05 (d)[03] - The organization notifies organization-defined personnel or roles within the organization-defined time period when individuals are reassigned or transferred to other positions within the organization.

Result: Not Assessed

Control Title: PS-06 -Access Agreements

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Develops and documents access agreements for organizational information systems;
b. Reviews and updates the access agreements [%Assignment: organization-defined frequency (b)%]; and
c. Ensures that individuals requiring access to organizational information and information systems:
1. Sign appropriate access agreements prior to being granted access; and
2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [%Assignment: organization-defined frequency (c)(2)%].

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Human Resources & HITS Contractors.

Assessment Objective: PS-6 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* Personnel security policy
* Procedures addressing access agreements for organizational information and information systems
* Security plan
* Access agreements
* Records of access agreement reviews and updates
* Other relevant documents or records

Interview
* Organizational personnel with personnel security responsibilities
* Organizational personnel who have signed/resigned access agreements
* Organizational personnel with information security responsibilities

Test
* Organizational processes for access agreements
* Automated mechanisms supporting access agreements

Determine If Statement: PS-06 (a) - The organization develops and documents access agreements for organizational information systems.

Result: Not Assessed

Determine If Statement: PS-06 (b)[01] - The organization defines the frequency to review and update the access agreements.

Result: Not Assessed

Determine If Statement: PS-06 (b)[02] - The organization reviews and updates the access agreements with the organization-defined frequency.

Result: Not Assessed

Determine If Statement: PS-06 (c)(01) - The organization ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.

Result: Not Assessed

Determine If Statement: PS-06 (c)(02)[01] - The organization defines the frequency to re-sign access agreements to maintain access to organizational information systems when access agreements have been updated.

Result: Not Assessed

Determine If Statement: PS-06 (c)(02)[02] - The organization ensures that individuals requiring access to organizational information and information systems re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or with the organization-defined frequency.

Result: Not Assessed

Control Title: PS-07 -Third-Party Personnel Security

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
c. Documents personnel security requirements;
d. Requires third-party providers to notify [%Assignment: organization-defined personnel or roles%] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [%Assignment: organization-defined time period%]; and
e. Monitors provider compliance.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Office of IT Security.

Assessment Objective: PS-7 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* Personnel security policy
* Procedures addressing third-party personnel security
* List of personnel security requirements
* Acquisition documents
* Service-level agreements
* Compliance monitoring process
* Other relevant documents or records

Interview
* Organizational personnel with personnel security responsibilities
* Third-party providers
* System/network administrators
* Organizational personnel with account management responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for managing and monitoring third-party personnel security
* Automated mechanisms supporting and/or implementing monitoring of provider compliance

Determine If Statement: PS-07 (a) - The organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers.
Result: Not Assessed

Determine If Statement: PS-07 (b) - The organization requires third-party providers to comply with personnel security policies and procedures established by the organization.
Result: Not Assessed

Determine If Statement: PS-07 (c) - The organization documents personnel security requirements.
Result: Not Assessed

Determine If Statement: PS-07 (d)[01] - The organization defines personnel or roles to be notified of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges.
Result: Not Assessed

Determine If Statement: PS-07 (d)[02] - The organization defines the time period within which third-party providers are required to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges.
Result: Not Assessed

Determine If Statement: PS-07 (d)[03] - The organization requires third-party providers to notify organization-defined personnel or roles within the organization-defined time period of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges.
Result: Not Assessed

Determine If Statement: PS-07 (e) - The organization monitors provider compliance.
Result: Not Assessed

Control Title: PS-08 -Personnel Sanctions
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notifies [%Assignment: organization-defined personnel or roles%] within [%Assignment: organization-defined time period%] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HUD Office of

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

IT Security.

Assessment Objective: PS-8 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Personnel security policy
* Procedures addressing personnel sanctions
* Rules of behavior
* Records of formal sanctions
* Other relevant documents or records

Interview
* Organizational personnel with personnel security responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for managing personnel sanctions
* Automated mechanisms supporting and/or implementing notifications

Determine If Statement: PS-08 (a) - The organization employs a formal sanctions process for individuals failing to comply with established information security policies and procedures.

Result: Not Assessed

Determine If Statement: PS-08 (b)[01] - The organization defines personnel or roles to be notified when a formal employee sanctions process is initiated.

Result: Not Assessed

Determine If Statement: PS-08 (b)[02] - The organization defines the time period within which organization-defined personnel or roles must be notified when a formal employee sanctions process is initiated.

Result: Not Assessed

Determine If Statement: PS-08 (b)[03] - The organization notifies organization-defined personnel or roles within the organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Result: Not Assessed

Control Title: RA-01 -Risk Assessment Policy And Procedures

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:

a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

b. Reviews and updates the current:
   1. Risk assessment policy [%Assignment: organization-defined frequency (b)(1)%]; and
   2. Risk assessment procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 Section 3.9 Risk Management and Risk Assessment documents risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. This is a common control, the implementation of which is the responsibility of The Office of IT Security.

Implementation Statement for **Develop IT Security Standards and Policy**

HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented risk assessment policy within Section 3.1. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to risk

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

assessment.
The risk assessment policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The risk assessment procedures to facilitate the implementation of the risk assessment policy and associated risk assessment security controls are documented within the Section 3.1 of the Information Technology Security Procedures, dated November 1, 2013.
The risk assessment procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: RA-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Risk assessment policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with risk assessment responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: RA-01 (a)(01)[01] - The organization develops and documents a risk assessment policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: RA-01 (a)(01)[02] - The organization defines personnel or roles to whom the risk assessment policy is to be disseminated.

Result: Not Assessed

Determine If Statement: RA-01 (a)(01)[03] - The organization disseminates the risk assessment policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: RA-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: RA-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: RA-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: RA-01 (b)(01)[01] - The organization defines the frequency to review and update the current risk assessment policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: RA-01 (b)(01)[02] - The organization reviews and updates the current risk assessment policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: RA-01 (b)(02)[01] - The organization defines the frequency to review and update the current risk assessment procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: RA-01 (b)(02)[02] - The organization reviews and updates the current risk assessment procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: RA-02 -Security Categorization

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Implementation Statement: The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations TRACS was reviewed on 1/17/2014, and the ATO was signed by Carolyn Cockrell (system owner), Harold Williams (Security), and Carol Galante (Authorizing Official.). The system was categorized in accordance with FIPS 199 and NIST 800-60. Results are documented in the system security plan (SSP). The categorization is reviewed by the HUD Chief Information Security Officer. F87 TRACS system has a Security Categorization of Moderate.
_____ Note: Information systems containing privacy act data should ensure that data categorization is consistent with Federal Standards as documented in NIST Special Publication 800-60. Systems that contain Personal Identifiable Information (PII) are automatically either a moderate or high level sensitivity.

Assessment Objective: RA-2 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* Risk assessment policy
* Security planning policy and procedures
* Procedures addressing security categorization of organizational information and information systems
* Security plan
* Security categorization documentation
* Other relevant documents or records

Interview
* Organizational personnel with security categorization and risk assessment responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for security categorization

Determine If Statement: RA-02 (a) - The organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Result: Not Assessed

Determine If Statement: RA-02 (b) - The organization documents the security categorization results (including supporting rationale) in the security plan for the information system.

Result: Not Assessed

Determine If Statement: RA-02 (c) - The organization ensures the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Result: Not Assessed

Control Title: RA-03 -Risk Assessment

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in [%Selection: security plan; risk assessment report; [Assignment: organization-defined document]%];
c. Reviews risk assessment results [%Assignment: organization-defined frequency (c)%];
d. Disseminates risk assessment results to [%Assignment: organization-defined personnel or roles%]; and
e. Updates the risk assessment [%Assignment: organization-defined frequency (e)%] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Implementation Statement: The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency

Assessment Objective: RA-3 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Risk assessment policy
* Security planning policy and procedures
* Procedures addressing organizational assessments of risk
* Security plan
* Risk assessment
* Risk assessment results
* Risk assessment reviews
* Risk assessment updates
* Other relevant documents or records

Interview

* Organizational personnel with risk assessment responsibilities
* Organizational personnel with information security responsibilities

Test

* Organizational processes for risk assessment
* Automated mechanisms supporting and/or for conducting, documenting, reviewing, disseminating, and updating the risk assessment

Determine If Statement: RA-03 (a) - The organization conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of:
* the information system;
* the information the system processes, stores, or transmits.

Result: Not Assessed

Determine If Statement: RA-03 (b)[01] - The organization defines a document in which risk assessment results are to be documented (if not documented in the security plan or risk assessment report).

Result: Not Assessed

Determine If Statement: RA-03 (b)[02] - The organization documents risk assessment results in one of the following:
* the security plan;
* the risk assessment report; or
* the organization-defined document.

Result: Not Assessed

Determine If Statement: RA-03 (c)[01] - The organization defines the frequency to review risk assessment results.

Result: Not Assessed

Determine If Statement: RA-03 (c)[02] - The organization reviews risk assessment results with the organization-defined frequency.

Result: Not Assessed

Determine If Statement: RA-03 (d)[01] - The organization defines personnel or roles to whom risk assessment results are to be disseminated.

Result: Not Assessed

Determine If Statement: RA-03 (d)[02] - The organization disseminates risk assessment results to organization-defined personnel or roles.

Result: Not Assessed

Determine If Statement: RA-03 (e)[01] - The organization defines the frequency to update the risk assessment.

Result: Not Assessed

Determine If Statement: RA-03 (e)[02][a] - The organization updates the risk assessment with the organization-defined frequency.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: RA-03 (e)[02][b] - The organization updates the risk assessment whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities).

Result: Not Assessed

Determine If Statement: RA-03 (e)[02][c] - The organization updates the risk assessment whenever there are other conditions that may impact the security state of the system.

Result: Not Assessed

Control Title: RA-05 -Vulnerability Scanning

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Scans for vulnerabilities in the information system and hosted applications [%Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process%] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities [%Assignment: organization-defined response times%] in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with [%Assignment: organization-defined personnel or roles%] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Implementation Statement: Vulnerability Scanning capability is employed within the HUD Information Technology Infrastructure. HUD Operations Division conducts vulnerability scans regularly. This is a common control, the implementation of which is the responsibility of the HITS contract under EDS/Lockheed Martin Security and the Office of the Chief Information Officer.

Assessment Objective: RA-5 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Risk assessment policy
* Procedures addressing vulnerability scanning
* Risk assessment
* Security plan
* Security assessment report
* Vulnerability scanning tools and associated configuration documentation
* Vulnerability scanning results
* Patch and vulnerability management records
* Other relevant documents or records

Interview
* Organizational personnel with risk assessment, security control assessment and vulnerability scanning responsibilities
* Organizational personnel with vulnerability scan analysis responsibilities
* Organizational personnel with vulnerability remediation responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for vulnerability scanning, analysis, remediation, and information sharing
* Automated mechanisms supporting and/or implementing vulnerability scanning, analysis, remediation, and information sharing

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: RA-05 (a)[01] - The organization
* defines the frequency for conducting vulnerability scans on the information system and hosted applications; and/or
* defines the process for conducting random vulnerability scans on the information system and hosted applications.

Result: Not Assessed

Determine If Statement: RA-05 (a)[02][a] - The organization in accordance with the organization-defined frequency and/or organization-defined process for conducting random scans, scans for vulnerabilities in the information system.

Result: Not Assessed

Determine If Statement: RA-05 (a)[02][b] - The organization in accordance with the organization-defined frequency and/or organization-defined process for conducting random scans, scans for vulnerabilities in hosted applications.

Result: Not Assessed

Determine If Statement: RA-05 (a)[03][a] - The organization when new vulnerabilities potentially affecting the system/applications are identified and reported, scans for vulnerabilities in the information system.

Result: Not Assessed

Determine If Statement: RA-05 (a)[03][b] - The organization when new vulnerabilities potentially affecting the system/applications are identified and reported, scans for vulnerabilities in hosted applications.

Result: Not Assessed

Determine If Statement: RA-05 (b)(01)[01] - The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for enumerating platforms.

Result: Not Assessed

Determine If Statement: RA-05 (b)(01)[02] - The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for enumerating software flaws.

Result: Not Assessed

Determine If Statement: RA-05 (b)(01)[03] - The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for enumerating improper configurations.

Result: Not Assessed

Determine If Statement: RA-05 (b)(02)[01] - The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for formatting checklists.

Result: Not Assessed

Determine If Statement: RA-05 (b)(02)[02] - The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for formatting test procedures.

Result: Not Assessed

Determine If Statement: RA-05 (b)(03) - The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for measuring vulnerability impact.

Result: Not Assessed

Determine If Statement: RA-05 (c)[01] - The organization analyzes vulnerability scan reports.

Result: Not Assessed

Determine If Statement: RA-05 (c)[02] - The organization analyzes results from security control assessments.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: RA-05 (d)[01] - The organization defines response times to remediate legitimate vulnerabilities in accordance with an organizational assessment of risk.

Result: Not Assessed

Determine If Statement: RA-05 (d)[02] - The organization remediates legitimate vulnerabilities within the organization-defined response times in accordance with an organizational assessment of risk.

Result: Not Assessed

Determine If Statement: RA-05 (e)[01] - The organization defines personnel or roles with whom information obtained from the vulnerability scanning process and security control assessments is to be shared.

Result: Not Assessed

Determine If Statement: RA-05 (e)[02] - The organization shares information obtained from the vulnerability scanning process with organization-defined personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Result: Not Assessed

Determine If Statement: RA-05 (e)[03] - The organization shares information obtained from security control assessments with organization-defined personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Result: Not Assessed

Control Title: RA-05(1) -Update Tool Capability

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

Implementation Statement: HUD operations as part of the HITS contract conducts regular vulnerability scanning to determine vulnerablilities in the system.

Assessment Objective: RA-5(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Procedures addressing vulnerability scanning
* Security plan
* Security assessment report
* Vulnerability scanning tools and associated configuration documentation
* Vulnerability scanning results
* Patch and vulnerability management records
* Other relevant documents or records

Interview
* Organizational personnel with vulnerability scanning responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for vulnerability scanning
* Automated mechanisms/tools supporting and/or implementing vulnerability scanning

Determine If Statement: RA-05(01) - The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

Result: Not Assessed

Control Title: RA-05(2) -Update By Frequency / Prior To New Scan / When Identified

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization updates the information system vulnerabilities scanned [%Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported%].

Implementation Statement: The organization updates the information system vulnerabilities scanned regularly when new vulnerabilities are identified and reported as POAM.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Assessment Objective: RA-5(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* Procedures addressing vulnerability scanning
* Security plan
* Security assessment report
* Vulnerability scanning tools and associated configuration documentation
* Vulnerability scanning results
* Patch and vulnerability management records
* Other relevant documents or records

Interview
* Organizational personnel with vulnerability scanning responsibilities
* Organizational personnel with vulnerability scan analysis responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators

Test
* Organizational processes for vulnerability scanning
* Automated mechanisms/tools supporting and/or implementing vulnerability scanning

Determine If Statement: RA-05(02) [01] - The organization defines the frequency to update the information system vulnerabilities scanned.

Result: Not Assessed

Determine If Statement: RA-05(02) [02] - The organization updates the information system vulnerabilities scanned one or more of the following:
* with the organization-defined frequency;
* prior to a new scan; and/or
* when new vulnerabilities are identified and reported.

Result: Not Assessed

Control Title: RA-05(5) -Privileged Access

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system implements privileged access authorization to [%Assignment: organization-identified information system components%] for selected [%Assignment: organization-defined vulnerability scanning activities%].

Implementation Statement: HUD authorizes privileged access authorization to TRACS system for selected defined coding vulnerability scanning activities which are addressed in a software release.

Assessment Objective: RA-5(5) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* Risk assessment policy
* Procedures addressing vulnerability scanning
* Security plan
* Information system design documentation
* Information system configuration settings and associated documentation
* List of information system components for vulnerability scanning
* Personnel access authorization list
* Authorization credentials
* Access authorization records
* Other relevant documents or records

Interview
* Organizational personnel with vulnerability scanning responsibilities
* System/network administrators
* Organizational personnel responsible for access control to the information system
* Organizational personnel responsible for configuration management of the information system
* System developers
* Organizational personnel with information security responsibilities

Test
* Organizational processes for vulnerability scanning
* Organizational processes for access control
* Automated mechanisms supporting and/or implementing access control
* Automated mechanisms/tools supporting and/or implementing vulnerability scanning

Determine If Statement: RA-05(05) [01] - The organization defines information system components to which privileged access is authorized for selected vulnerability scanning activities.

Result: Not Assessed

Determine If Statement: RA-05(05) [02] - The organization defines vulnerability scanning activities selected for privileged access authorization to organization-defined information system components.

Result: Not Assessed

Determine If Statement: RA-05(05) [03] - The information system implements privileged access authorization to organization-defined information system components for selected organization-defined vulnerability scanning activities.

Result: Not Assessed

Control Title: SA-01 -System And Services Acquisition Policy And Procedures

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:

a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:

1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

b. Reviews and updates the current:

1. System and services acquisition policy [%Assignment: organization-defined frequency (b)(1)%]; and

2. System and services acquisition procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: HUD IT security policy (inclusive of system and services acquisition) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. System and services acquisition compliance policy is specifically addressed in Sections 3.2, 3.3, 4.6.2, 4.6.3, and 4.7.2 of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 3.3 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation. This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security
The HUD Information Technology Security Policy – Handbook 2400.25 Rev. 2 documents, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, and compliance. This is a common control, the implementation of which is the responsibility of the Office of IT Security.

Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented system and services acquisition policy within Section 3.3. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to system and services acquisition.
The system and services acquisition policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The system and services acquisition procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition security controls are documented within the Section 3.3 of the Information Technology Security Procedures, dated November 1, 2013.
The system and services acquisition procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: SA-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and services acquisition policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with system and services acquisition responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: SA-01 (a)(01)[01] - The organization develops and documents a system and services acquisition policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SA-01 (a)(01)[02] - The organization defines personnel or roles to whom the system and services acquisition policy is to be disseminated.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SA-01 (a)(01)[03] - The organization disseminates the system and services acquisition policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SA-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SA-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Not Assessed

Determine If Statement: SA-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SA-01 (b)(01)[01] - The organization defines the frequency to review and update the current system and services acquisition policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SA-01 (b)(01)[02] - The organization reviews and updates the current system and services acquisition policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SA-01 (b)(02)[01] - The organization defines the frequency to review and update the current system and services acquisition procedures.

Result: Not Assessed

Determine If Statement: SA-01 (b)(02)[02] - The organization reviews and updates the current system and services acquisition procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: SA-02 -Allocation Of Resources

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Determines information security requirements for the information system or information system service in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Implementation Statement: Security requirements for the TRACS System are incorporated into development/operations/ maintenance contracts and Service Level Agreements with the HITS Contractors. These documents, as well as the funding necessary to ensure the required level of security protection, are reviewed and adjusted annually. This is a common control, the implementation of which is the responsibility of the HUD Office of Information Technology Investment Management.

Assessment Objective: SA-2 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* System and services acquisition policy
* Procedures addressing the allocation of resources to information security requirements
* Procedures addressing capital planning and investment control
* Organizational programming and budgeting documentation
* Other relevant documents or records

Interview
* Organizational personnel with capital planning, investment control, organizational programming and budgeting responsibilities
* Organizational personnel responsible for determining information security requirements for information systems/services
* Organizational personnel with information security responsibilities

Test
* Organizational processes for determining information security requirements
* Organizational processes for capital planning, programming, and budgeting
* Automated mechanisms supporting and/or implementing organizational capital planning, programming, and budgeting

Determine If Statement: SA-02 (a) - The organization determines information security requirements for the information system or information system service in mission/business process planning.

Result: Not Assessed

Determine If Statement: SA-02 (b)[01] - The organization to protect the information system or information system service as part of its capital planning and investment control process determines the resources required.

Result: Not Assessed

Determine If Statement: SA-02 (b)[02] - The organization to protect the information system or information system service as part of its capital planning and investment control process documents the resources required.

Result: Not Assessed

Determine If Statement: SA-02 (b)[03] - The organization to protect the information system or information system service as part of its capital planning and investment control process allocates the resources required.

Result: Not Assessed

Determine If Statement: SA-02 (c) - The organization establishes a discrete line item for information security in organizational programming and budgeting documentation.

Result: Not Assessed

Control Title: SA-03 -System Development Life Cycle

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Manages the information system using [%Assignment: organization-defined system development life cycle%] that incorporates information security considerations;
b. Defines and documents information security roles and responsibilities throughout the system development life cycle;
c. Identifies individuals having information security roles and responsibilities; and
d. Integrates the organizational information security risk management process into system development life cycle activities.

Implementation Statement: The TRACS System is managed in accordance with the system development life cycle (SDLC) methodology enforced by the HUD Office of Systems Integration and Efficiency and documented in the HUD System Development Methodology, Release 6.05, and June 2005. The system is currently in the SDLC phase of the system life cycle. This is a common control, the implementation of which is the responsibility of the HUD Office of Systems Integration and Efficiency.

Assessment Objective: SA-3 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* System and services acquisition policy
* Procedures addressing the integration of information security into the system development life cycle process
* Information system development life cycle documentation
* Information security risk management strategy/program documentation
* Other relevant documents or records

Interview
* Organizational personnel with information security and system life cycle development responsibilities
* Organizational personnel with information security risk management responsibilities
* Organizational personnel with information security responsibilities

Test
* Organizational processes for defining and documenting the SDLC
* Organizational processes for identifying SDLC roles and responsibilities
* Organizational process for integrating information security risk management into the SDLC
* Automated mechanisms supporting and/or implementing the SDLC

Determine If Statement: SA-03 (a)[01] - The organization defines a system development life cycle that incorporates information security considerations to be used to manage the information system.

Result: Not Assessed

Determine If Statement: SA-03 (a)[02] - The organization manages the information system using the organization-defined system development life cycle.

Result: Not Assessed

Determine If Statement: SA-03 (b) - The organization defines and documents information security roles and responsibilities throughout the system development life cycle.

Result: Not Assessed

Determine If Statement: SA-03 (c) - The organization identifies individuals having information security roles and responsibilities.

Result: Not Assessed

Determine If Statement: SA-03 (d) - The organization integrates the organizational information security risk management process into system development life cycle activities.

Result: Not Assessed

Control Title: SA-04 -Acquisition Process

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:
a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Requirements for protecting security-related documentation;
f. Description of the information system development environment and environment in which the system is intended to operate; and
g. Acceptance criteria.

Implementation Statement: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.

Assessment Objective: SA-4 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and services acquisition policy
* Procedures addressing the integration of information security requirements, descriptions, and criteria into the acquisition process
* Acquisition contracts for the information system, system component, or information system service
* Information system design documentation
* Other relevant documents or records

Interview

* Organizational personnel with acquisition/contracting responsibilities
* Organizational personnel with responsibility for determining information system security functional, strength, and assurance requirements
* System/network administrators
* Organizational personnel with information security responsibilities

Test

* Organizational processes for determining information system security functional, strength, and assurance requirements
* Organizational processes for developing acquisition contracts
* Automated mechanisms supporting and/or implementing acquisitions and inclusion of security requirements in contracts

Determine If Statement: SA-04 - The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contracts for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

* security functional requirements;
* security strength requirements;
* security assurance requirements;
* security-related documentation requirements;
* requirements for protecting security-related documentation;
* description of the information system development environment; the environment in which the system is intended to operate; and
* acceptance criteria.

Result: Not Assessed

Control Title: SA-04(1) -Functional Properties Of Security Controls

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Implementation Statement: The organization requires solicitation documents to provide functional properties of security controls with sufficient detail to permit analysis and testing of the controls.
The Functional Requirements Document describes the properties of security controls.

Assessment Objective: SA-4(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and services acquisition policy
* Procedures addressing the integration of information security requirements, descriptions, and criteria into the acquisition process
* Solicitation documents
* Acquisition documentation
* Acquisition contracts for the information system, system component, or information system services
* Other relevant documents or records

Interview

* Organizational personnel with acquisition/contracting responsibilities
* Organizational personnel with responsibility for determining information system security functional requirements
* Information system developer or service provider
* Organizational personnel with information security responsibilities

Test

* Organizational processes for determining information system security functional, requirements
* Organizational processes for developing acquisition contracts
* Automated mechanisms supporting and/or implementing acquisitions and inclusion of security requirements in contracts

Determine If Statement: SA-04(01) - The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Result: Not Assessed

Control Title: SA-04(2) -Design / Implementation Information For Security Controls

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [%Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]%] at [%Assignment: organization-defined level of detail%].

Implementation Statement: The organization requires the information system to provide design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces; high-level design, including internet/intranet access identifier, employee/contractor/business partner identifier, sub-system role or action code, field/regional/HQ access to TRACS.

Assessment Objective: SA-4(2) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and services acquisition policy
* Procedures addressing the integration of information security requirements, descriptions, and criteria into the acquisition process
* Solicitation documents
* Acquisition documentation
* Acquisition contracts for the information system, system components, or information system services
* Design and implementation information for security controls employed in the information system, system component, or information system service
* Other relevant documents or records

Interview

* Organizational personnel with acquisition/contracting responsibilities
* Organizational personnel with responsibility for determining information system security requirements
* Information system developer or service provider
* Organizational personnel with information security responsibilities

Test

* Organizational processes for determining level of detail for system design and security controls
* Organizational processes for developing acquisition contracts
* Automated mechanisms supporting and/or implementing development of system design details

Determine If Statement: SA-04(02) [01] - The organization defines level of detail that the developer is required to provide in design and implementation information for the security controls to be employed in the information system, system component, or information system service.

Result: Not Assessed

Determine If Statement: SA-04(02) [02] - The organization defines design/implementation information that the developer is to provide for the security controls to be employed (if selected).

Result: Not Assessed

Determine If Statement: SA-04(02) [03] - The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes, at the organization-defined level of detail, one or more of the following:

* security-relevant external system interfaces;
* high-level design;
* low-level design;
* source code;
* hardware schematics; and/or
* organization-defined design/implementation information.

Result: Not Assessed

Control Title: SA-04(9) -Functions / Ports / Protocols / Services In Use

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

Implementation Statement: The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. This is coordinated with MFDCS personnel who keep records.

Assessment Objective: SA-4(9) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and services acquisition policy
* Procedures addressing the integration of information security requirements, descriptions, and criteria into the acquisition process
* Information system design documentation
* Information system documentation including functions, ports, protocols, and services intended for organizational use
* Acquisition contracts for information systems or services
* Acquisition documentation
* Solicitation documentation
* Service-level agreements
* Organizational security requirements, descriptions, and criteria for developers of information systems, system components, and information system services
* Other relevant documents or records

Interview

* Organizational personnel with acquisition/contracting responsibilities
* Organizational personnel with responsibility for determining information system security requirements
* System/network administrators
* Organizational personnel operating, using, and/or maintaining the information system
* Information system developers
* Organizational personnel with information security responsibilities

Determine If Statement: SA-04(09) [01] - The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle the functions intended for organizational use.

Result: Not Assessed

Determine If Statement: SA-04(09) [02] - The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle the ports intended for organizational use.

Result: Not Assessed

Determine If Statement: SA-04(09) [03] - The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle the protocols intended for organizational use.

Result: Not Assessed

Determine If Statement: SA-04(09) [04] - The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle the services intended for organizational use.

Result: Not Assessed

Control Title: SA-04(10) -Use Of Approved Piv Products

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Implementation Statement: The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Assessment Objective: SA-4(10) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and services acquisition policy
* Procedures addressing the integration of information security requirements, descriptions, and criteria into the acquisition process
* Solicitation documentation
* Acquisition documentation
* Acquisition contracts for the information system, system component, or information system service
* Service-level agreements
* Other relevant documents or records

Interview

* Organizational personnel with acquisition/contracting responsibilities
* Organizational personnel with responsibility for determining information system security requirements
* Organizational personnel with responsibility for ensuring only FIPS 201-approved products are implemented
* Organizational personnel with information security responsibilities

Test

* Organizational processes for selecting and employing FIPS 201-approved products

Determine If Statement: SA-04(10) - The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Result: Not Assessed

Control Title: SA-05 -Information System Documentation

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:

a. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

b. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;

c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [%Assignment: organization-defined actions%] in response;

d. Protects documentation as required, in accordance with the risk management strategy; and

e. Distributes documentation to [%Assignment: organization-defined personnel or roles%].

Implementation Statement: The organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.

Assessment Objective: SA-5 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and services acquisition policy
* Procedures addressing information system documentation
* Information system documentation including administrator and user guides
* Records documenting attempts to obtain unavailable or nonexistent information system documentation
* List of actions to be taken in response to documented attempts to obtain information system, system component, or information system service documentation
* Risk management strategy documentation
* Other relevant documents or records

Interview

* Organizational personnel with acquisition/contracting responsibilities
* Organizational personnel with responsibility for determining information system security requirements
* System administrators
* Organizational personnel operating, using, and/or maintaining the information system
* Information system developers
* Organizational personnel with information security responsibilities

Test

* Organizational processes for obtaining, protecting, and distributing information system administrator and user documentation

Determine If Statement: SA-05 (a)(01)[01] - The organization obtains administrator documentation for the information system, system component, or information system service that describes secure configuration of the system, system component, or service.

Result: Not Assessed

Determine If Statement: SA-05 (a)(01)[02] - The organization obtains administrator documentation for the information system, system component, or information system service that describes secure installation of the system, system component, or service.

Result: Not Assessed

Determine If Statement: SA-05 (a)(01)[03] - The organization obtains administrator documentation for the information system, system component, or information system service that describes secure operation of the system, system component, or service.

Result: Not Assessed

Determine If Statement: SA-05 (a)(02)[01] - The organization obtains administrator documentation for the information system, system component, or information system service that describes effective use of the security features/mechanisms.

Result: Not Assessed

Determine If Statement: SA-05 (a)(02)[02] - The organization obtains administrator documentation for the information system, system component, or information system service that describes effective maintenance of the security features/mechanisms.

Result: Not Assessed

Determine If Statement: SA-05 (a)(03) - The organization obtains administrator documentation for the information system, system component, or information system service that describes known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SA-05 (b) - The organization obtains user documentation for the information system, system component, or information system service that describes:
* user-accessible security functions/mechanisms; how to effectively use those functions/mechanisms;
* methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner;
* user responsibilities in maintaining the security of the system, component, or service.

Result: Not Assessed

Determine If Statement: SA-05 (c)[01] - The organization defines actions to be taken after documented attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.

Result: Not Assessed

Determine If Statement: SA-05 (c)[02] - The organization documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.

Result: Not Assessed

Determine If Statement: SA-05 (c)[03] - The organization takes organization-defined actions in response.

Result: Not Assessed

Determine If Statement: SA-05 (d) - The organization protects documentation as required, in accordance with the risk management strategy.

Result: Not Assessed

Determine If Statement: SA-05 (e)[01] - The organization defines personnel or roles to whom documentation is to be distributed.

Result: Not Assessed

Determine If Statement: SA-05 (e)[02] - The organization distributes documentation to organization-defined personnel or roles.

Result: Not Assessed

Control Title: SA-08 -Security Engineering Principles

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Implementation Statement: The organization designs and implements the information system using security engineering principles.

Assessment Objective: SA-8 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and services acquisition policy
* Procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the information system
* Information system design documentation
* Information security requirements and specifications for the information system
* Other relevant documents or records

Interview

* Organizational personnel with acquisition/contracting responsibilities
* Organizational personnel with responsibility for determining information system security requirements
* Organizational personnel with information system specification, design, development, implementation, and modification responsibilities
* Information system developers
* Organizational personnel with information security responsibilities

Test

* Organizational processes for applying security engineering principles in information system specification, design, development, implementation, and modification
* Automated mechanisms supporting the application of security engineering principles in information system specification, design, development, implementation, and modification

Determine If Statement: SA-08 [01] - The organization applies information system security engineering principles in the specification of the information system.

Result: Not Assessed

Determine If Statement: SA-08 [02] - The organization applies information system security engineering principles in the design of the information system.

Result: Not Assessed

Determine If Statement: SA-08 [03] - The organization applies information system security engineering principles in the development of the information system.

Result: Not Assessed

Determine If Statement: SA-08 [04] - The organization applies information system security engineering principles in the implementation of the information system.

Result: Not Assessed

Determine If Statement: SA-08 [05] - The organization applies information system security engineering principles in the modification of the information system.

Result: Not Assessed

Control Title: SA-09 -External Information System Services

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ [%Assignment: organization-defined security controls%] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

c. Employs [%Assignment: organization-defined processes, methods, and techniques%] to monitor security control compliance by external service providers on an ongoing basis.

Implementation Statement: The organization ensures that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance.

Assessment Objective: SA-9 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and services acquisition policy
* Procedures addressing external information system services
* Procedures addressing methods and techniques for monitoring security control compliance by external service providers of information system services
* Acquisition contracts, service-level agreements
* Organizational security requirements and security specifications for external provider services
* Security control assessment evidence from external providers of information system services
* Other relevant documents or records

Interview

* Organizational personnel with system and services acquisition responsibilities
* External providers of information system services
* Organizational personnel with information security responsibilities

Test

* Organizational processes for monitoring security control compliance by external service providers on an ongoing basis
* Automated mechanisms for monitoring security control compliance by external service providers on an ongoing basis

Determine If Statement: SA-09 (a)[01] - The organization defines security controls to be employed by providers of external information system services.

Result: Not Assessed

Determine If Statement: SA-09 (a)[02] - The organization requires that providers of external information system services comply with organizational information security requirements.

Result: Not Assessed

Determine If Statement: SA-09 (a)[03] - The organization requires that providers of external information system services employ organization-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Result: Not Assessed

Determine If Statement: SA-09 (b) - The organization
* defines and documents government oversight with regard to external information system services;
* defines and documents user roles and responsibilities with regard to external information system services.

Result: Not Assessed

Determine If Statement: SA-09 (c)[01] - The organization defines processes, methods, and techniques to be employed to monitor security control compliance by external service providers.

Result: Not Assessed

Determine If Statement: SA-09 (c)[02] - The organization employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

Result: Not Assessed

Control Title: SA-09(2) -Identification Of Functions / Ports / Protocols / Services

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization requires providers of [%Assignment: organization-defined external information system services%] to identify the functions, ports, protocols, and other services required for the use of such services.

Implementation Statement: The organization requires providers of TRACS information system to identify the functions, ports, protocols, and other services required for the use of such services. This is recorded by MFDCS.

Assessment Objective: SA-9(2) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and services acquisition policy
* Procedures addressing external information system services
* Acquisition contracts for the information system, system component, or information system service
* Acquisition documentation
* Solicitation documentation, service-level agreements
* Organizational security requirements and security specifications for external service providers
* List of required functions, ports, protocols, and other services
* Other relevant documents or records

Interview

* Organizational personnel with system and services acquisition responsibilities
* Organizational personnel with information security responsibilities
* System/network administrators
* External providers of information system services

Determine If Statement: SA-09(02) [01] - The organization defines external information system services for which providers of such services are to identify the functions, ports, protocols, and other services required for the use of such services.

Result: Not Assessed

Determine If Statement: SA-09(02) [02][a] - The organization requires providers of organization-defined external information system services to identify the functions required for the use of such services.

Result: Not Assessed

Determine If Statement: SA-09(02) [02][b] - The organization requires providers of organization-defined external information system services to identify the ports required for the use of such services.

Result: Not Assessed

Determine If Statement: SA-09(02) [02][c] - The organization requires providers of organization-defined external information system services to identify the protocols required for the use of such services.

Result: Not Assessed

Determine If Statement: SA-09(02) [02][d] - The organization requires providers of organization-defined external information system services to identify the other services required for the use of such services.

Result: Not Assessed

Control Title: SA-10 -Developer Configuration Management

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization requires the developer of the information system, system component, or information system service to:

a. Perform configuration management during system, component, or service [%Selection (one or more): design; development; implementation; operation%];

b. Document, manage, and control the integrity of changes to [%Assignment: organization-defined configuration items under configuration management%];

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to [%Assignment: organization-defined personnel%].

Implementation Statement: The system has a dedicated configuration management specialist who manages approved changes to design at each testing phase and implements changes during software releases via a HARTS request and file list to the MFDCS integration team.

Assessment Objective: SA-10 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and services acquisition policy
* Procedures addressing system developer configuration management
* Solicitation documentation
* Acquisition documentation
* Service-level agreements
* Acquisition contracts for the information system, system component, or information system service
* System developer configuration management plan
* Security flaw and flaw resolution tracking records
* System change authorization records
* Change control records
* Configuration management records
* Other relevant documents or records

Interview

* Organizational personnel with system and services acquisition responsibilities
* Organizational personnel with information security responsibilities
* Organizational personnel with configuration management responsibilities
* System developers

Test

* Organizational processes for monitoring developer configuration management
* Automated mechanisms supporting and/or implementing the monitoring of developer configuration management

Determine If Statement: SA-10 (a) - The organization requires the developer of the information system, system component, or information system service to perform configuration management during one or more of the following:

* system, component, or service design;
* system, component, or service development;
* system, component, or service implementation; and/or
* system, component, or service operation.

Result: Not Assessed

Determine If Statement: SA-10 (b)[01] - The organization defines configuration items to be placed under configuration management.

Result: Not Assessed

Determine If Statement: SA-10 (b)[02][a] - The organization requires the developer of the information system, system component, or information system service to document the integrity of changes to organization-defined items under configuration management.

Result: Not Assessed

Determine If Statement: SA-10 (b)[02][b] - The organization requires the developer of the information system, system component, or information system service to manage the integrity of changes to organization-defined items under configuration management.

Result: Not Assessed

Determine If Statement: SA-10 (b)[02][c] - The organization requires the developer of the information system, system component, or information system service to control the integrity of changes to organization-defined items under configuration management.

Result: Not Assessed

Determine If Statement: SA-10 (c) - The organization requires the developer of the information system, system component, or information system service to implement only organization-approved changes to the system, component, or service.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SA-10 (d)[01] - The organization requires the developer of the information system, system component, or information system service to document approved changes to the system, component, or service.

Result: Not Assessed

Determine If Statement: SA-10 (d)[02] - The organization requires the developer of the information system, system component, or information system service to document the potential security impacts of such changes.

Result: Not Assessed

Determine If Statement: SA-10 (e)[01] - The organization defines personnel to whom findings, resulting from security flaws and flaw resolution tracked within the system, component, or service, are to be reported.

Result: Not Assessed

Determine If Statement: SA-10 (e)[02][a] - The organization requires the developer of the information system, system component, or information system service to track security flaws within the system, component, or service.

Result: Not Assessed

Determine If Statement: SA-10 (e)[02][b] - The organization requires the developer of the information system, system component, or information system service to track security flaw resolution within the system, component, or service.

Result: Not Assessed

Determine If Statement: SA-10 (e)[02][c] - The organization requires the developer of the information system, system component, or information system service to report findings to organization-defined personnel.

Result: Not Assessed

Control Title: SA-11 -Developer Security Testing And Evaluation

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization requires the developer of the information system, system component, or information system service to:
a. Create and implement a security assessment plan;
b. Perform [%Selection (one or more): unit; integration; system; regression%] testing/evaluation at [%Assignment: organization-defined depth and coverage%];
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during security testing/evaluation.

Implementation Statement: The information system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.

Assessment Objective: SA-11 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* System and services acquisition policy
* Procedures addressing system developer security testing
* Procedures addressing flaw remediation
* Solicitation documentation
* Acquisition documentation
* Service-level agreements
* Acquisition contracts for the information system, system component, or information system service
* System developer security test plans
* Records of developer security testing results for the information system, system component, or information system service
* Security flaw and remediation tracking records
* Other relevant documents or records

Interview
* Organizational personnel with system and services acquisition responsibilities
* Organizational personnel with information security responsibilities
* Organizational personnel with developer security testing responsibilities
* System developers

Test
* Organizational processes for monitoring developer security testing and evaluation
* Automated mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation

Determine If Statement: SA-11 (a) - The organization requires the developer of the information system, system component, or information system service to create and implement a security plan.

Result: Not Assessed

Determine If Statement: SA-11 (b)[01] - The organization defines the depth of testing/evaluation to be performed by the developer of the information system, system component, or information system service.

Result: Not Assessed

Determine If Statement: SA-11 (b)[02] - The organization defines the coverage of testing/evaluation to be performed by the developer of the information system, system component, or information system service.

Result: Not Assessed

Determine If Statement: SA-11 (b)[03] - The organization requires the developer of the information system, system component, or information system service to perform one or more of the following testing/evaluation at the organization-defined depth and coverage:
* unit testing/evaluation;
* integration testing/evaluation;
* system testing/evaluation; and/or
* regression testing/evaluation.

Result: Not Assessed

Determine If Statement: SA-11 (c)[01] - The organization requires the developer of the information system, system component, or information system service to produce evidence of the execution of the security assessment plan.

Result: Not Assessed

Determine If Statement: SA-11 (c)[02] - The organization requires the developer of the information system, system component, or information system service to produce evidence of the results of the security testing/evaluation.

Result: Not Assessed

Determine If Statement: SA-11 (d) - The organization requires the developer of the information system, system component, or information system service to implement a verifiable flaw remediation process.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SA-11 (e) - The organization requires the developer of the information system, system component, or information system service to correct flaws identified during security testing/evaluation.

Result: Not Assessed

Control Title: SC-01 -System And Communications Protection Policy And Procedures

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:

a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:

1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates the current:

1. System and communications protection policy [%Assignment: organization-defined frequency (b)(1)%]; and

2. System and communications protection procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: HUD IT security policy (inclusive of system and communications protection) is formally documented in Sections 1.1 (purpose), 1.2 (scope), 2.0 (roles and responsibilities), and 2.1 – 2.12 (management commitment and coordination among organizational entities) of the HUD Information Technology Security Policy, HUD Handbook 2400.25, Rev 2.0 April 2007. System and communications protection compliance policy is specifically addressed in Sections 5.4 (and associated sub-sections) and 5.5 (and associated sub-sections) of this handbook. Procedures to facilitate implementation of this policy are formally documented in Section 5.4 (and associated sub-sections) of the HUD Information Technology Security Procedures, Version 1.4, June 9, 2006. A softcopy of both the Policy handbook and the Procedures reside on the HUD website http://hudatwork.hud.gov and are accessible by all HUD employees and contractors. Both the Policy and the Procedures document are reviewed, and updated as required, as part of the CIO's annual Information Security Program evaluation.
This is a common control, the implementation of which is the responsibility of the HUD Office of IT Security.

Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented system and communications protection policy within Section 5.4. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to system and communications protection.
The system and communications protection policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The system and communications protection procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection security controls are documented within the Section 5.4 of the Information Technology Security Procedures, dated November 1, 2013.
The system and communications protection procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: SC-1 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and communications protection policy and procedures
* Other relevant documents or records

Interview

* Organizational personnel with system and communications protection responsibilities
* Organizational personnel with information security responsibilities

Determine If Statement: SC-01 (a)(01)[01] - The organization develops and documents a system and communications protection policy that addresses:

* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SC-01 (a)(01)[02] - The organization defines personnel or roles to whom the system and communications protection policy is to be disseminated.

Result: Not Assessed

Determine If Statement: SC-01 (a)(01)[03] - The organization disseminates the system and communications protection policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SC-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SC-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Not Assessed

Determine If Statement: SC-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SC-01 (b)(01)[01] - The organization defines the frequency to review and update the current system and communications protection policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SC-01 (b)(01)[02] - The organization reviews and updates the current system and communications protection policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SC-01 (b)(02)[01] - The organization defines the frequency to review and update the current system and communications protection procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SC-01 (b)(02)[02] - The organization reviews and updates the current system and communications protection procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Control Title: SC-02 -Application Partitioning

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system separates user functionality (including user interface services) from information system management functionality.

Implementation Statement: The information system separates user functionality (including user interface services) from information system management functionality. User access to functionality and access level (view, update, add, delete) is determined by assigned WASS role(s) and/or action(s). The application layer is separate from the database data management server.

Assessment Objective: SC-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* System and communications protection policy
* Procedures addressing application partitioning
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developer

Test
* Separation of user functionality from information system management functionality

Determine If Statement: SC-02 - The information system separates user functionality (including user interface services) from information system management functionality.

Result: Not Assessed

Control Title: SC-04 -Information In Shared Resources

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The information system prevents unauthorized and unintended information transfer via shared system resources.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**

z/OS provides explicit object reuse functionality for the following objects, and z/OS ensures that these objects are prepared for reuse before they are allocated to another subject:

● Memory objects are filled with zeros before they are allocated for the first time to a subject {OR.1::OR.1.1}.

● z/OS data sets are erased when the data is released when the erase-on-scratch option is active {OR.1::OR.1.2}.

● z/OS system log streams that reside in z/OS data sets are cleared by the system logger before it writes any data into them. Similarly, for z/OS log stream data residing in a coupling facility the system logger clears the structure data in the coupling facility before writing any data into the structure {OR.1::OR.1-R9-LOGGER-1}.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

z/OS tape volumes are erased when they are returned to the scratch pool by appropriately configuring the SECCLS parmlib option for the parmlib member EDGRMMxx {OR.1::OR.1-R8-RMM-1} or under control of the appropriate data set profile's ERASE option when TAPEAUTHDSN=YES is specified in SYS1.PARMLIB(DEVSUPxx) {OR.1::OR.1-R8-RMM-2}.
● z/OS UNIX file system objects and z/OS UNIX IPC objects are cleared before they are made accessible to a new subject (for zFS files, this requires that the zFS IOEFSPRM parameter file has the NBS option defaulted or set to enabled, and that any mount commands or multi-file-system aggregates also have the NBS option set) {OR.1::OR.1.3}.
● LDAP LDBM objects are not specifically cleared when they are deleted, but LDAP does ensure that any data returned from an object is not residual data from some previous object that may have occupied the same physical space in the LDBM database {OR.1::OR.1-R8-LDAP-1}.

Assessment Objective: SC-4 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and communications protection policy
* Procedures addressing information protection in shared system resources
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developer

Test
* Automated mechanisms preventing unauthorized and unintended transfer of information via shared system resources

Determine If Statement: SC-04 - The information system prevents unauthorized and unintended information transfer via shared system resources.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SC-05 -Denial Of Service Protection

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The information system protects against or limits the effects of the following types of denial of service attacks: [%Assignment: organization-defined types of denial of service attacks or reference to source for such information%] by employing [%Assignment: organization-defined security safeguards%].

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**

Denial of Service protection for the GSS is implemented through the boundary firewalls. Denial of Service protection for the GSS is managed, administered, and secured by firewalls and monitored by IDS sensors. These sensors are strategically located at all possible external boundaries and key internal boundaries within the HUD intra-network.

Assessment Objective: SC-5 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and communications protection policy
* Procedures addressing denial of service protection
* Information system design documentation
* Security plan
* List of denial of services attacks requiring employment of security safeguards to protect against or limit effects of such attacks
* List of security safeguards protecting against or limiting the effects of denial of service attacks
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel with incident response responsibilities
* System developer

Test

* Automated mechanisms protecting against or limiting the effects of denial of service attacks

Determine If Statement: SC-05 [01] - The organization defines types of denial of service attacks or reference to source of such information for the information system to protect against or limit the effects.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-05 [02] - The organization defines security safeguards to be employed by the information system to protect against or limit the effects of organization-defined types of denial of service attacks.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-05 [03] - The information system protects against or limits the effects of the organization-defined denial or service attacks (or reference to source for such information) by employing organization-defined security safeguards.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SC-07 -Boundary Protection

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The information system:
a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
b. Implements subnetworks for publicly accessible system components that are [%Selection: physically; logically%] separated from internal organizational networks; and
c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
External communications are controlled by boundary firewalls and monitored by IDS sensors. External connections are only made through managed interfaces in accordance with HUD security architecture. Boundary protection for the GSS is managed, administered, and secured by firewalls and monitored by IDS sensors, which are LAN/WAN GSS components and which are strategically located at all possible external boundaries and key internal boundaries within the HUD intra-network.

Assessment Objective: SC-7 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* System and communications protection policy
* Procedures addressing boundary protection
* List of key internal boundaries of the information system
* Information system design documentation
* Boundary protection hardware and software
* Information system configuration settings and associated documentation
* Enterprise security architecture documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developer
* Organizational personnel with boundary protection responsibilities

Test
* Automated mechanisms implementing boundary protection capability

Determine If Statement: SC-07 (a)[01] - The information system monitors communications at the external boundary of the information system.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-07 (a)[02] - The information system monitors communications at key internal boundaries within the system.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-07 (a)[03] - The information system controls communications at the external boundary of the information system.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-07 (a)[04] - The information system controls communications at key internal boundaries within the system.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-07 (b) - The information system implements subnetworks for publicly accessible system components that are either:
* physically separated from internal organizational networks; and/or
* logically separated from internal organizational networks.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-07 (c) - The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SC-07(3) -Access Points

Applicability: Fully Inherited **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization limits the number of external network connections to the information system.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
HUD limits the number of access points to those approved per HUD policy to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

Assessment Objective: SC-7(3) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and communications protection policy
* Procedures addressing boundary protection
* Information system design documentation
* Boundary protection hardware and software
* Information system architecture and configuration documentation
* Information system configuration settings and associated documentation
* Communications and network traffic monitoring logs
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel with boundary protection responsibilities

Test
* Automated mechanisms implementing boundary protection capability
* Automated mechanisms limiting the number of external network connections to the information system

Determine If Statement: SC-07(03) - The organization limits the number of external network connections to the information system.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SC-07(4) -External Telecommunications Services
Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization:
(a) Implements a managed interface for each external telecommunication service;
(b) Establishes a traffic flow policy for each managed interface;
(c) Protects the confidentiality and integrity of the information being transmitted across each interface;
(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
(e) Reviews exceptions to the traffic flow policy [%Assignment: organization-defined frequency%] and removes exceptions that are no longer supported by an explicit mission/business need.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
Each telecommunication service is connected through a managed interface. Traffic flow policies are established based on business need at the time of the connection request through a service desk ticket. There are currently no excetions to traffic flow policies. Exception requests will be processed in accordance with HUD policy. Boundary protection for the HUD intra-network is managed, administered, and secured by internal and external firewalls (components of the LAN GSS and WAN GSS, respectively), which restrict traffic at every access point and, in most instances, encrypt inbound and outbound data transfer. All possible remote access entry points are monitored continually by IDS sensors. The firewall restrictions at the access point are performed annually. Exceptions that are no longer needed to support a mission/business need are removed. All external communications come in either via point-to-point VPNs or transit the firewall.

Assessment Objective: SC-7(4) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and communications protection policy
* Traffic flow policy
* Information flow control policy
* Procedures addressing boundary protection
* Information system security architecture
* Information system design documentation
* Boundary protection hardware and software
* Information system architecture and configuration documentation
* Information system configuration settings and associated documentation
* Records of traffic flow policy exceptions
* Information system audit records
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel with boundary protection responsibilities

Test

* Organizational processes for documenting and reviewing exceptions to the traffic flow policy
* Organizational processes for removing exceptions to the traffic flow policy
* Automated mechanisms implementing boundary protection capability
* Managed interfaces implementing traffic flow policy

Determine If Statement: SC-07(04) (a) - The organization implements a managed interface for each external telecommunication service.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-07(04) (b) - The organization establishes a traffic flow policy for each managed interface.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-07(04) (c) - The organization protects the confidentiality and integrity of the information being transmitted across each interface.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-07(04) (d) - The organization documents each exception to the traffic flow policy with:
* a supporting mission/business need;
* duration of that need.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-07(04) (e)[01] - The organization defines a frequency to review exceptions to traffic flow policy.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-07(04) (e)[02] - The organization reviews exceptions to the traffic flow policy with the organization-defined frequency.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SC-07(04) (e)[03] - The organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SC-07(5) -Deny By Default / Allow By Exception

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
All firewalls implement a deny-all by default policy. Boundary protection for the GSS is managed, administered, and secured by internal and external firewalls, which are components of the LAN GSS and WAN GSS, respectively. Firewalls are configured to deny network traffic by default and allow it by exception.

Assessment Objective: SC-7(5) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and communications protection policy
* Procedures addressing boundary protection
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developer
* Organizational personnel with boundary protection responsibilities

Test
* Automated mechanisms implementing traffic management at managed interfaces

Determine If Statement: SC-07(05) [01] - The information system, at managed interfaces denies network traffic by default.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-07(05) [02] - The information system, at managed interfaces allows network traffic by exception.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SC-07(7) -Prevent Split Tunneling For Remote Devices

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors & System Owners of Major Applications.

Assessment Objective: SC-7(7) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:
Examine
* System and communications protection policy
* Procedures addressing boundary protection
* Information system design documentation
* Information system hardware and software
* Information system architecture
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developer
* Organizational personnel with boundary protection responsibilities

Test
* Automated mechanisms implementing boundary protection capability
* Automated mechanisms supporting/restricting non-remote connections

Determine If Statement: SC-07(07) - The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

Result: Not Assessed

Control Title: SC-08 -Transmission Confidentiality And Integrity

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The information system protects the [%Selection (one or more): confidentiality; integrity%] of transmitted information.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
Information is transmitted to and from the IBM over internal or dedicated networks. The IBM Mainframe transmits information via Transmission Control Protocol which provides for data integrity.

Assessment Objective: SC-8 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and communications protection policy
* Procedures addressing transmission confidentiality and integrity
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developer

Test
* Automated mechanisms supporting and/or implementing transmission confidentiality and/or integrity

Determine If Statement: SC-08 - The information system protects one or more of the following:
* confidentiality of transmitted information; and/or
* integrity of transmitted information.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SC-08(1) -Cryptographic Or Alternate Physical Protection

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The information system implements cryptographic mechanisms to [%Selection (one or more): prevent unauthorized disclosure of information; detect changes to information%] during transmission unless otherwise protected by [%Assignment: organization-defined alternative physical safeguards%].

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
SSL encryption and Secure File Transfer Protocol are employed where appropriate to protect the integrity of transmitted information. In addition, the transmission lines are protected by physical measures as documented within the PE security controls.

Assessment Objective: SC-8(1) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and communications protection policy
* Procedures addressing transmission confidentiality and integrity
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developer

Test
* Cryptographic mechanisms supporting and/or implementing transmission confidentiality and/or integrity
* Automated mechanisms supporting and/or implementing alternative physical safeguards
* Organizational processes for defining and implementing alternative physical safeguards

Determine If Statement: SC-08(01) [01] - The organization defines physical safeguards to be implemented to protect information during transmission when cryptographic mechanisms are not implemented.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-08(01) [02] - The information system implements cryptographic mechanisms to do one or more of the following during transmission unless otherwise protected by organization-defined alternative physical safeguards:
* prevent unauthorized disclosure of information; and/or
* detect changes to information.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SC-10 -Network Disconnect

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The information system terminates the network connection associated with a communications session at the end of the session or after [%Assignment: organization-defined time period%] of inactivity.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
Sessions are terminated after 10 minutes of inactivity in accordance with HUD Policy.

Assessment Objective: SC-10 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:
Examine
* System and communications protection policy
* Procedures addressing network disconnect
* Information system design documentation
* Security plan
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records
Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developer
Test
* Automated mechanisms supporting and/or implementing network disconnect capability

Determine If Statement: SC-10 [01] - The organization defines a time period of inactivity after which the information system terminates a network connection associated with a communications session.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SC-10 [02] - The information system terminates the network connection associated with a communication session at the end of the session or after the organization-defined time period of inactivity.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SC-12 -Cryptographic Key Establishment And Management

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [%Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction%].

Implementation Statement: Cryptography is not used in TRACS.

Implementation Statement for **P207 - Mainframe (IBM)**
Cryptographic keys are generated and managed by the IBM mainframe internally.

Assessment Objective: SC-12 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and communications protection policy
* Procedures addressing cryptographic key establishment and management
* Information system design documentation
* Cryptographic mechanisms
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records
Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel with responsibilities for cryptographic key establishment and/or management
Test
* Automated mechanisms supporting and/or implementing cryptographic key establishment and management

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SC-12 [01] - The organization defines requirements for cryptographic key:
* generation;
* distribution;
* storage;
* access;
* destruction.

Result: Not Assessed

Determine If Statement: SC-12 [02] - The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation, distribution, storage, access, and destruction.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SC-13 -Cryptographic Protection

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system implements [%Assignment: organization-defined cryptographic uses and type of cryptography required for each use%] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Implementation Statement: Cryptography is not used in TRACS.

Assessment Objective: SC-13 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* System and communications protection policy
* Procedures addressing cryptographic protection
* Information system design documentation
* Information system configuration settings and associated documentation
* Cryptographic module validation certificates
* List of FIPS validated cryptographic modules
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developer
* Organizational personnel with responsibilities for cryptographic protection

Test
* Automated mechanisms supporting and/or implementing cryptographic protection

Determine If Statement: SC-13 [01] - The organization defines cryptographic uses.

Result: Not Assessed

Determine If Statement: SC-13 [02] - The organization defines the type of cryptography required for each use.

Result: Not Assessed

Determine If Statement: SC-13 [03] - The information system implements the organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Result: Not Assessed

Control Title: SC-15 -Collaborative Computing Devices

Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The information system:
a. Prohibits remote activation of collaborative computing devices with the following exceptions: [%Assignment: organization-defined exceptions where remote activation is to be allowed%]; and
b. Provides an explicit indication of use to users physically present at the devices.

Implementation Statement: There is no collaborative computing allowed for this system.

Assessment Objective: SC-15 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* System and communications protection policy
* Procedures addressing collaborative computing
* Access control policy and procedures
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developer
* Organizational personnel with responsibilities for managing collaborative computing devices

Test
* Automated mechanisms supporting and/or implementing management of remote activation of collaborative computing devices
* Automated mechanisms providing an indication of use of collaborative computing devices

Determine If Statement: SC-15 (a)[01] - The organization defines exceptions where remote activation of collaborative computing devices is to be allowed.

Result: Not Assessed

Determine If Statement: SC-15 (a)[02] - The information system prohibits remote activation of collaborative computing devices, except for organization-defined exceptions where remote activation is to be allowed.

Result: Not Assessed

Determine If Statement: SC-15 (b) - The information system provides an explicit indication of use to users physically present at the devices.

Result: Not Assessed

Control Title: SC-17 -Public Key Infrastructure Certificates

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization issues public key certificates under an [%Assignment: organization-defined certificate policy%] or obtains public key certificates from an approved service provider.

Implementation Statement: The infrastructure support organization defines a certificate policy for issuing public key certificates.

Assessment Objective: SC-17 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and communications protection policy
* Procedures addressing public key infrastructure certificates
* Public key certificate policy or policies
* Public key issuing process
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel with responsibilities for issuing public key certificates
* Service providers

Test

* Automated mechanisms supporting and/or implementing the management of public key infrastructure certificates

Determine If Statement: SC-17 [01] - The organization defines a certificate policy for issuing public key certificates.
Result: Not Assessed

Determine If Statement: SC-17 [02] - The organization issues public key certificates:
* under an organization-defined certificate policy: or
* obtains public key certificates from an approved service provider.

Result: Not Assessed

Control Title: SC-18 -Mobile Code
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

Implementation Statement: The organization defines acceptable and unacceptable mobile code and mobile code technologies.

Assessment Objective: SC-18 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* System and communications protection policy
* Procedures addressing mobile code
* Mobile code usage restrictions, mobile code implementation policy and procedures
* List of acceptable mobile code and mobile code technologies
* List of unacceptable mobile code and mobile technologies
* Authorization records
* Information system monitoring records
* Information system audit records
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel with responsibilities for managing mobile code

Test

* Organizational process for controlling, authorizing, monitoring, and restricting mobile code
* Automated mechanisms supporting and/or implementing the management of mobile code
* Automated mechanisms supporting and/or implementing the monitoring of mobile code

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SC-18 (a) - The organization defines acceptable and unacceptable mobile code and mobile code technologies.
Result: Not Assessed

Determine If Statement: SC-18 (b)[01] - The organization establishes usage restrictions for acceptable mobile code and mobile code technologies.
Result: Not Assessed

Determine If Statement: SC-18 (b)[02] - The organization establishes implementation guidance for acceptable mobile code and mobile code technologies.
Result: Not Assessed

Determine If Statement: SC-18 (c)[01] - The organization authorizes the use of mobile code within the information system.
Result: Not Assessed

Determine If Statement: SC-18 (c)[02] - The organization monitors the use of mobile code within the information system.
Result: Not Assessed

Determine If Statement: SC-18 (c)[03] - The organization controls the use of mobile code within the information system.
Result: Not Assessed

Control Title: SC-19 -Voice Over Internet Protocol
Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
b. Authorizes, monitors, and controls the use of VoIP within the information system.

Implementation Statement: Voice over Internet Protocol is not used in the TRACS system.

Assessment Objective: SC-19 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and communications protection policy
* Procedures addressing VoIP
* VoIP usage restrictions
* VoIP implementation guidance
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system monitoring records
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel with responsibilities for managing VoIP

Test
* Organizational process for authorizing, monitoring, and controlling VoIP
* Automated mechanisms supporting and/or implementing authorizing, monitoring, and controlling VoIP

Determine If Statement: SC-19 (a) - The organization
* establishes usage restrictions for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously;
* establishes implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SC-19 (b)[01] - The organization authorizes the use of VoIP within the information system.
Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac
Result: **Assessed by:** **Date:**

Determine If Statement: SC-19 (b)[02] - The organization monitors the use of VoIP within the information system.
Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac
Result: **Assessed by:** **Date:**

Determine If Statement: SC-19 (b)[03] - The organization controls the use of VoIP within the information system.
Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac
Result: **Assessed by:** **Date:**

Control Title: SC-20 -Secure Name / Address Resolution Service (Authoritative Source)
Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The information system:
a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Assessment Objective: SC-20 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and communications protection policy
* Procedures addressing secure name/address resolution service (authoritative source)
* Information system design documentation
* Information system configuration settings and associated documentation
* Other relevant documents or records
Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel with responsibilities for managing DNS
Test
* Automated mechanisms supporting and/or implementing secure name/address resolution service

Determine If Statement: SC-20 (a) - The information system provides additional data origin and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.

Inherited From: [Externally Inherited] TRACS
Result: **Assessed by:** **Date:**

Determine If Statement: SC-20 (b)[01] - The information system provides the means to, when operating as part of a distributed, hierarchical namespace indicate the security status of child zones.
Inherited From: [Externally Inherited] TRACS
Result: **Assessed by:** **Date:**

Determine If Statement: SC-20 (b)[02] - The information system provides the means to, when operating as part of a distributed, hierarchical namespace enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).
Inherited From: [Externally Inherited] TRACS
Result: **Assessed by:** **Date:**

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: SC-21 -Secure Name / Address Resolution Service (Recursive Or Caching Resolver)
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Implementation Statement: TRACS information system performs data integrity verification on the monthly entries the system receives from trusted business sources. TRACS uses https: secured sockets protocol where users sign in with an assigned user id.

Assessment Objective: SC-21 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and communications protection policy
* Procedures addressing secure name/address resolution service (recursive or caching resolver)
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel with responsibilities for managing DNS

Test
* Automated mechanisms supporting and/or implementing data origin authentication and data integrity verification for name/address resolution services

Determine If Statement: SC-21 [01] - The information system requests data origin authentication on the name/address resolution responses the system receives from authoritative sources.
Result: Not Assessed

Determine If Statement: SC-21 [02] - The information system requests data integrity verification on the name/address resolution responses the system receives from authoritative sources.
Result: Not Assessed

Determine If Statement: SC-21 [03] - The information system performs data origin authentication on the name/address resolution responses the system receives from authoritative sources.
Result: Not Assessed

Determine If Statement: SC-21 [04] - The information system performs data integrity verification on the name/address resolution responses the system receives from authoritative sources.
Result: Not Assessed

Control Title: SC-22 -Architecture And Provisioning For Name / Address Resolution Service
Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Assessment Objective: SC-22 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and communications protection policy
* Procedures addressing architecture and provisioning for name/address resolution service
* Access control policy and procedures
* Information system design documentation
* Assessment results from independent, testing organizations
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel with responsibilities for managing DNS

Test

* Automated mechanisms supporting and/or implementing name/address resolution service for fault tolerance and role separation

Determine If Statement: SC-22 [01] - The information systems that collectively provide name/address resolution service for an organization are fault tolerant.

Inherited From: [Externally Inherited] TRACS

Result: **Assessed by:** **Date:**

Determine If Statement: SC-22 [02] - The information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.

Inherited From: [Externally Inherited] TRACS

Result: **Assessed by:** **Date:**

Control Title: SC-23 -Session Authenticity

Applicability: Fully Inherited **Result:** Implemented

Control Requirement: The information system protects the authenticity of communications sessions.

Assessment Objective: SC-23 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* System and communications protection policy
* Procedures addressing session authenticity
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities

Test

* Automated mechanisms supporting and/or implementing session authenticity

Determine If Statement: SC-23 - The information system protects the authenticity of communications sessions.

Inherited From: [Externally Inherited] TRACS

Result: **Assessed by:** **Date:**

Control Title: SC-28 -Protection Of Information At Rest

Applicability: Hybrid **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The information system protects the [%Selection (one or more): confidentiality; integrity%] of [%Assignment: organization-defined information at rest%].

Implementation Statement: The information system does protect the confidentiality and integrity of information at rest.

Implementation Statement for **P207 - Mainframe (IBM)**
Physical access controls as implemented per PE-3 protect the confidentiality and integrity of information at rest on DASD disk drives.

Assessment Objective: SC-28 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and communications protection policy
* Procedures addressing protection of information at rest
* Information system design documentation
* Information system configuration settings and associated documentation
* Cryptographic mechanisms and associated configuration documentation
* List of information at rest requiring confidentiality and integrity protections
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developer

Test
* Automated mechanisms supporting and/or implementing confidentiality and integrity protections for information at rest

Determine If Statement: SC-28 [01] - The organization defines information at rest requiring one or more of the following:
* confidentiality protection; and/or
* integrity protection.

Result: Not Assessed

Determine If Statement: SC-28 [02] - The information system protects the:
* confidentiality of organization-defined information at rest; and/or
* integrity of organization-defined information at rest.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SC-32 -Information System Partitioning

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization partitions the information system into [%Assignment: organization-defined information system components%] residing in separate physical domains or environments based on [%Assignment: organization-defined circumstances for physical separation of components%].

Assessment Objective: SC-32 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and communications protection policy
* Procedures addressing information system partitioning
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system architecture
* List of information system physical domains (or environments)
* Information system facility diagrams
* Information system network diagrams
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel installing, configuring, and/or maintaining the information system
* Information system developers/integrators

Test

* Automated mechanisms supporting and/or implementing physical separation of information system components

Determine If Statement: SC-32 [01] - The organization defines circumstances for physical separation of information system components into information system partitions.

Result: NA-RTM **Assessed by:** **Date:**

Determine If Statement: SC-32 [02] - The organization defines information system components to reside in separate physical domains or environments based on organization-defined circumstances for physical separation of components.

Result: NA-RTM **Assessed by:** **Date:**

Determine If Statement: SC-32 [03] - The organization partitions the information system into organization-defined information system components residing in separate physical domains or environments based on organization-defined circumstances for physical separation of components.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SC-39 -Process Isolation

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system maintains a separate execution domain for each executing process.

Implementation Statement: The information system maintains a separate execution domain for each executing process, like tenant and voucher and manual voucher.

Assessment Objective: SC-39 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* Information system design documentation
* Information system architecture
* Independent verification and validation documentation
* Testing and evaluation documentation, other relevant documents or records

Interview

* Information system developers/integrators
* Information system security architect

Test

* Automated mechanisms supporting and/or implementing separate execution domains for each executing process

Determine If Statement: SC-39 - The information system maintains a separate execution domain for each executing process.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: SE-01 -Inventory Of Personally Identifiable Information
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Establishes, maintains, and updates [%Assignment: organization-defined frequency (a)%] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and
b. Provides each update of the PII inventory to the CIO or information security official [%Assignment: organization-defined frequency (b)%] to support the establishment of information security requirements for all new or modified information systems containing PII.

Implementation Statement: The organization establishes, maintains, and updates as needed an inventory of databases collecting or using personally identifiable information (PII); and updates the PII inventory with MFDCS to support information security requirements for new PII.

Assessment Objective: SE-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Inventory of programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII).
* Updates provided to CIO on inventory of programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII).
Interview
* Organizational personnel with privacy review responsibilities. [note: interview OCIO].
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and OCIO].

Determine If Statement: SE-01 (a) - The organization (1) Defines frequency of updating inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); (2) Establishes, maintains, and updates with organization-defined frequency an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

Result: Not Assessed

Determine If Statement: SE-01 (b) - The organization (1) Defines frequency of providing update to CIO of its PII inventory; (2) Provides each update of the PII inventory to the CIO or information security official with organization-defined frequency to support the establishment of information security requirements for all new or modified information systems containing PII.

Result: Not Assessed

Control Title: SE-02 -Privacy Incident Response
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Develops and implements a Privacy Incident Response Plan; and
b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

Implementation Statement: HUD develops and implements a Privacy Incident Response Plan; and provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan. The HUD Privacy Officer assures that service and service arrangement meet privacy policies regarding the protection, dissemination, and disclosure of information. The organization conducts a privacy impact assessment (PIA) on the information system in accordance with OMB policy. Related HUD Policy: 3.2.5

Assessment Objective: SE-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Department policy and procedures.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview CPLCO/OPCL and OCIO].

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SE-02 (a) - The organization develops and implements a Privacy Incident Response Plan.
Result: Not Assessed

Determine If Statement: SE-02 (b) - The organization provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.
Result: Not Assessed

Control Title: SI-01 -System And Information Integrity Policy And Procedures
Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The organization:
a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:
1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
b. Reviews and updates the current:
1. System and information integrity policy [%Assignment: organization-defined frequency (b)(1)%]; and
2. System and information integrity procedures [%Assignment: organization-defined frequency (b)(2)%].

Implementation Statement: This is a hybrid common control, the implementation of which is the responsibility of the HUD Office of IT Security.

Implementation Statement for **Develop IT Security Standards and Policy**
HUD developed the HUD Handbook 2400.25 REV-3, Information Technology Security Policy, dated August 30, 2013. The HUD Handbook 2400.25 contains a formal documented system and information integrity policy within Section 4.6. Additionally, within the HUD Handbook 2400.25 contains the roles and responsibilities, and management commitment. Furthermore, Section 1.0 contains management commitment, coordination amongst HUD entities, and compliance with the policy pertaining to system and information integrity.
The system and information integrity policy contained within the HUD Handbook 2400.25 is disseminated amongst HUD employees and contractors via the following
link http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/hudclips/handbooks/cio/2400.25 on the HUD Intranet portal.
The system and information integrity procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity security controls are documented within the Section 4.6 of the Information Technology Security Procedures, dated November 1, 2013.
The system and information integrity procedures contained within the Information Technology Security Procedures are disseminated amongst HUD employees and contractors via the following
link http://hudatwork.hud.gov/po/i/it/security/secure.cfm on the HUD Intranet portal.
The HUD Office of Information Technology Security (OITS) reviews/updates the HUD Handbook 2400.25 and the Information Technology Security Procedures on an annual basis or whenever there is a significant change.

Assessment Objective: SI-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and information integrity policy and procedures
* Other relevant documents or records
Interview
* Organizational personnel with system and information integrity responsibilities
* Organizational personnel with information security responsibilities

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SI-01 (a)(01)[01] - The organization develops and documents a system and information integrity policy that addresses:
* purpose;
* scope;
* roles;
* responsibilities;
* management commitment;
* coordination among organizational entities;
* compliance.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SI-01 (a)(01)[02] - The organization defines personnel or roles to whom the system and information integrity policy is to be disseminated.

Result: Not Assessed

Determine If Statement: SI-01 (a)(01)[03] - The organization disseminates the system and information integrity policy to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SI-01 (a)(02)[01] - The organization develops and documents procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SI-01 (a)(02)[02] - The organization defines personnel or roles to whom the procedures are to be disseminated.

Result: Not Assessed

Determine If Statement: SI-01 (a)(02)[03] - The organization disseminates the procedures to organization-defined personnel or roles.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SI-01 (b)(01)[01] - The organization defines the frequency to review and update the current system and information integrity policy.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SI-01 (b)(01)[02] - The organization reviews and updates the current system and information integrity policy with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SI-01 (b)(02)[01] - The organization defines the frequency to review and update the current system and information integrity procedures.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Determine If Statement: SI-01 (b)(02)[02] - The organization reviews and updates the current system and information integrity procedures with the organization-defined frequency.

Inherited From: Develop IT Security Standards and Policy

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Title: SI-02 -Flaw Remediation
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within [%Assignment: organization-defined time period%] of the release of the updates; and
d. Incorporates flaw remediation into the organizational configuration management process.

Implementation Statement: TRACS: a. Identifies, reports, and corrects flaws; b. Tests software updates for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process.
This is a common control, the implementation of which is the responsibility of HITS Contractors & System Owners of Major Applications. Data updates occur daily (mainframe) or weekly (server) as needed/requested. Corrective releases are scheduled quarterly, as needed. The application's flow control takes users from one page to the next. In addition, the front end includes edits, pop-up error messages, and HTML web controls.

Assessment Objective: SI-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and information integrity policy
* Procedures addressing flaw remediation
* Procedures addressing configuration management
* List of flaws and vulnerabilities potentially affecting the information system
* List of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws)
* Test results from the installation of software and firmware updates to correct information system flaws
* Installation/change control records for security-relevant software and firmware updates
* Other relevant documents or records
Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel installing, configuring, and/or maintaining the information system
* Organizational personnel with responsibility for flaw remediation
* Organizational personnel with configuration management responsibility
Test
* Organizational processes for identifying, reporting, and correcting information system flaws
* Organizational process for installing software and firmware updates
* Automated mechanisms supporting and/or implementing reporting, and correcting information system flaws
* Automated mechanisms supporting and/or implementing testing software and firmware updates

Determine If Statement: SI-02 (a)[01] - The organization identifies information system flaws.
Result: Not Assessed

Determine If Statement: SI-02 (a)[02] - The organization reports information system flaws.
Result: Not Assessed

Determine If Statement: SI-02 (a)[03] - The organization corrects information system flaws.
Result: Not Assessed

Determine If Statement: SI-02 (b)[01] - The organization tests software updates related to flaw remediation for effectiveness and potential side effects before installation.
Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SI-02 (b)[02] - The organization tests firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

Result: Not Assessed

Determine If Statement: SI-02 (c)[01] - The organization defines the time period within which to install security-relevant software updates after the release of the updates.

Result: Not Assessed

Determine If Statement: SI-02 (c)[02] - The organization defines the time period within which to install security-relevant firmware updates after the release of the updates.

Result: Not Assessed

Determine If Statement: SI-02 (c)[03] - The organization installs software updates within the organization-defined time period of the release of the updates.

Result: Not Assessed

Determine If Statement: SI-02 (c)[04] - The organization installs firmware updates within the organization-defined time period of the release of the updates.

Result: Not Assessed

Determine If Statement: SI-02 (d) - The organization incorporates flaw remediation into the organizational configuration management process.

Result: Not Assessed

Control Title: SI-02(2) -Automated Flaw Remediation Status

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization employs automated mechanisms [%Assignment: organization-defined frequency%] to determine the state of information system components with regard to flaw remediation.

Implementation Statement: The organization employs automated mechanisms organization defined set of users and resources to determine the state of information system components with regard to flaw remediation.

Assessment Objective: SI-2(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* System and information integrity policy
* Procedures addressing flaw remediation
* Automated mechanisms supporting centralized management of flaw remediation
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel installing, configuring, and/or maintaining the information system
* Organizational personnel with responsibility for flaw remediation

Test
* Automated mechanisms used to determine the state of information system components with regard to flaw remediation

Determine If Statement: SI-02(02) [01] - The organization defines a frequency to employ automated mechanisms to determine the state of information system components with regard to flaw remediation.

Result: Not Assessed

Determine If Statement: SI-02(02) [02] - The organization employs automated mechanisms with the organization-defined frequency to determine the state of information system components with regard to flaw remediation.

Result: Not Assessed

Control Title: SI-03 -Malicious Code Protection

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
1. Perform periodic scans of the information system [%Assignment: organization-defined frequency%] and real-time scans of files from external sources at [%Selection (one or more); endpoint; network entry/exit points%] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
2. [%Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]%] in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Implementation Statement: The organization employs malicious code protection mechanisms and provides updates whenever new releases are available.
SI-3: This is inherited - contractors use NESSUS for vulnerability scans. To address, TRACS implemented server side scripting to prevent cross-site XSS attacks. Additionally, system access is restricted to authorized users. System modifications must be tested by the users and tested by the HUD test center before implementation. Actual production access is restricted to the HITS team.

Assessment Objective: SI-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and information integrity policy
* Configuration management policy and procedures
* Procedures addressing malicious code protection
* Malicious code protection mechanisms
* Records of malicious code protection updates
* Information system design documentation
* Information system configuration settings and associated documentation
* Scan results from malicious code protection mechanisms
* Record of actions initiated by malicious code protection mechanisms in response to malicious code detection
* Information system audit records
* Other relevant documents or records
Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel installing, configuring, and/or maintaining the information system
* Organizational personnel with responsibility for malicious code protection
* Organizational personnel with configuration management responsibility
Test
* Organizational processes for employing, updating, and configuring malicious code protection mechanisms
* Organizational process for addressing false positives and resulting potential impact
* Automated mechanisms supporting and/or implementing employing, updating, and configuring malicious code protection mechanisms
* Automated mechanisms supporting and/or implementing malicious code scanning and subsequent actions

Determine If Statement: SI-03 (a)[01] - The organization employs malicious code protection mechanisms to detect and eradicate malicious code at information system entry points.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SI-03 (a)[02] - The organization employs malicious code protection mechanisms to detect and eradicate malicious code at information system exit points.

Result: Not Assessed

Determine If Statement: SI-03 (b) - The organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures (as identified in CM-1).

Result: Not Assessed

Determine If Statement: SI-03 (c)[01] - The organization defines a frequency for malicious code protection mechanisms to perform periodic scans of the information system.

Result: Not Assessed

Determine If Statement: SI-03 (c)[02] - The organization defines action to be initiated by malicious protection mechanisms in response to malicious code detection.

Result: Not Assessed

Determine If Statement: SI-03 (c)[03](01)[a] - The organization configures malicious code protection mechanisms to perform periodic scans of the information system with the organization-defined frequency.

Result: Not Assessed

Determine If Statement: SI-03 (c)[03](01)[b] - The organization configures malicious code protection mechanisms to perform real-time scans of files from external sources at endpoint and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy.

Result: Not Assessed

Determine If Statement: SI-03 (c)[03](02) - The organization configures malicious code protection mechanisms to do one or more of the following:
* block malicious code in response to malicious code detection;
* quarantine malicious code in response to malicious code detection;
* send alert to administrator in response to malicious code detection; and/or
* initiate organization-defined action in response to malicious code detection.

Result: Not Assessed

Determine If Statement: SI-03 (d)[01] - The organization addresses the receipt of false positives during malicious code detection and eradication.

Result: Not Assessed

Determine If Statement: SI-03 (d)[02] - The organization addresses the resulting potential impact on the availability of the information system.

Result: Not Assessed

Control Title: SI-03(1) -Central Management

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization centrally manages malicious code protection mechanisms.

Implementation Statement: The organization centrally manages malicious code protection mechanisms.

Assessment Objective: SI-3(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and information integrity policy
* Procedures addressing malicious code protection
* Automated mechanisms supporting centralized management of malicious code protection mechanisms
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel installing, configuring, and/or maintaining the information system
* Organizational personnel with responsibility for malicious code protection

Test

* Organizational processes for central management of malicious code protection mechanisms
* Automated mechanisms supporting and/or implementing central management of malicious code protection mechanisms

Determine If Statement: SI-03(01) - The organization centrally manages malicious code protection mechanisms.

Result: Not Assessed

Control Title: SI-03(2) -Automatic Updates

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system automatically updates malicious code protection mechanisms.

Implementation Statement: HUD HITS team automatically updates malicious code protection mechanisms.

Assessment Objective: SI-3(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* System and information integrity policy
* Procedures addressing malicious code protection
* Automated mechanisms supporting centralized management of malicious code protection mechanisms
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities
* System developers
* Organizational personnel installing, configuring, and/or maintaining the information system
* Organizational personnel with responsibility for malicious code protection

Test

* Automated mechanisms supporting and/or implementing automatic updates to malicious code protection capability

Determine If Statement: SI-03(02) - The information system automatically updates malicious code protection mechanisms.

Result: Not Assessed

Control Title: SI-04 -Information System Monitoring

Applicability: Hybrid **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Monitors the information system to detect:
1. Attacks and indicators of potential attacks in accordance with [%Assignment: organization-defined monitoring objectives%]; and
2. Unauthorized local, network, and remote connections;
b. Identifies unauthorized use of the information system through [%Assignment: organization-defined techniques and methods%];
c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
g. Provides [%Assignment: organization-defined information system monitoring information%] to [%Assignment: organization-defined personnel or roles%] [%Selection (one or more): as needed; [Assignment: organization-defined frequency]%].

Implementation Statement: This is a common control administered by the HITS Infrastructure team.

Implementation Statement for **P207 - Mainframe (IBM)**
This control is implemented via the Intrusion Detection System (IDS) (a component of the WAN GSS) to monitor/detects events. IDS compares the packets of data with known "signatures" of harmful attacks to detect intrusion attempts and records all attack-related information (including the attack source and destination IP address) in its database. The IDS database is reviewed daily by security personnel for unusual or suspicious activity. Device identification and authentication mechanisms (see controls IA-3 and AC-20.1) provide additional protection against attackers.
Auditing on the IBM Mainframe are used to identifies unauthorized use. IDS sensors are strategically placed at key HUD intra-network boundary points to monitor for malicious network traffic. Additionally, as applicable, IDS sensors are used to collect essential information and at ad hoc locations within the system to track specific types of transactions of interest to the HUD. In the event that HUD heightens the level of information system monitoring activity the IDS monitoring can be increased whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.
Monitoring activities are performed in accordance with HUD. Audit logs are reviewed daily and any anomalies are investigated and reported to HUD CIRT if appropriate. Mainframes do not have monitoring devices.

Assessment Objective: SI-4 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* Continuous monitoring strategy
* System and information integrity policy
* Procedures addressing information system monitoring tools and techniques
* Facility diagram/layout
* Information system design documentation
* Information system monitoring tools and techniques documentation
* Locations within information system where monitoring devices are deployed
* Information system configuration settings and associated documentation
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel installing, configuring, and/or maintaining the information system
* Organizational personnel with responsibility monitoring the information system

Test

* Organizational processes for information system monitoring
* Automated mechanisms supporting and/or implementing information system monitoring capability

Determine If Statement: SI-04 (a)(01)[01] - The organization defines monitoring objectives to detect attacks and indicators of potential attacks on the information system.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-04 (a)(01)[02][a] - The organization monitors the information system to detect, in accordance with organization-defined monitoring objectives, attacks.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-04 (a)(01)[02][b] - The organization monitors the information system to detect, in accordance with organization-defined monitoring objectives, indicators of potential attacks.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-04 (a)(02)[01] - The organization monitors the information system to detect unauthorized local connections.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Determine If Statement: SI-04 (a)(02)[01] - The organization monitors the information system to detect unauthorized local connections.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Determine If Statement: SI-04 (a)(02)[01] - The organization monitors the information system to detect unauthorized local connections.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SI-04 (a)(02)[02] - The organization monitors the information system to detect unauthorized network connections.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Determine If Statement: SI-04 (a)(02)[02] - The organization monitors the information system to detect unauthorized network connections.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Determine If Statement: SI-04 (a)(02)[02] - The organization monitors the information system to detect unauthorized network connections.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-04 (a)(02)[03] - The organization monitors the information system to detect unauthorized remote connections.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Determine If Statement: SI-04 (a)(02)[03] - The organization monitors the information system to detect unauthorized remote connections.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Determine If Statement: SI-04 (a)(02)[03] - The organization monitors the information system to detect unauthorized remote connections.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-04 (b)(01) - The organization defines techniques and methods to identify unauthorized use of the information system.

Result: Not Assessed

Determine If Statement: SI-04 (b)(02) - The organization identifies unauthorized use of the information system through organization-defined techniques and methods.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-04 (c)[01] - The organization deploys monitoring devices strategically within the information system to collect organization-determined essential information.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-04 (c)[02] - The organization deploys monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SI-04 (d)[01] - The organization protects information obtained from intrusion-monitoring tools from unauthorized access.

Inherited From: [Externally Inherited] This control is inherited. It is controlled by HUD OCIO Infrastructure Support and their contrac

Result: **Assessed by:** **Date:**

Determine If Statement: SI-04 (d)[02] - The organization protects information obtained from intrusion-monitoring tools from unauthorized modification.

Result: Not Assessed

Determine If Statement: SI-04 (d)[03] - The organization protects information obtained from intrusion-monitoring tools from unauthorized deletion.

Result: Not Assessed

Determine If Statement: SI-04 (e) - The organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-04 (f) - The organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-04 (g)[01] - The organization defines personnel or roles to whom information system monitoring information is to be provided.

Result: Not Assessed

Determine If Statement: SI-04 (g)[02] - The organization defines information system monitoring information to be provided to organization-defined personnel or roles.

Result: Not Assessed

Determine If Statement: SI-04 (g)[03] - The organization defines a frequency to provide organization-defined information system monitoring to organization-defined personnel or roles.

Inherited From: [Externally Inherited] All remote access to TRACS is through the HUD VPN and is managed by HUD OCIO Infrastructure Suppo

Result: **Assessed by:** **Date:**

Determine If Statement: SI-04 (g)[04] - The organization provides organization-defined information system monitoring information to organization-defined personnel or roles one or more of the following:
* as needed; and/or
* with the organization-defined frequency.

Result: Not Assessed

Control Title: SI-04(2) -Automated Tools For Real-Time Analysis

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization employs automated tools to support near real-time analysis of events.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
HPES employs automated IDS monitoring tools to support near real-time analysis of events.

Assessment Objective: SI-4(2) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and information integrity policy
* Procedures addressing information system monitoring tools and techniques
* Information system design documentation
* Information system monitoring tools and techniques documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel installing, configuring, and/or maintaining the information system
* Organizational personnel with responsibility for monitoring the information system
* Organizational personnel with responsibility for incident response/management

Test

* Organizational processes for near real-time analysis of events
* Organizational processes for information system monitoring
* Automated mechanisms supporting and/or implementing information system monitoring
* Automated mechanisms/tools supporting and/or implementing analysis of events

Determine If Statement: SI-04(02) - The organization employs automated tools to support near real-time analysis of events.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SI-04(4) -Inbound And Outbound Communications Traffic

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The information system monitors inbound and outbound communications traffic [%Assignment: organization-defined frequency%] for unusual or unauthorized activities or conditions.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**

The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

Assessment Objective: SI-4(4) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* System and information integrity policy
* Procedures addressing information system monitoring tools and techniques
* Information system design documentation
* Information system monitoring tools and techniques documentation
* Information system configuration settings and associated documentation
* Information system protocols
* Information system audit records
* Other relevant documents or records

Interview

* System/network administrators
* Organizational personnel with information security responsibilities
* Organizational personnel installing, configuring, and/or maintaining the information system
* Organizational personnel with responsibility for monitoring the information system
* Organizational personnel with responsibility for the intrusion detection system

Test

* Organizational processes for intrusion detection/information system monitoring
* Automated mechanisms supporting and/or implementing intrusion detection capability/information system monitoring
* Automated mechanisms supporting and/or implementing monitoring of inbound/outbound communications traffic

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SI-04(04) [01] - The organization defines a frequency to monitor:
* inbound communications traffic for unusual or unauthorized activities or conditions;
* outbound communications traffic for unusual or unauthorized activities or conditions.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-04(04) [02][a] - The organization monitors, with the organization-defined frequency inbound communications traffic for unusual or unauthorized activities or conditions.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-04(04) [02][b] - The organization monitors, with the organization-defined frequency outbound communications traffic for unusual or unauthorized activities or conditions.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SI-04(5) -System-Generated Alerts

Applicability: Hybrid **Result:** Not Implemented

Control Requirement: The information system alerts [%Assignment: organization-defined personnel or roles%] when the following indications of compromise or potential compromise occur: [%Assignment: organization-defined compromise indicators%].

Implementation Statement: This is a common control administered by the HITS Infrastructure team.

Implementation Statement for **P207 - Mainframe (IBM)**
The information system provides near real-time alerts based on IDS signatures maintained by the IDS provider are triggered beyond normalized thresh holds. The SOC notifies assigned personnel with HPES who will review the findings. If warranted HUD-CIRT will be notified per Incident Response procedures.

Assessment Objective: SI-4(5) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and information integrity policy
* Procedures addressing information system monitoring tools and techniques
* Information system monitoring tools and techniques documentation
* Information system configuration settings and associated documentation
* Alerts/notifications generated based on compromise indicators
* Information system audit records
* Other relevant documents or records

Interview
* System/network administrators
* Organizational personnel with information security responsibilities
* System developers
* Organizational personnel installing, configuring, and/or maintaining the information system
* Organizational personnel with responsibility for monitoring the information system
* Organizational personnel with responsibility for the intrusion detection system

Test
* Organizational processes for intrusion detection/information system monitoring
* Automated mechanisms supporting and/or implementing intrusion detection/information system monitoring capability
* Automated mechanisms supporting and/or implementing alerts for compromise indicators

Determine If Statement: SI-04(05) [01] - The organization defines compromise indicators for the information system.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SI-04(05) [02] - The organization defines personnel or roles to be alerted when indications of compromise or potential compromise occur.

Result: Not Assessed

Determine If Statement: SI-04(05) [03] - The information system alerts organization-defined personnel or roles when organization-defined compromise indicators occur.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SI-05 -Security Alerts, Advisories, And Directives

Applicability: Fully Inherited **Result:** Not Implemented

Control Requirement: The organization:
a. Receives information system security alerts, advisories, and directives from [%Assignment: organization-defined external organizations%] on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to: [%Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]%]; and
d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Implementation Statement: Implementation Statement for **P207 - Mainframe (IBM)**
HPES receives security alerts across a range of systems and components. HPES receives information system security alerts and advisories from US-CERT, NIST, Microsoft, CISCO, IBM, Symantec and other applicable software vendors are reviewed by designated security personnel and system/network administrators on a continual basis. In addition, the HPES GSOC generates security advisories. HUD CIRT creates and disseminates internal security alerts, advisories, and directives and is handled according. Security alerts, advisories, and directives to system administrators and Security Personnel. Security directives are implemented in accordance with established time frames, or notify the HUD of the degree of noncompliance.

Assessment Objective: SI-5 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* System and information integrity policy
* Procedures addressing security alerts, advisories, and directives
* Records of security alerts and advisories
* Other relevant documents or records
Interview
* Organizational personnel with security alert and advisory responsibilities
* Organizational personnel implementing, operating, maintaining, and using the information system
* Organizational personnel, organizational elements, and/or external organizations to whom alerts, advisories, and directives are to be disseminated
* System/network administrators
* Organizational personnel with information security responsibilities
Test
* Organizational processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives
* Automated mechanisms supporting and/or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives
* Automated mechanisms supporting and/or implementing security directives

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SI-05 (a)[01] - The organization defines external organizations from whom information system security alerts, advisories and directives are to be received.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-05 (a)[02] - The organization receives information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-05 (b) - The organization generates internal security alerts, advisories, and directives as deemed necessary.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-05 (c)[01] - The organization defines personnel or roles to whom security alerts, advisories, and directives are to be provided.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-05 (c)[02] - The organization defines elements within the organization to whom security alerts, advisories, and directives are to be provided.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-05 (c)[03] - The organization defines external organizations to whom security alerts, advisories, and directives are to be provided.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-05 (c)[04] - The organization disseminates security alerts, advisories, and directives to one or more of the following:
* organization-defined personnel or roles;
* organization-defined elements within the organization; and/or
* organization-defined external organizations.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Determine If Statement: SI-05 (d) - The organization
* implements security directives in accordance with established time frames; or
* notifies the issuing organization of the degree of noncompliance.

Inherited From: P207 - Mainframe (IBM)

Result: Not Assessed

Control Title: SI-07 -Software, Firmware, And Information Integrity

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization employs integrity verification tools to detect unauthorized changes to [%Assignment: organization-defined software, firmware, and information%].

Implementation Statement: Edits are conducted on data entered and received by the system to ensure integrity. Data that does not pass critical edits is rejected. Some examples are valid contract number, record/date format, duplicate checks.

Assessment Objective: SI-7 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and information integrity policy
* Procedures addressing software, firmware, and information integrity
* Information system design documentation
* Information system configuration settings and associated documentation
* Integrity verification tools and associated documentation
* Records generated/triggered from integrity verification tools regarding unauthorized software, firmware, and information changes
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibility for software, firmware, and/or information integrity
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Software, firmware, and information integrity verification tools

Determine If Statement: SI-07 [01] - The organization
* defines software requiring integrity verification tools to be employed to detect unauthorized changes;
* defines firmware requiring integrity verification tools to be employed to detect unauthorized changes;
* defines information requiring integrity verification tools to be employed to detect unauthorized changes.

Result: Not Assessed

Determine If Statement: SI-07 [02][a] - The organization employs integrity verification tools to detect unauthorized changes to organization-defined software.

Result: Not Assessed

Determine If Statement: SI-07 [02][b] - The organization employs integrity verification tools to detect unauthorized changes to organization-defined firmware.

Result: Not Assessed

Determine If Statement: SI-07 [02][c] - The organization employs integrity verification tools to detect unauthorized changes to organization-defined information.

Result: Not Assessed

Control Title: SI-07(1) -Integrity Checks

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system performs an integrity check of [%Assignment: organization-defined software, firmware, and information%] [%Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]%].

Implementation Statement: This is a common control administered by the HITS Infrastructure team. They reassess the integrity of software and information by performing Component-defined frequency integrity scans of the system.

Assessment Objective: SI-7(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine
* System and information integrity policy
* Procedures addressing software, firmware, and information integrity
* Information system design documentation
* Information system configuration settings and associated documentation
* Integrity verification tools and associated documentation
* Records of integrity scans
* Other relevant documents or records

Interview
* Organizational personnel with responsibility for software, firmware, and/or information integrity
* Organizational personnel with information security responsibilities
* System/network administrators
* System developer

Test
* Software, firmware, and information integrity verification tools

Determine If Statement: SI-07(01) [01] - The organization defines:
* software requiring integrity checks to be performed;
* firmware requiring integrity checks to be performed;
* information requiring integrity checks to be performed.

Result: Not Assessed

Determine If Statement: SI-07(01) [02] - The organization defines transitional states or security-relevant events requiring integrity checks of organization-defined:
* software;
* firmware;
* information.

Result: Not Assessed

Determine If Statement: SI-07(01) [03] - The organization defines a frequency with which to perform an integrity check of organization-defined:
* software;
* firmware;
* information.

Result: Not Assessed

Determine If Statement: SI-07(01) [04] - The information system performs an integrity check of organization-defined software, firmware, and information one or more of the following:
* at startup;
* at organization-defined transitional states or security-relevant events; and/or
* with the organization-defined frequency.

Result: Not Assessed

Control Title: SI-07(7) -Integration Of Detection And Response

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization incorporates the detection of unauthorized [%Assignment: organization-defined security-relevant changes to the information system%] into the organizational incident response capability.

Implementation Statement: The organization incorporates the detection of unauthorized security-relevant changes to the information system into the organizational incident response capability.

Assessment Objective: SI-7(7) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and information integrity policy
* Procedures addressing software, firmware, and information integrity
* Procedures addressing incident response
* Information system design documentation
* Information system configuration settings and associated documentation
* Incident response records
* Information audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibility for software, firmware, and/or information integrity
* Organizational personnel with information security responsibilities
* Organizational personnel with incident response responsibilities

Test

* Organizational processes for incorporating detection of unauthorized security-relevant changes into the incident response capability
* Software, firmware, and information integrity verification tools
* Automated mechanisms supporting and/or implementing incorporation of detection of unauthorized security-relevant changes into the incident response capability

Determine If Statement: SI-07(07) [01] - The organization defines unauthorized security-relevant changes to the information system.

Result: Not Assessed

Determine If Statement: SI-07(07) [02] - The organization incorporates the detection of unauthorized organization-defined security-relevant changes to the information system into the organizational incident response capability.

Result: Not Assessed

Control Title: SI-08 -Spam Protection

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Implementation Statement: This is not applicable - TRACS is not an email system. Email SPAM protection is a common control, the implementation of which is the responsibility of HITS Contractors.

Assessment Objective: SI-8 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and information integrity policy
* Configuration management policy and procedures (CM-1)
* Procedures addressing spam protection
* Spam protection mechanisms
* Records of spam protection updates
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibility for spam protection
* Organizational personnel with information security responsibilities
* System/network administrators
* System developer

Test

* Organizational processes for implementing spam protection
* Automated mechanisms supporting and/or implementing spam protection

Determine If Statement: SI-08 (a)[01] - The organization employs spam protection mechanisms at information system entry points to detect unsolicited messages.

Result: Not Assessed

Determine If Statement: SI-08 (a)[02] - The organization employs spam protection mechanisms at information system entry points to take action on unsolicited messages.

Result: Not Assessed

Determine If Statement: SI-08 (a)[03] - The organization employs spam protection mechanisms at information system exit points to detect unsolicited messages.

Result: Not Assessed

Determine If Statement: SI-08 (a)[04] - The organization employs spam protection mechanisms at information system exit points to take action on unsolicited messages.

Result: Not Assessed

Determine If Statement: SI-08 (b) - The organization updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Result: Not Assessed

Control Title: SI-08(1) -Central Management

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization centrally manages spam protection mechanisms.

Implementation Statement: HUD centrally manages spam protection mechanisms.

Assessment Objective: SI-8(1) - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and information integrity policy
* Procedures addressing spam protection
* Spam protection mechanisms
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibility for spam protection
* Organizational personnel with information security responsibilities
* System/network administrators

Test

* Organizational processes for central management of spam protection
* Automated mechanisms supporting and/or implementing central management of spam protection

Determine If Statement: SI-08(01) - The organization centrally manages spam protection mechanisms.
Result: Not Assessed

Control Title: SI-08(2) -Automatic Updates
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system automatically updates spam protection mechanisms.

Implementation Statement: TRACS relies on HUD's automatic updates to the agency's spam protection mechanisms.

Assessment Objective: SI-8(2) - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* System and information integrity policy
* Procedures addressing spam protection
* Spam protection mechanisms
* Records of spam protection updates
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibility for spam protection
* Organizational personnel with information security responsibilities
* System/network administrators
* System developer

Test

* Organizational processes for spam protection
* Automated mechanisms supporting and/or implementing automatic updates to spam protection mechanisms

Determine If Statement: SI-08(02) - The information system automatically updates spam protection mechanisms.
Result: Not Assessed

Control Title: SI-10 -Information Input Validation
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system checks the validity of [%Assignment: organization-defined information inputs%].

Implementation Statement: The information system checks information inputs for accuracy, completeness, and validity. Edits are in place to ensure data integrity. Some examples include checks on format, valid dates, non-blanks, drop downs, duplicate entry, threshhold amounts, status or expiration date, available funds. Certain words are not used in code or data

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

entry.

Assessment Objective: SI-10 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* System and information integrity policy
* Access control policy and procedures
* Separation of duties policy and procedures
* Procedures addressing information input validation
* Documentation for automated tools and applications to verify validity of information
* List of information inputs requiring validity checks
* Information system design documentation
* Information system configuration settings and associated documentation
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with responsibility for information input validation
* Organizational personnel with information security responsibilities
* System/network administrators
* System developer

Test
* Automated mechanisms supporting and/or implementing validity checks on information inputs

Determine If Statement: SI-10 [01] - The organization defines information inputs requiring validity checks.
Result: Not Assessed

Determine If Statement: SI-10 [02] - The information system checks the validity of organization-defined information inputs.
Result: Not Assessed

Control Title: SI-11 -Error Handling
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system:
a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
b. Reveals error messages only to [%Assignment: organization-defined personnel or roles%].

Implementation Statement: The information system identifies and handles error conditions in an expeditious manner. Edits are issued real-time online and edits on files submitted occur every 15 minutes and are transmitted back to the sender. Additional edits also occur during batch processing and are returned to the user.

Assessment Objective: SI-11 - Determine if the following statement(s) have been satisfied.

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Potential Assessment Methods and Objects:

Examine

* System and information integrity policy
* Procedures addressing information system error handling
* Information system design documentation
* Information system configuration settings and associated documentation
* Documentation providing structure/content of error messages
* Information system audit records
* Other relevant documents or records

Interview

* Organizational personnel with responsibility for information input validation
* Organizational personnel with information security responsibilities
* System/network administrators
* System developer

Test

* Organizational processes for error handling
* Automated mechanisms supporting and/or implementing error handling
* Automated mechanisms supporting and/or implementing management of error messages

Determine If Statement: SI-11 (a) - The information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

Result: Not Assessed

Determine If Statement: SI-11 (b)[01] - The organization defines personnel or roles to whom error messages are to be revealed.

Result: Not Assessed

Determine If Statement: SI-11 (b)[02] - The information system reveals error messages only to organization-defined personnel or roles.

Result: Not Assessed

Control Title: SI-12 -Information Handling And Retention

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Implementation Statement: This is a common control, the implementation of which is the responsibility of HITS Contractors. Data is retained in the TRACS production and archived tables in accordance with MFH specifications – quarterly for iMAX, yearly+ for mainframe.

Assessment Objective: SI-12 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine

* System and information integrity policy
* Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements applicable to information handling and retention
* Media protection policy and procedures
* Procedures addressing information system output handling and retention
* Information retention records, other relevant documents or records

Interview

* Organizational personnel with responsibility for information handling and retention
* Organizational personnel with information security responsibilities/network administrators

Test

* Organizational processes for information handling and retention
* Automated mechanisms supporting and/or implementing information handling and retention

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: SI-12 [01] - The organization, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements handles information within the information system.

Result: Not Assessed

Determine If Statement: SI-12 [02] - The organization, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements handles output from the information system.

Result: Not Assessed

Determine If Statement: SI-12 [03] - The organization, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements retains information within the information system.

Result: Not Assessed

Determine If Statement: SI-12 [04] - The organization, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements retains output from the information system.

Result: Not Assessed

Control Title: SI-16 -Memory Protection

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The information system implements [%Assignment: organization-defined security safeguards%] to protect its memory from unauthorized code execution.

Implementation Statement: TRACS relies mainly on HUD's hardware-enforced safety mechanisms to protect its memory from unauthorized code execution. In addition, TRACS mainframe allocates memory for specified jobs and this assists in protecting from unauthorized data execution.

Assessment Objective: SI-16 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:

Examine
* System and information integrity policy
* Procedures addressing memory protection for the information system
* Information system design documentation
* Information system configuration settings and associated documentation
* List of security safeguards protecting information system memory from unauthorized code execution
* Information system audit records
* Other relevant documents or records

Interview
* Organizational personnel with responsibility for memory protection
* Organizational personnel with information security responsibilities
* System/network administrators
* System developer

Test
* Automated mechanisms supporting and/or implementing safeguards to protect information system memory from unauthorized code execution

Determine If Statement: SI-16 [01] - The organization defines security safeguards to be implemented to protect information system memory from unauthorized code execution.

Result: Not Assessed

Determine If Statement: SI-16 [02] - The information system implements organization-defined security safeguards to protect its memory from unauthorized code execution.

Result: Not Assessed

Control Title: TR-01 -Privacy Notice

Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization:
a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;
b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and
c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Implementation Statement: HUD Multifamily provides effective notice to the public and to individuals regarding its activities that impact privacy, including its collection, use, sharing and safeguarding of personally identifiable information (PII). Notices also reflect changes in practice or policy that affect PII. System Security Awareness training and Rules of Behavior support the safety message.

Assessment Objective: TR-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Privacy compliance process and documentation to ensure that the public is provided with effective notice.
* Privacy compliance process and documentation.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and record and system managers, and OPCL].

Determine If Statement: TR-01 (a) - The organization provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary.

Result: Not Assessed

Determine If Statement: TR-01 (b) - The organization describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected.

Result: Not Assessed

Determine If Statement: TR-01 (c) - The organization revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Result: Not Assessed

Control Title: TR-02 -System Of Records Notices And Privacy Act Statements

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);
b. Keeps SORNs current; and
c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

Implementation Statement: HUD publishes SORNs in the Federal Register and the HUD portal keeps updated SORNs at the following link:
http://portal.hud.gov/hudportal/HUD?src=/program_offices/cio/privacy/pia/fednotice

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Each program office has their list of references, including H-11: Tenant Housing Assistance and Contract Verification Data that defines categories of individuals, records, and uses.
http://portal.hud.gov/hudportal/HUD?src=/program_offices/cio/privacy/sorns/h_11
The Privacy Act Statement appears at the top of form HUD-50059 which collects tenant data, the owner's certification of tenant eligibility.

Assessment Objective: TR-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Privacy compliance process and documentation.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and OPCL].
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and record and system managers, and OPCL].

Determine If Statement: TR-02 (a) - The organization publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII).
Result: Not Assessed

Determine If Statement: TR-02 (b) - The organization keeps SORNs current.
Result: Not Assessed

Determine If Statement: TR-02 (c) - The organization includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.
Result: Not Assessed

Control Title: TR-03 -Dissemination Of Privacy Program Information
Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and
b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Implementation Statement: The public has access to information about HUD's privacy activities and is able to communicate with the Privacy Act Officer with a link to send email.
Contact information for CPO and the privacy practices are publicly available through the HUD website: http://portal.hud.gov/hudportal/HUD?src=/program_offices/cio/privacy/pia/fednotice

Assessment Objective: TR-3 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Department website and policies, procedures, and public reports.
* Department and component website and policies, procedures, and public reports.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview OPCL].
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and OPCL].

Determine If Statement: TR-03 (a) - The organization ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO).
Result: Not Assessed

Determine If Statement: TR-03 (b) - The organization ensures that its privacy practices are publicly available through organizational websites or otherwise.
Result: Not Assessed

Control Title: UL-01 -Internal Use
Applicability: Applicable **Result:** Not Implemented

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Control Requirement: The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Implementation Statement: HUD uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices. For example, household income is part of form HUD-50059 to derive the tenant payment and assistance amount.

Assessment Objective: UL-1 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Privacy compliance process and documentation.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and record and system managers, and OPCL].

Determine If Statement: UL-01 - The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Result: Not Assessed

Control Title: UL-02 -Information Sharing With Third Parties

Applicability: Applicable **Result:** Not Implemented

Control Requirement: The organization:
a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;
b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;
c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and
d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Implementation Statement: HUD Multifamily shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act or described in its notice(s) or for a purpose that is compatible with those purposes. Where appropriate, the agency enters into Memoranda of Agreement with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, such as income verification.

Assessment Objective: UL-2 - Determine if the following statement(s) have been satisfied.

Potential Assessment Methods and Objects:
Examine
* Privacy compliance process and documentation, and Department policies and procedures.
* Privacy compliance process, documentation, and agreements.
* Training policies, procedures, and programs.
Interview
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and record and system managers, and OPCL].
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs, OPCL, and JMD].
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and OPCL].
* Organizational personnel with privacy review responsibilities. [note: interview component SCOPs and system owners, OPCL, and JMD].

Determine If Statement: UL-02 (a) - The organization shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes.

Result: Not Assessed

Security Assessment Report

System: F87 - Tenant Rental Assistance Certification Sys.

Org: HOUSING MF **System Type:** Major Application **Operational Status:** Operational

Determine If Statement: UL-02 (b) - The organization where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used.

Result: Not Assessed

Determine If Statement: UL-02 (c) - The organization monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

Result: Not Assessed

Determine If Statement: UL-02 (d) - The organization evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is require

Result: Not Assessed

Security Assessment Report

Report Selection Criteria:

Created On: 12/2/2015 7:11 PM
Created By: jbarker
Filtered By:
System Name - Acronym: F87 - Tenant Rental Assistance Certification Sys. - TRACS
System Operational Status: All
System Type: All
Assessment Motive: All
Applicability: Applicable and all Inherited/Hybrid
Assessment Result: All
Implementation Result: All
Control Family: All
Control: All
Control Class: All
Include Implementation Statement?: Yes
Include Control Reviews?: No
Review Type: All
Review Result: All
Show POA&MS: No
POA&M Status: All
POA&M Workflow Status: All
Show Milestones: No
Sort By: Control Family