U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

| DEPARTMENTAL MANUAL | NUMBER:<br>DM 4620-002 |
|---|---|
| SUBJECT: Common Identification Standard for U.S. Department of Agriculture (USDA) | DATE:<br>December 9, 2021 |
| OPI: Office of Safety, Security, and Protection (OSSP) | EXPIRATION DATE:<br>December 9, 2024 |

1. PURPOSE

a. This Departmental Manual (DM) provides procedures for United States Department of Agriculture (USDA) staff to meet the Personal Identity Verification (PIV) requirements of the Departmental Regulation (DR) 4620-002, *Common Identification Standard for U.S. Department of Agriculture*. This DM primarily complies with the guidelines of Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors* (and related policies) mandating the development and implementation of a mandatory, Governmentwide Standard for secure and reliable forms of identification (ID) issued to Federal employees and contractors. HSPD-12 compliant identification:

(1) Is issued based on sound criteria for verifying an individual employee's identity;

(2) Is strongly resistant to identity fraud, tampering, counterfeiting, and exploitation;

(3) Can be rapidly authenticated electronically; and

(4) Is issued only by providers whose reliability has been established by an official accreditation process.

b. The National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB) 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, dated August 2013:

(1) Defines a reliable, Governmentwide PIV system for use in applications such as access to federally controlled facilities or information systems;

(2) Specifies a PIV system within which common identification badges can be created and later used to verify a claimed identity; and

(3) Requires identity proofing and background investigations (BI) to verify identity.

c. Office of Management and Budget (OMB) Memoranda M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, and M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access*

*Management*, provide guidance for implementing the requirements in FIPS PUB 201-2 and HSPD-12. The guidance clarifies timelines, applicability, and the requirements of PIV.

2. SCOPE

a. Per FIPS PUB 201-2, the standard "is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to federally controlled facilities and logical access to federally controlled information systems except for "national security systems" as defined by 44 United States code (U.S.C.) § 3552(b)(6)(A).

b. Specifically, PIV applies to all employees (as defined in 5 U.S.C. § 2105, *Employee*) within the Department, a Mission Area, agency, or staff office. For USDA credentialing purposes, the general term "non-Federal employee" applies to non-Federal employees, such as affiliates, contractors, fellows, interns, vendors, and volunteers, who perform a service to USDA under a contract, grant, or other agreement.

c. In addition, all part-time employees (as defined in 5 Code of Federal Regulations (CFR) Part 340) and non-Federal employees who require routine unaccompanied access to federally controlled or leased structures and information systems will be subject to PIV. Routine is defined as performed as part of a regular procedure rather than for a special reason. USDA's PIV compliant credential is called the LincPass, as it is designed to link a person's identity to an identification card and the card to a person's ability to access federally controlled or leased structures and computer systems. Alternatively, USDA has implemented a PIV-I (Personal Identity Verification Interoperable) credential (called AltLinc), which may be issued as an alternative to the LincPass for cases in which short-term Federal employees and non-Federal employees require limited access to federally controlled facilities and information systems for fewer than 6 months, as well as a derived PIV (or PIV-D; Personal Identify Verification Derived) credential called MobileLinc for logical access. Refer to the USDA Credential Matrix in Appendix D for guidance regarding the credential issuance risk assessment process.

d. Individuals requiring limited access to Federal facilities, and systems or applications can be issued alternate credentials as described in this manual. These individuals are also subject to a credential issuance risk assessment per the USDA Credential Matrix. Written work agreements for such individuals (e.g., volunteer agreement, guest researcher agreement, memorandum of understanding (MOU), and extramural agreement) must include a statement regarding PIV as required per a Mission Area, agency, or staff office-conducted credential risk assessment. Written work agreements must also include the eligibility requirements for a PIV credential. Refer to the USDA Credential Matrix in Appendix D.

e. This policy also applies to foreign national employees and non-Federal employees. Due to the limitations in an Investigative Service Provider's (ISP) ability to collect BI information in locations outside the United States, special investigative considerations apply when a PIV credential is needed for a non-U.S. national in either U.S. based locations or foreign locations. Credentialing of non-U.S. Nationals must adhere to the standards defined in the Office of Personnel Management (OPM) *Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for PIV Credentials* ("*OPM Credentialing Standards*"), Appendix A, *Credentialing Eligibility of Non-United States Nationals.*

## 3. SPECIAL INSTRUCTIONS/CANCELLATIONS

a. This manual supersedes DM 4620-002, *Common Identification Standard for U.S. Department of Agriculture*, dated January 14, 2009.

b. Mission Area, agency, and staff office HSPD-12 designated Leads and Alternates are designated by the Mission Area Chief of Staff. HSPD-12 Leads and Alternates are responsible for the distribution of DR 4620-002 and DM 4620-002 and the administration of the HSPD-12 program within their Mission Area, agency, and staff office as defined in the MOU between the Office of Safety, Security, and Protection (OSSP) and the Mission Area, agency, or staff office.

## 4. BACKGROUND

Prior to the inception of HSPD-12, Government agencies used a wide range of methods to authenticate Federal employees and contractors as a requirement to enter Government-controlled or leased structures and use Government systems. HSPD-12 requires all Government agencies to develop specific and consistent standards for both physical and logical identification systems.

Subsequent policies have established detailed standards on implementing processes and systems to fulfill the requirements of HSPD-12. USDA has outlined the policies for HSPD-12 implementation in DR 4620-002.

## 5. PRIVACY POLICY

HSPD-12 explicitly states that "protect[ing] personal privacy" is a requirement of the PIV system. As a USAccess customer, USDA's PIV process and system is in accordance with the spirit and letter of all privacy controls specified in FIPS PUB 201-2, as well as those specified in Federal privacy laws and policies including but not limited to the *E-Government Act of 2002*, the *Privacy Act of 1974*, and OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, as applicable.

## 6. ROLES AND RESPONSIBILITIES

### a. Role Holder

The role holder actions defined in this section are to be completed in the following authoritative systems for USDA:

(1) Authoritative Human Resources (HR) System – EmpowHR. Processing for Federal and Non-Federal personnel must be completed in the following modules:

(a) Personnel Action Request (PAR) Processing – for Federal personnel; or

(b) Non-Employee Processing (commonly referred to as Person Model) – for non-Federal personnel.

(2) Authoritative PIV Issuance System – USAccess. General Services Administration's (GSA) shared service system for the issuance of the PIV and PIV-I card utilized by USDA.

### b. Mission Areas, Agencies, and Staff Offices

The HSPD-12 program is governed by the USDA HSPD-12 Program Management Office (PMO). The PMO partners with Mission Area, agency, or staff office in implementing HSPD-12 throughout USDA. HSPD-12 implementation is coordinated through a partnership between the PMO and the Designated Mission Area, agency, or staff office Lead and Backup Mission Area, agency, or staff office Lead from each Mission Area, agency, or staff office. Mission Area, agency, and staff office Participation in the HSPD-12 program requires the establishment of a MOU between the Mission Area, agency, and staff office and the PMO. The MOU defines the PMO responsibility and Mission Area, agency, and staff office responsibility for HSPD-12 implementation.

The PIV process contains critical roles associated with the identity proofing, registration, and issuance process. These roles may be collateral duties assigned to personnel who have other primary duties. The PIV identity proofing, registration and issuance process must adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.

The following roles must be employed for identity proofing, registration, and issuance.

### c. Applicant

The Applicant is an individual who requires a credential as a condition of employment with a Mission Area, agency, or staff office that will be entered into the authoritative PIV issuance system. Applicants will:

(1) Provide Sponsor with any necessary information;

(2) Input information into Electronic Questionnaires for Investigations Processing (e-QIP; if available) or fill out the appropriate form as directed by the security office if no BI has been completed or is in progress;

(3) Submit fingerprints for a background check;

(4) Schedule an enrollment appointment;

(5) Appear for the enrollment appointment at the time and place scheduled;

(6) Provide the Registrar with two U.S. Citizenship and Immigration Services (USCIS) Form I-9 listed identity documents;

(7) Submit to a digital photo taken by the Registrar;

(8) Submit ten fingerprints (rolls and slaps). If the capture of 10 fingerprints is not feasible due to missing or damaged fingers, this will be annotated in the system;

(9) Digitally sign the enrollment package;

(10) Activate the credential via biometric verification and Personal Identification Number (PIN) creation;

(11) Ensure the credential is registered for logical and physical access;

(12) Ensure that the Sponsor or Agency Security Officer is notified if the card is lost or stolen immediately;

(13) Store credentials in an approved badge holder and fastened to either an item of clothing or lanyard;

(14) Wear credentials above the waist in such a manner that the ID photograph is clearly visible from the front at all times;

(15) Wear an armband holder or place the credential in a pocket, if it is permissible, if the applicant works in a hazardous environment where it would be unsafe to wear the credential in the manner outlined;

(16) Properly wear and display the credential once the person leaves the hazardous work area (e.g., if the credential had been placed in the pocket, it must be properly worn and displayed again). Mission Areas, agencies, or staff offices must define the work areas in which it would be unsafe to wear the credential as outlined in this section; and

(17) Return expired or terminated credentials to the Agency Security Officer, local badging office, or mail to the address printed on the back of the PIV card.

d. HR User

The HR User is responsible for creating and modifying an Applicant's information in the authoritative HR system(s). Often the HR User and the Sponsor roles are held by the same person, but it is not required.

e. Sponsor

The Sponsor is the Mission Area, agency, or staff office official (Federal employee) who has undergone Sponsor training and is designated to perform Sponsor functions. The Sponsor is responsible for authorizing an individual to apply for a credential. In the case of non-Federal employees, the Sponsor may be the Contracting Officer's Representative (COR) or other designated program official. To leverage existing roles in the LincPass process, MobileLinc responsibilities have been added to the Sponsor role. Sponsors will:

(1) Validate that the Applicant's information has been entered into the authoritative HR system;

(2) Determine the required credential type by utilizing the USDA Credential Matrix (Appendix D);

(3) Modify the Applicant's identity record in the authoritative database based on updates to user status and relevant information;

(4) Update and maintain the Applicant's Sponsorship in the authoritative HR system;

(5) Maintain current employment status:

(a) Termination: As needed, set employment status to Terminated in the Human Resources (HR) record in the authoritative HR system; and

(b) Suspended: As needed, set the employment status to Suspended in the HR record in the authoritative HR system.

To ensure timely provision and de-provision of accounts (e.g., desktops, eAuthentication, building access, National Finance Center (NFC) applications, MobileLinc credential management accounts), Mission Areas, agencies, or staff offices must record hiring and termination events in the authoritative HR database as soon as possible. New hires and re-hires should be entered at least 3 days before their start date.

(6) Trigger card actions in authoritative HR and PIV issuance systems:

(a) Suspense: Monitor card status and change to “Suspend.” If suspense is based on employment status, ensure the card status change is reflected in both the authoritative HR and PIV issuance systems. If suspense is a result of disciplinary action, manually update the card status to “Suspend” in the authoritative PIV issuance system first and notify the Agency Security Officer, subsequently making the update in the authoritative HR system. If possible, recover the suspended credentials and send to the Agency Security Officer for secure storage pending resolution of issue(s);

(b) Termination: Monitor card status change to “Terminate.” If termination is based on employment status, ensure the card status change is reflected in the authoritative HR and PIV issuance systems. If termination is a result of disciplinary action, manually update the card status to “Terminate” in the authoritative PIV issuance system first and notify the Agency Security Officer, subsequently making the update in the authoritative HR system. If possible, recover the revoked credentials and send them to the Agency Security Officer for destruction;

(c) Card Suspense or Termination: If card Suspense or Termination is due to notification of imminent risk, immediately make the change directly in the authoritative PIV issuance system and notify the Agency Security Officer and HSPD-12 Adjudicator, subsequently making the change in the authoritative HR system;

(d) Re-enrollment: Initiate re-enrollments for current or previous cardholders in the event of a change in the Applicant’s identity information or an expired enrollment;

(e) Recertification: Ensure the HR record is accurate and trigger a card update or certificate rekey as appropriate;

(f) Renewal: Ensure cards are renewed every 5 years per FIPS PUB 201-2, at the 10 year mark the applicant must re-enroll and a re-issuance required; and

(g) Reprint: Ensure cards are reprinted as needed due to damage or loss.

f. Registrar

The Registrar is an individual responsible for identity proofing the Applicant, as well as capturing biographic information, digital photo, and biometrics. Registrars will:

(1) Manage schedule for enrollment workstations;

(2) Answer any privacy or system related questions that an Applicant may have;

(3) Locate and open the Applicant's information and verify the information with the Applicant;

(4) Contact the Sponsor if the Applicant's record cannot be found in the system to investigate and resolve the problem;

(5) Verify and scan the Applicant's two identity source (Form I-9) documents;

(6) Verify and enter biometric information;

(7) Capture the Applicant's facial image in the system via a digital photograph;

(8) Capture 10 fingerprints (rolls and slaps) into the system. If capture of 10 fingerprints is not feasible due to missing or damaged fingers, annotate the record in the system;

(9) Verify the primary and secondary fingerprints against the minutiae to ensure that the templates will work when put on the credential;

(10) Flag any issues during enrollment; and

(11) Digitally sign and send the enrollment package to the Credential Printing Facility and inform the Applicant of next steps (i.e., credential issuance and activation process).

g. HSPD-12 Adjudicator

The HSPD-12 Adjudicator is a Federal employee of the sponsoring Mission Area, agency, and staff office who records the results of the Federal Bureau of Investigation (FBI) National Criminal History Check (FBI fingerprint check) and the BI (T1 (Tier 1) or higher) into the authoritative HR system. The HSPD-12 Adjudicator role referenced here is not to be confused with the BI Adjudicator role as defined by Office of Homeland Security (OHS) Personnel and Document Security Division (PDSD). While both roles can be held by the same person, it is not required.

PIV adjudication is aligned with the OHS-PDSD suitability and BI processes. Results of the suitability and BI process as determined by OHS-PDSD standards will be utilized as the interim and final determination for PIV adjudication results. These results will be recorded in the authoritative HR system by the HSPD-12 Adjudicator.

HSPD-12 Adjudicators will:

(1) Enter fingerprint check results in the authoritative HR system. Entry of fingerprint check results separately from BI results will expedite printing of the LincPass and is highly recommended. This will result in an interim PIV issuance, pending

completion of the BI. If the results are favorable, this will allow the LincPass to print. If the results are unfavorable, this will terminate the card issuance process. To issue an interim PIV issuance the following steps must be complete:

(a) Presentation by the appointee or employee of two identity source documents, at least one of which is a Federal or State government-issued picture identification;

(b) Favorable review of the intended PIV recipient's completed investigative questionnaire;

(c) Initiation of the intended PIV recipient's required BI (T1 or higher) request, meaning the request has been submitted to the Federal background ISP, and the ISP has scheduled the investigation; and

(d) Favorable review of the results of the intended PIV recipient's FBI National Criminal History Check (FBI fingerprint check) portion of the required BI

(2) Confirm and enter the BI results in the authoritative HR system: entry of BI results will finalize the eligibility process for the Applicant. If the results are favorable, this will allow the Applicant to maintain their LincPass. If the results are unfavorable, this will terminate the card;

(3) Respond to inquiries on adjudication status from Applicants; and

(4) Report any changes in PIV eligibility to the applicant Sponsor and Agency Security Officer and update authoritative systems as necessary.

h. Print Operator

The Print Operator is the individual responsible for processing credential production at a designated USDA Local Printing station. The Print operator verifies that the Applicant is the person to whom the credentials are to be printed. Print Operators will:

(1) Receive blank cardstock credentials from the HSPD-12 PMO and sign for packages (dependent on shipping model);

(2) Secure blank cardstock in a locked safe or lockable filing cabinet, and monitor all credentials that are deposited or removed from the safe;

(3) Verify that the Card Serial Number and other Applicant information entered in the system and the information on the printed credential is in agreement;

(4) Hand the newly printed credential to the Activator for activation;

(5) Flag the credential in the system and note problems with card printing;

(6) Collect the misprinted credentials and keep a log;

(7) If applicable, destroy misprinted credentials or ship them to the Agency Security Officer as appropriate; and

(8) When requested, securely send credentials to another Activation Station.

i. Activator

The Activator is the individual responsible for processing credential activations. The Activator verifies that the Applicant is the person to whom the credentials are to be issued and guides the Applicant through the activation process.

Most activation stations will be unattended, meaning that Applicants will use the system without assistance to activate their credentials. In the event that there is an issue causing the unattended activation to fail, the Activator will assist the Applicant in completing the activation, or collect the credential, note the issue in the system, and flag the record for issue resolution.

The Activator can also assist in card maintenance activities such as certificate updates and PIN resets. Activators will:

(1) Receive "to-be-activated" credentials from the authoritative PIV issuance systems centralized printing facility or another station, and sign for packages (dependent on shipping model);

(2) Log credentials into the system, and send out electronic notifications to the Applicants;

(3) Secure credentials in a locked safe or lockable filing cabinet, and monitor all credentials that are deposited or removed from the safe;

(4) Hand the credential to the individual after document and visual verification;

(5) Verify that the Applicant information entered in the system and information displayed on the credential is in agreement;

(6) Flag the credential in the system and note problems with activation;

(7) Collect the credential if activation fails. In the event a card becomes damaged or defective, cards must be returned to the Agency Security Officer or: USDA South Building – OSSP Facility Protection Division (FPD), 1400 Independence Avenue SW, Room 1408, Washington, DC 20250;

(8) If applicable, collect Applicants' previous credentials and destroy or ship to Agency Security Officer as appropriate. In the event a card becomes damaged or defective, cards must be returned to USDA South Building – OSSP FPD, 1400 Independence Avenue SW, Room 1408, Washington, DC 20250; and

(9) When requested, send credentials to another Activation Station using sealed non-transparent packaging.

j. Role Administrator

The Role Administrator is the individual responsible for managing the Mission Area, agency, and staff office Sponsors, HSPD-12 Adjudicators, Registrars, Security Officers and Activators. USDA has one Role Administrator who oversees all individual Mission Area, agency, and staff office Role Administrators. The Role Administrator will verify that the appropriate separation of duty policies are followed and will verify that all the training certification requirements have been met. Role Administrators will:

(1) Ensure separation of HSPD-12 duties;

(2) Ensure that role holders are adequately trained for their assigned role;

(3) Submit access requests to authoritative HR system for appropriate roles;

(4) Approve role holder portal privileges in the authoritative PIV issuance system for new role holders; and

(5) Revoke role privileges and portal access for users in cases where the role will no longer be performed by the user or upon employment termination.

k. Agency Security Officer

The HSPD-12 Security Officer is the individual responsible for maintaining credential security and integrity of Applicant identity information. To leverage existing roles in the LincPass process, PIV-D credential responsibilities have been added to the Agency Security Officer role. Agency Security Officers will:

(1) When required, immediately change the status of a credential between active, suspended, or terminated due to security related situations such as notification of imminent risk;

(a) If suspense or termination is a result of disciplinary action, or imminent danger, immediately manually update the card status in USAccess if the Sponsor has not done so;

(b) If possible, recover the credential immediately and store securely until destruction can occur;

(c) Notify the following groups of the imminent risk:

1 HSPD-12 Sponsor and Adjudicator, if these Points Of Contacts (POC) are not known please contact the HSPD-12 Help Desk at USDAhspd12help@usda.gov;

2 Security services at the impacted Federal facility – in the case of the National Capital Region (NCR), contact OSSP at securityservicehelp@usda.gov;

3 Local law enforcement – 911 for emergency;

4 Federal law enforcement through the Department of Homeland Security (DHS) Fusion Center (*Fusion Center Locations and Contact Information*);

5 OHS Insider Threat (insider@usda.gov), Counterintelligence (CI@usda.gov), and OHS PDSD (CNSIS@usda.gov);

6 Office of Human Resources (OHRM) (humanresources@usda.gov) or applicable Mission Area, agency, and staff office Personnel Security staff if records are not held by OHRM; and

7 USDA Workplace Violence Prevention Program Contact (Contact Information);

(2) Report any potential security anomalies, suspicious behavior, concerns, or incidents regarding USDA employees or contractors to OHS PDSD at CNSIS@usda.gov and OHS Insider Threat Program at insider@usda.gov;

(3) Report any potential security anomalies, suspicious behavior, concerns, or incidents regarding foreign national visitors to the OHS Counterintelligence Program at CI@usda.gov;

(4) Collect and destroy credentials. In the event a card becomes damaged or defective, destroy the card following the steps dictated in the *USDA HSPD-12 LincPass Destruction Guide* or return the card to USDA South Building – OSSP FPD, 1400 Independence Avenue SW, Room 1408, Washington, DC 20250;

(5) In the event of duplicate records in the authoritative PIV issuance system, verify the Applicants' identity information and purge erroneous records;

(6) When required, request that the Mission Area, agency, or staff office information technology (IT) support help desk personnel revoke the PIV-D credentials in the event of a lost or stolen device or a security incident; and

(7) Review and make determinations on any records flagged during the enrollment process for Security Officer review.

l. Site Manager

The Site Manager is responsible for managing credentialing center information and the schedule for USDA Credentialing stations. Site managers will:

(1) Manage site information, weekly site schedules, and site POCs for all types of credentialing stations in the authoritative PIV issuance system's site inventory tool;

(2) Validate the concurrence of ship-to location information between the authoritative HR system and the authoritative PIV issuance system, and correct conflicts as needed;

(3) Validate the concurrence of all types of credentialing stations between the authoritative PIV issuance system's site inventory tool and the USDA Master Deployment Inventory; and

(4) Validate the concurrence of all types of credentialing stations between the authoritative PIV issuance system's site inventory tool and center locator tool.

m. Federal Employee and Permissible Contractor Roles

Some HSPD-12 roles require Federal employment; however, some HSPD-12 roles allow a contractor to perform the function. Please see Table 1, *Role Holder Requirements*, below for employment requirements by role:

TABLE 1 – Role Holder Requirements

| **Role** | **Description** | **Type: Federal Employee** | **Type: Non-Federal Employee** |
|---|---|---|---|
| **HSPD-12 Adjudicator** | The Mission Area, agency, or staff office HSPD-12 Adjudicator is a Government employee of the sponsoring Mission Area, agency, or staff office who is responsible for entering the results of the adjudication decision as well as the supporting BI information into the authoritative systems. | Yes | Not Applicable |

| Role | Description | Type: Federal Employee | Type: Non-Federal Employee |
|---|---|---|---|
| **Activator** | The Activator is the individual responsible for processing credential activations. The Activator verifies that the Applicant is the person to whom the credentials are to be issued and guides the Applicant through the issuance process. | Yes | Yes |
| **Agency Role Administrator** | The Agency Role Administrator is the individual responsible for managing the Mission Area, agency, or staff office Sponsor, HSPD-12 Adjudicator, Registrar, or Activators. The Agency Role Administrator will verify that the appropriate separation of duty policy is followed and will verify that all the training certification requirements have been met. | Yes | Not Applicable |
| **USDA Security Officer** | The OSSP Chief Security Director, serving as the USDA Chief Security Officer, is the individual responsible for maintaining credential security as well as physical building security within USDA. The USDA Security Officer is nominated by the Department. | Yes | Not Applicable |
| **Agency Security Officer** | The Agency Security Officer is the individual responsible for maintaining credential security as well as physical building security for their Mission Area, agency, or staff office. The Agency Security Officer is nominated by the Mission Area, agency, or staff office. | Yes | Not Applicable |
| **Sponsor** | The Sponsor is the employer or Mission Area, agency, or staff office official responsible for authorizing an individual to apply for a credential, who has undergone Sponsor training, and is designated to perform Sponsor functions. In the case of contractor employees, the Sponsor may be the COR or another designated program official. | Yes | Not Applicable |
| **Registrar** | The Registrar is an individual responsible for identity proofing the Applicant, as well as capturing biographic information, digital photo, and biometrics. | Yes | Yes |

## 7. ROLE HOLDER TRAINING

Training for HSPD-12 roles (Role Administrators, Sponsors, Registrars, HSPD-12 Adjudicators, and Activators) is required.

### a. Authoritative PIV Issuance System Training

GSA provides training modules for HSPD-12 Role Holders in the authoritative PIV issuance system. All Role Administrators, Registrars, Activators, and Agency Security Officers must take training and be certified to perform their duties. These training modules are available in the GSA *GoLearn* system. There are four training modules with a certification test at the end of each module as shown in Table 2, *Authoritative PIV Issuance System Training Modules*. Please note that Sponsor and HSPD-12 Adjudicator training is consolidated in USDA based training and is covered in Table 4, *Authoritative HR System Training Module Descriptions for Sponsorship and Adjudication of Federal Personnel*.

TABLE 2 – Authoritative PIV Issuance System Training Modules

| Training Module | Est. Duration | Description |
|---|---|---|
| GSA PIV Registrar Training | 60 minutes | Includes audio, screen shots, Small Web Format (SWF) movies, and video |
| GSA PIV Activator Training | 30 minutes | Includes audio, screenshots, SWF movies, maybe some video |
| GSA PIV Security Officer Training | 40 minutes | Includes audio, screen shots, SWF movies |
| GSA PIV Role Administrator Training | 20 to 30 minutes | Includes audio, screen shots, SWF movies |

Training results will be recorded in *GoLearn*, to which the Role Administrator and Agency Role Administrator will have access for training management.

### b. USDA Role Holder Training

All USDA managed training modules are available in USDA's Learning Management System (LMS), AgLearn. They are also available on the USDA HSPD-12 *Role Holder Training* website.

(1) Role Administrator Training

TABLE 3 – Role Administrator Training Module Descriptions

| Training Module | Est. Duration | Description |
|---|---|---|
| Role Administrator Training | 30 minutes | Includes policies, screenshots, and instructions for Role Administrators. |

(2) Authoritative HR System Training – For Sponsorship and Adjudication of Federal Personnel

All Sponsor and HSPD-12 Adjudicator users must take the appropriate training for their role and be certified per Mission Area, agency, and staff office policies to perform their duties. Sponsors and HSPD-12 Adjudicators of Federal employees must be designated as role holders by their Role Administrator. Training must be completed for records to process successfully. Table 4, *Authoritative HR System Training Module Descriptions for Sponsorship and Adjudication of Federal Personnel*, provides descriptions for the training modules.

TABLE 4 – Authoritative HR System Training Module Descriptions for Sponsorship and Adjudication of Federal Personnel

| Training Module | Est. Duration | Description |
|---|---|---|
| Sponsorship of Federal Personnel | 60 to 90 minutes | Includes screenshots and instructions for Sponsor functions to be completed in the authoritative HR system. |
| Post-Sponsorship Training for Sponsors of Federal and Non-Federal Personnel | 60 minutes | Includes screenshots and instructions for Sponsor functions that need to be performed within the authoritative PIV issuance system. |
| Adjudication of Federal Personnel Training | 30 to 45 minutes | Includes screenshots and instructions for Adjudication actions to be completed in the authoritative HR system. |

(3) Authoritative HR System Training – For Sponsorship and Adjudication of Non-Federal Personnel

All Sponsors and HSPD-12 Adjudicators must take the appropriate training for their role and be certified per Mission Area, agency, and staff office policies to perform their duties. Sponsors and HSPD-12 Adjudicators of non-Federal employees must be designated as role holders by their Role Administrator. Training must be completed for records to process successfully. Table 5, Authoritative HR System Training Module Descriptions for Sponsorship and Adjudication of Non-Federal Personnel, provides descriptions for the training modules.

TABLE 5 – Authoritative HR System Training Module Descriptions for Sponsorship and Adjudication of Non-Federal Personnel

| Training Module | Est. Duration | Description |
|---|---|---|
| Sponsorship of Non-Federal Personnel | 60 to 90 minutes | Includes screenshots and instructions for Sponsor functions to be completed in the authoritative HR system. |
| Post-Sponsorship Training for Sponsors of Federal and Non-Federal Personnel | 60 minutes | Includes screenshots and instructions for Sponsor functions that need to be performed within the authoritative PIV issuance system. |
| HSPD-12 Adjudication of Non-Federal Personnel Training | 30 to 45 minutes | Includes screenshots and instructions for HSPD-12 Adjudication actions to be completed in the authoritative HR system. |

## 8. PROCEDURES

### a. Reciprocity of Credentialing Determinations

Per the OPM Credentialing Standards, USDA must not re-investigate or re-adjudicate individuals visiting or temporarily or permanently transferring from another Federal Department or Agency provided a final favorable PIV eligibility determination exists based on an investigation that is at an appropriate tier for the new position.

USDA standards and processes regarding reciprocity are defined by OHS-PDSD.

### b. PIV Issuance Guidelines

(1) PIV Applicability

(a) PIV requires the implementation of registration, identity proofing, and issuance procedures in line with the requirements of FIPS PUB 201-2.

(b) All individuals must follow the procedures outlined to apply for and receive their credentials. USDA uses the USAccess program, a certified NIST Special Publication (SP) 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, PIV Card Issuing Organization, for PIV issuance. USAccess is a system-based model with increased functionality to improve efficiency and accuracy in processing PIV applications. The PIV procedures and processes utilizing USAccess are discussed in detail in Section 8.

(c) A Social Security Number (SSN) is required for entry of applicant records into USDA HR systems. OHS has the authority to issue a pseudo-SSN for foreign national applicants who do not have an SSN.

(2) Credentialing Standards

In accordance with OPM guidelines, a PIV credential will not be issued to an individual if any of the following applies:

(a) The individual is known to be or reasonably suspected of being a terrorist;

(b) The employer is unable to verify the individual's claimed identity;

(c) The employer has a reasonable basis to believe the individual has submitted fraudulent information concerning their identity;

(d) The employer has a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the *Privacy Act*, information that is proprietary in nature, or other sensitive or protected information;

(e) The employer has a reasonable basis to believe the individual will use an identity credential outside the workplace or inappropriately; or

(f) The employer has a reasonable basis to believe the individual will use federally controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

(3) Revocation and Suspense of PIV Eligibility

(a) Mission Areas, agencies, and staff offices must develop procedures which adhere to standards defined by OHS-PDSD in order to notify the cardholder's HSPD-12 role holders (Sponsor, HSPD-12 Adjudicator, and Agency Security

Officer) in the event of any incident or adverse credible information that would impact PIV Eligibility.

(b) HSPD-12 role holders must follow the steps defined in the role holder's responsibilities section of this document to ensure timely suspension or revocation of the PIV card due to the result of a change in eligibility.

(c) Making the required status and eligibility changes in the authoritative USDA systems, will automatically remove logical access to IT systems as well as physical access to Enterprise Physical Access Control Systems (ePACS).

(d) USDA Mission Area, agency or staff offices may perform Barring Actions at their respective locations outside the NCR. These actions will be done in accordance with USDA Mission Area, agency or staff office policies and will be reported to OSSP.

(4) Background Investigation Requirements

BI Requirements and processes are developed and maintained by OHS.

(5) Appeal Procedures for Denial or Revocation of Credential

Appeal procedures are developed and maintained by OHS.

(6) Expiration Date Requirements

(a) LincPass Expiration Date

All PIV credentials issued to the USDA must have a printed expiration date. The printed expiration date on the LincPass is set for 5 years from the date the card was issued unless the appointment or hiring term is for a period less than 5 years. In this case the expiration date will be set for the end of the identified term. Certificates embedded on the card enabling digital signatures are only valid for 3 years. Because of the evolving nature of technology and encryption of certificates on the card, the 3-year certificate expiration ensures the card functions properly. PIV credentials for non-Federal employees must be inactivated at the end of the contract, grant, or agreement period of performance.

(b) AltLinc Expiration Date

Please refer to the AltLinc PIV-I Policy documentation at the USDA *HSPD-12 Policies, Procedures, and Forms* web page for details on the certificate and printed expiration date for short term resources.

(7) Contracting Impacts

(a) All non-Federal employees must abide by the identity proofing and registration requirements outlined in this DM. USDA contract statements of work must indicate that all contractors requiring routine access to federally controlled facilities or information systems go through the identity proofing and registration process and have a successfully adjudicated T1 or Defense Counterintelligence and Security Agency/National Security (DCSA/NS) BI to serve on the contract.

(b) While there is no official USDA procurement policy requiring PIV language to be included in grants or agreements, in keeping with the policies and procedures for contracting, it is recommended that the process outlined in this manual is followed for other non-contractor, non-Federal employees (e.g., affiliates, fellows, interns, or volunteers).

(c) Contractor LincPasses will be issued after a favorably adjudicated fingerprint check has been received by Mission Area, agency, or staff office Adjudicator, and upon an initiated T1or DCSA/NS BI. All contracts must specify periods of performance. Contractors must renew their credentials based on the period of performance.

(d) Certain PIV language must be implemented in all contracts. This language is found in *Federal Acquisition Regulations* (FAR) 48 CFR Subpart 4.13, *Personal Identity Verification* of Contractor Personnel. HSPD-12 clauses include FAR 48 CFR Clause 52.204-9, *Personal Identity Verification of Contractor Personnel*. The *USDA Contracting Desk Book*, Subpart 404.13, *Personal Identity Verification*, contains additional procurement guidance.

(e) The language provided in the *USDA Contracting Desk Book*, Subpart 404.13 may be modified for use in any non-contract grants or agreements.

(8) Audit and Records Management

(a) The Office of the Inspector General (OIG) has responsibility for auditing identity proofing and registration records. As such, all Mission Areas, agencies, or staff offices should be prepared for such reviews.

(b) Mission Areas, agencies, or staff offices must comply with DR 3080-001, *Records Management*, for the creation, maintenance, use, and disposition of all records associated with the PIV process.

c. PIV Issuance Process

(1) LincPass Issuance Standard Operating Procedures

The PIV process comprises a series of steps performed by designated role holders. LincPass credentialing steps are divided into the following:

(a) Sponsorship;

(b) Adjudication;

(c) Enrollment;

(d) Issuance;

(e) Activation; and

(f) Maintenance.

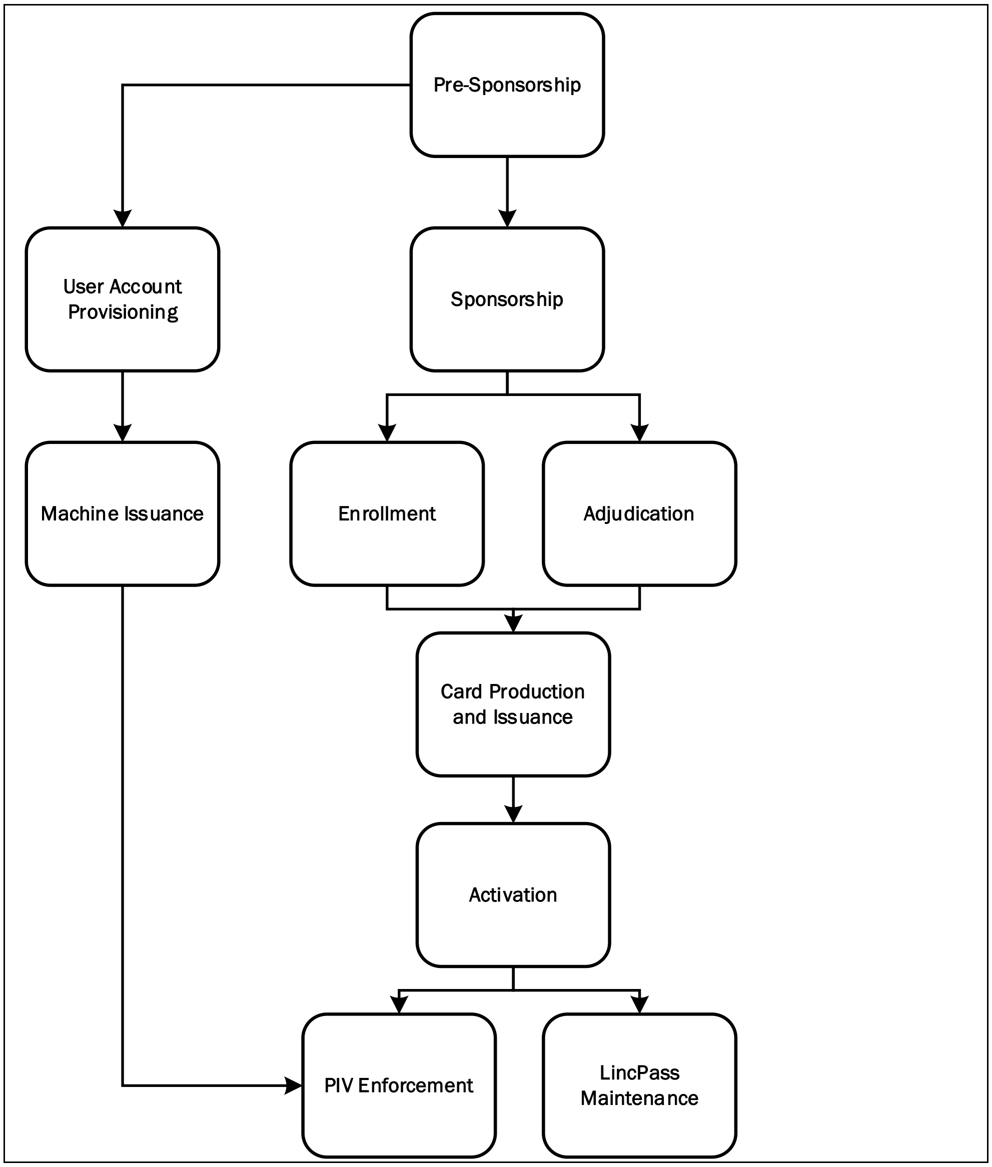
Associated process steps related to onboarding or card usage occur during the credentialing process, specifically, Pre-Sponsorship, User Account Provisioning, Machine Issuance, PIV Enforcement, and LincPass Maintenance.

Long term active USDA personnel with an active LincPass will be eligible for Derived PIV credentials as part of the MobileLinc program if they have been assigned an authorized mobile device registered with the USDA Enterprise Mobility Management (EMM). Refer to the Office of the Chief Information Officer (OCIO) Identity, Credential, and Access Management (ICAM) *Personal Identity Verification Derived Credentials Issuing Operations Plan* for more information. You can also obtain additional information at the USDA *MobileLinc Credential Portal* website.

(2) LincPass Issuance Steps

Figure 1, *LincPass Card Onboarding Process*, below provides an overview of the LincPass credentialing steps and associated processes for onboarding and card usage.

FIGURE 1 – LincPass Card Onboarding Process



(a) Pre-Sponsorship

1 The Sponsor uses the USDA Credential Matrix to determine whether the Applicant requires a LincPass. All full-time Federal Employees require a LincPass. However, some seasonal or temporary Federal or non-Federal Employees may not require a LincPass based on the USDA Credential Matrix in Appendix D.

2 The Sponsor enters or validates the required Applicant information into the authoritative HR system. Applicants may already have a record

entered, in which case the Sponsor verifies and updates the record as needed.

3 Sponsors may request a pseudo-SSN for foreign national applicants who do not have an SSN, which is required for entry into USDA HR systems. The Foreign National LincPass Request may be obtained by contacting OHS. The Sponsor must complete the requests and OHS will issue a unique pseudo-SSN for the applicant.

(b) Sponsorship

1 The Sponsor locates the Applicant's record in the appropriate HR system, selects the appropriate card type option (i.e., LincPass, AltLinc, No LincPass/AltLinc) and enters Card Shipping Information.

2 The Applicant will be notified by e-mail to schedule an appointment to enroll.

(c) User Account Provisioning

1 The HR system feeds identity data to the USDA OCIO ICAM system.

2 ICAM creates a record for the Applicant in the authoritative PIV issuance system.

3 Upon System Authorization Access Request submission and approval, ICAM creates a user account in the Enterprise Active Directory (EAD).

4 ICAM feeds PIV credential data to EAD. Refer to DR 3640-001, *Identity, Credential, and Access Management*, for more information.

(d) Machine Issuance

1 Machine entered into Active Directory as PIV Enforced.

2 30-day exemption granted for PIV enforcement.

3 Active Directory is updated to exempt machine from PIV enforcement for 30 days.

4 Applicant is issued machine that has 30-day exemption. Refer to DR 3640-001 for more information.

(f) Enrollment

1 The Applicant schedules an appointment time and location in the scheduling tool.

2 Upon the arrival of the Applicant to the enrollment station, the Registrar locates and opens the Applicant's information, and verifies the information with the Applicant.

3 The Registrar validates and scans the Applicant's two identity source (Form I-9) documents.

4 The Registrar obtains Applicant's fingerprints (rolls and slaps) and photo and verifies that the Applicant's fingerprints can be matched to the scanned images that will be used to create the biometric template.

5 The Registrar verifies all information is correct and complete, endorsing with a digital signature.

6 The Registrar completes Applicant's enrollment file and sends to DCSA.

(g) Adjudication

1 The HSPD-12 Adjudicator receives BI results from BI Adjudicator.

2 The HSPD-12 Adjudicator enters results in the authoritative HR system.

(h) Card Production and Issuance

1 Authoritative PIV Issuance System Centralized printing:

a Credential is printed at card production facility.

b Credential is shipped to the designated shipping address.

c Finalization instructions to activate credential are emailed to the Applicant.

2 USDA Local Printing:

a Credential is printed at a designated USDA printing facility.

b Credential is transferred to the local activation station or shipped to the designated shipping address.

c Finalization instructions to activate credential are emailed to the Applicant.

(i) Activation

Most activation stations will be unattended, meaning that Applicants will use the system without assistance to activate their credentials. In the event that there is an issue causing the unattended activation to fail, the Activator will assist the Applicant in completing the activation, or collect the credential, note the issue in the system, and flag the record for issue resolution.

1 Activator verifies identity of Applicant.

2 The Activator retrieves the credential from storage.

3 Activator compares the picture on the credential with the Applicant and provides the credential to the Applicant if they match. If the picture on the credential does not match, the Activator contacts their Security Officer for resolution.

4 If the Applicant biometric sample matches the biometric read from the credential, the Applicant is authenticated to be the owner of the credential. If the biometric sample does not match the biometric read from the credential, the Activator contacts their Agency Security Officer for resolution.

5 The Applicant uses the credential number and system-generated PIN (provided to Applicant in an e-mail) to log on to the self-service activation web application.

6 The Applicant provides the primary fingerprint using the biometric card reader for a 1:1 match in the Identify Management System (IDMS) database. A successful match will result in the credential being unlocked. An unsuccessful match will result in an Activator-assisted activation process. If the Activator-assisted activation is unsuccessful, the Activator contacts the USDA HSPD-12 Help Desk at 1-833-682-4675.

7 The Endorsement screen appears requiring the Applicant's acknowledgement of agreement to terms and conditions for receipt of the credential.

8 The Applicant sets their new PIN which will be six to eight digits in length.

9 The system encodes the credential with the digital certificates and will display a confirmation when finished. The system will prompt the Applicant to remove the LincPass from the Smart Card Reader.

(j) PIV Enforcement

1 The Active Directory Administrator is notified that the PIV card has been activated.

2 The Active Directory Administrator removes the PIV exemption from the machine account in Active Directory to allow the cardholder to be LincPass compliant.

3 Applicant is issued machine that has 30-day exemption. Refer to DR 3640-001 for more information.

(k) LincPass Maintenance

1 The Sponsor maintains the cardholder's sponsorship information and updates as needed.

2 The Agency Security Officer can manually suspend or terminate cards based on derogatory information, as well as reactivate cards as appropriate.

3 Physical Access Control System (PACS) and Logical Access Control System (LACS) access are granted or revoked as appropriate.

4 The cardholder maintains their LincPass activity and renews certificates as notified.

5 In the event a card becomes damaged or defective, cards must be returned to the Agency Security Officer or mailed to USDA South Building – OSSP FPD, 1400 Independence Avenue SW, Room 1408, Washington, DC 20250.

(3) Credential Protection

Mission Area, agency, or staff offices with active roles in the HSPD-12 processes must ensure, at a minimum that the following items are secured in a lockable filing cabinet within a secured office or space:

(a) Card stock.

(b) Credentials awaiting destruction.

(c) ID Credentials not in the personal custody of authorized user.

(d) In case of emergency evacuation, stored credentials should be relocated to an alternate secure location.

## 9. USDA's HSPD-12 IMPLEMENTATION

USDA participates in the GSA Managed Service Office (MSO) USAccess program for issuance of the LincPass and AltLinc credentials. With the USAccess Program, the MSO offers a shared service that provides participating Federal agencies and departments with all the key components necessary to manage the full lifecycle of a PIV credential. The service allows for a single authoritative PIV issuance system to sponsor, enroll, issue and maintain a common identity credential for each applicant, and includes built-in workflow processes at every stage of the credentialing process for USDA's LincPass credential.

GSA MSO's Shared Service Solution also includes Mobile and Fixed Credentialing Units as well as Light Activation Stations that provide USDA Mission Areas, agencies, or staff offices with the capability to complete both activations and enrollments. USDA is responsible for maintaining and managing USDA's footprint for credentialing stations but can also leverage shared locations managed by outside federal agencies and departments.

### a. Authoritative PIV Issuance System Card Issuance Services

The LincPass card issuance lifecycle requires services to support each step of the entire lifecycle. These services are detailed in the table below.

TABLE 6 - LincPass Card Issuance Services

| **Service Name** | **Card Issuance Service Description** |
|---|---|
| a. PIV Enrollment | This service creates a record in the Identity Management Service and enables the Mission Area, agency, or staff office to submit fingerprints for initial check without incurring the cost of printing a credential. |
| b. PIV Printing and Issuance | Card printing fee includes Issuance, and activation services for a fully configured PIV credential. The PIV credential may contain up to four PKI certificates and meets NIST standards. The PIV credential will be delivered to the location designated by the Sponsor. The price includes the first month of maintenance for the credential. |

| **Service Name** | **Card Issuance Service Description** |
|---|---|
| c. PIV Credential Monthly Maintenance | Maintenance service for the PIV credential includes all of the certificates and shared services. The maintenance period starts the month following the issuance of the original PIV credential. |
| d. Re-Enrollment | Re-enrollment service allows for Mission Areas, agencies, or staff offices to request a new credential for an individual who was previously enrolled in the authoritative PIV issuance system. The action is requested because his or her credential has been compromised, lost, stolen or the credential holder has had a status or attribute changes (e.g., new legal name). |
| e. Replacement Credential | Replacement credential service allows for Mission Areas, agencies, or staff offices to order a replacement credential for an individual enrolled in the authoritative PIV issuance system. This may be required because the card no longer functions due to normal wear and tear. The action to replace is the result of a Reprint order. Customer will not be charged for credentials with manufacturer defects. |
| f. Renewal Credential | Renewal credential service allows for Mission Areas, agencies, or staff offices to order a new card for an existing and active credential holder because the individual's credential is expiring. The action will result in a new card being printed and require the individual to pick up and activate. The PIV credential will be delivered to the location designated by the Sponsor. Customer will not be charged for credentials with manufacturer defects. |

b. Credentialing Unit Services

USDA Mission Areas, agencies, and staff offices are responsible for the purchase of GSA managed equipment, inclusive of ordering Fixed Credentialing Units, Mobile Credentialing Units, Light Activation Stations, and Local Printing Services. In addition, other services that can be requested by Mission Areas, agencies, or staff offices are station moves, replacement Pelican cases, Virtual Private Network (VPN) Equipment Replacement without Field Service and technical support for setting up credentialing units. Additional information and pricing details can be found at the GSA *Fed ID Card* website.

## 10. TEMPORARY CREDENTIALS

USDA has identified categories of individuals, temporary employees or non-Federal employees, guests, and occasional visitors, who will not require LincPasses based on a credentialing risk assessment using the USDA Credential Matrix. These individuals, however, may need credentials to gain access to facilities on an unaccompanied or escorted basis. Mission Areas, agencies, or staff offices may choose to implement stricter requirements at their own discretion following the USDA Credential Matrix. Only a single credential may be issued to Federal and non-Federal personnel.

a. Site Credential or Badge

A site credential is issued locally by the facility to persons that have had a favorably adjudicated fingerprint check who do not require a LincPass and do not have IT access rights but need unaccompanied access to the workspace only. Also, a site credential is issued to individuals requiring a LincPass who have had their fingerprints taken and are waiting for credential to be printed and returned for activation. Refer to the USDA Credential Matrix for information regarding the issuance risk assessment.

b. Visitor Credential or Badge

A Visitor credential is issued locally to persons requiring temporary escorted physical access to controlled USDA facilities or assets. Each USDA Mission Area, agency, or staff office will establish their own visitor procedures.

c. AltLinc Credential

(1) USDA has implemented a PIV-I solution for individuals who are short-term Federal employees or non-Federal employees assigned to or associated with the Mission Area, agency, or staff office requiring limited access to federally controlled facilities or information systems for fewer than 6 months. USDA's PIV-I credential has been named AltLinc, as it is an alternative credential to the existing LincPass credential.

(2) AltLinc credentials will be used to control physical access to designated federally controlled facilities and logical access to designated federally controlled information systems through a contact or contactless interface. The AltLinc will be a token to allow both logical and physical access and requires a favorable fingerprint adjudication.

(3) The AltLinc will be issued using the same process as the LincPass, with the exception of the T1 BI initiation. In addition, the AltLinc process will leverage the existing roles that have been established for the LincPass process. Please refer to AltLinc policy for further information regarding AltLinc issuance and policy at the USDA HSPD-12 *Policies, Procedures, and Forms* web page.

## 11. PIV USAGE

a. Physical Access Control Systems (PACS)

(1) In concurrence with HSPD-12's goal of rapid electronic authentication, USDA has developed and implemented a FIPS PUB 201-2 compliant ePACS infrastructure in order to rapidly provision and de-provision LincPasses (and all USDA issued electronic credentials) based on the PIV process. All authentication mechanism standards described in FIPS PUB 201-2 have been met by the ePACS as mandated by the OMB. As of October 2011, all USDA PACS must be HSPD-12 compliant and interface with the USDA ePACS infrastructure. Mission Area, agency, or staff office PACS must interface with the USDA ePACS through one of the following options:

(a) Integration Option A: HSPD-12 compatible Lenel Hardware and Software that communicates directly with the USDA ePACS Lenel Infrastructure.

(b) Integration Option B: Non-Lenel HSPD-12 compatible systems that are made to communicate with the USDA ePACS Lenel infrastructure using middleware or similar technology.

(c) Integration Option C: Non-Lenel HSPD-12 compatible systems that do not communicate with the USDA ePACS, but have a verified connection to an authoritative personnel database or data feed.

(2) If Integration Option B or C is selected, a full cost benefit analysis must be completed prior to procurement of the PACS equipment. This cost benefit analysis must take into account all facets of the PACS installation, including Infrastructure Hardware costs, Infrastructure Licensing Costs, undergoing full Security Assessment and Authorization (SA&A), receiving Authorization to Operate (ATO), *Federal Information Security Modernization Act* (FISMA) Audit and Reporting of the PACS System, authoritative database, feed, and middleware development and maintenance costs and PACS Infrastructure support costs. This cost benefit analysis must be submitted the ePACS PMO for review as well as the Mission Area Assistant Chief Information Officer (CIO) and the ePACS Agency Segment Administrator (ASA) for approval.

(3) Any Mission Area, agency, or staff office facility with a PACS should have met the mandated deadline of October 2011 for full compliance. The only non-compliant PACS within USDA which do not interface with ePACS will be legacy systems installed prior this deadline. Once these systems have reached end of life, they must be replaced with an HSPD-12 compliant system as defined in OMB Memorandum M-19-17.

(4) All USDA Mission Areas, agencies, and staff offices need to establish implementation plans for the following scenarios at USDA leased and owned facilities:

(a) Converting an existing PACS to meet compliance.

(b) Purchase and installation of a new compliant PACS.

(5) The ePACS program is governed by the USDA ePACS Change Control Board which is comprised of representatives from the OSSP Facility Protection Division as well as the Mission Area Assistant CIO from each Mission Area, agency, and staff office. Mission Area, agency, or staff office participation in the ePACS program requires the establishment of a MOU between the Mission Area, agency, or staff office and the PMO. The MOU defines Mission Area, agency, or staff office responsibility as well as the identification of the Agency Segment Administrators to serve as the liaison between the Mission Area, agency, or staff office and the PMO.

(6) To participate in the ePACS program, Mission Area, agency, or staff office hardware must comply with the hardware and network requirements and specifications defined in the ePACS documentation. For copies of this documentation please contact the OSSP FPD at physicalsecurity@dm.usda.gov.

(7) Procedures for integrating PACS into ePACS are as follows:

(a) Contact the ePACS PMO before the integration of an existing PACS or new PACS installation for pre-planning and implementation guidance.

(b) If using Integration Option B or C, then prior to procuring PACS hardware and software for a new PACS installation the ePACS Cost Benefit Analysis template spreadsheet should be filled out to ensure USDA Mission Areas, agencies, or staff offices select the most cost-effective manner to meet HSPD-12 and ePACS compliance while meeting their operational security needs. Contact the OSSP FPD at physicalsecurity@dm.usda.gov for a copy of this spreadsheet.

(c) Notify the ePACS PMO of any PACS-related hardware and software that is involved in the integration with ePACS or planned to be added to ensure budget numbers are captured for software licensing for the following fiscal year.

(d) Vendors chosen to support USDA PACS facilities must be GSA approved HSPD-12 integrators, which are listed on the *Approved Products List* (APL). Review and comply with the GSA APL when ordering PACS hardware or software or services (integrators). The current APL is located at GSA, *FIPS 201 Evaluation Program* website.

(e) Chosen PACS must meet HSPD-12 compliance and interoperability requirements as well as ePACS requirements.

(f) If using Integration Option A, all USDA Mission Areas, agencies, or staff offices must submit all ePACS Change Management Requests through their ePACS ASA member. Please contact the ePACS Help Desk at 1-833-682-4675 for Mission Area, agency, or staff office POC information or assistance.

(g) If using Integration Options B or C the compliant PACS must undergo the SA&A process with security assessments according to NIST, SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, if they are not integrated into the ePACS. Contact the OCIO Information Security Center (ISC) office for SA&A requirements and deadlines.

(8) Allowing non-USDA Mission Area, agency, or staff office PIV credentials in ePACS:

(a) Each Mission Area, agency, or staff office makes an access rights and privilege determination based on the non-USDA individuals need for electronic physical access (e.g., detail to USDA; co-located space).

If access is determined to be needed, the PIV credential will need to be manually enrolled in ePACS as defined in ePACS documentation. For copies of this documentation please contact the OSSP FPD at physicalsecurity@dm.usda.gov.

(b) De-provisioning of the cards will also be a manual process until all Certificate Revocation Lists (CRL) can be pushed down to ePACS. The manual de-provisioning process can be obtained by contacting the OSSP FPD at physicalsecurity@dm.usda.gov.

b. Logical Access Control Systems (LACS)

(1) PIV operations consist of the technical interoperability requirements of HSPD-12, specifically, the technical infrastructure for providing interoperable credentials for Federal employees and non-Federal employees. All authentication mechanisms described in FIPS PUB 201-2 are to be met with the use of integrated circuit cards. As part of the GSA USAccess program, USDA is included in the USAccess System of Records Notice (SORN), Federal Personal Identity Verification Identity Management System (PIV IDMS).

(2) FIPS PUB 201-2 describes minimum technical requirements for the PIV-compliant credentials. These requirements include interfacing specifications, cryptographic specifications, Public Key Infrastructure (PKI) and certificate specifications, card topology specifications, and biometric data specifications. The PIV-compliant credentials issued will be used to control physical access to all federally controlled facilities and logical access to all federally controlled information systems through a contact or contactless interface.

(3) See DR 3640-001 for guidance related to logical access.

(4) See DR 3505-003, *Access Control for Information and Information Systems*, for guidance related to exceptions to card utilization for logical access. Additionally, there is a "Waiver Request for Long-Term Expiration" template available for Mission Area, agency, or staff offices to request logical access waivers.

(5) Refer to ICAM's Personal Identity Verification Derived Credentials Issuing Operations Plan for more information. You can also obtain additional information at the USDA *MobileLinc Credential Portal* website.

## 12. INQUIRIES

Questions regarding this DM should be directed to OSSP at 202-690-6777 or securityservicehelp@usda.gov.

-END-

# APPENDIX A

## ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| ACL | Access Control List |
| AD | Agriculture Department (Prefix for Departmental Forms) |
| AGAR | Agriculture Acquisition Regulation |
| AIM | Automatic Identification and Mobility |
| APL | Approved Products List |
| ASA | Agency Segment Administrator |
| ATO | Authorization to Operate |
| BI | Background Investigation |
| CBP | U.S. Customs and Border Protection (DHS Component) |
| CFR | Code of Federal Regulations |
| CIO | Chief Information Officer |
| CO | Contracting Officer |
| COR | Contracting Officer’s Representative |
| CRL | Certificate Revocation List |
| CVS | Central Verification System |
| DCSA | Defense Counterintelligence and Security Agency |
| DCSA/NS | Defense Counterintelligence and Security Agency/National Security |
| DG | Departmental Guidebook |
| DHS | Department of Homeland Security |
| DM | Departmental Manual |
| DPCI | Derived PIV Credential Issuers |
| DPI | Dots Per Inch |
| DR | Departmental Regulation |
| EAD | Enterprise Active Directory |
| EMM | Enterprise Mobility Management |
| EO | Executive Order |
| ePACS | Enterprise Physical Access Control System |
| eQIP | Electronic Questionnaires for Investigations Processing |
| ERT | Emergency Response Team |
| FA | Facility Administrator |
| FAR | Federal Acquisition Regulations |
| FBI | Federal Bureau of Investigation |
| FBI NCHC | Federal Bureau of Investigation National Criminal History Check |
| FD | Federal Database |
| FERO | Federal Emergency Response Official |
| FIPS PUB | Federal Information Processing Standards Publication |
| FISMA | Federal Information Security Modernization Act |
| FPD | Facility Protection Division (OSSP Component) |
| GSA | General Services Administration |
| HR | Human Resources |
| HSPD-12 | Homeland Security Presidential Directive 12 |

| | |
|---|---|
| ICAM | Identity, Credential, and Access Management |
| ID | Identification |
| IDMS | Identity Management System |
| ISC | Information Security Center (OCIO Component) |
| ISP | Investigative Service Provider |
| IT | Information Technology |
| LACS | Logical Access Control System |
| LMS | Learning Management System |
| MOU | Memorandum of Understanding |
| MSO | Managed Service Office |
| NAC | National Agency Check |
| NACI | National Agency Check with (Written) Inquiries |
| NCR | National Capital Region |
| NFC | National Finance Center |
| NIST | National Institute of Standards and Technology |
| OCIO | Office of the Chief Information Officer |
| OF | Optional Form |
| OFI | Office of Federal Investigations |
| OHRM | Office of Human Resource Management |
| OHS | Office of Homeland Security |
| OIG | Office of the Inspector General |
| OMB | Office of Management and Budget |
| OPM | Office of Personnel Management |
| OSSP | Office of Safety, Security, and Protection |
| PACS | Physical Access Control System |
| PAR | Personnel Action Request |
| PCI | Personal Identity Verification Card Issuers |
| PDF | Portable Data File |
| PDSD | Personnel and Document Security Division (OHS Component) |
| PIN | Personal Identification Number |
| PIV | Personal Identity Verification |
| PIV-D | Personal Identity Verification Derived |
| PIV-I | Personal Identify Verification Interoperable |
| PIV IDMS | Personal Identity Verification Identity Management System |
| PKI | Public Key Infrastructure |
| P.L. | Public Law |
| PM | Program Manager |
| PMO | Program Management Office |
| POC | Point of Contact |
| PRA | Paperwork Reduction Act |
| SA&A | Security Assessment and Authorization |
| SAC | Special Agreement Check |
| SAVE | Systematic Alien Verification for Entitlements |
| SF | Standard Form |
| SORN | System of Records Notice |
| SP | Special Publication |

|  |  |
|---|---|
| SSN | Social Security Number |
| SWF | Small Web Format |
| T1 | Tier One |
| U.S.C. | United States Code |
| USCIS | U.S. Citizenship and Immigration Services (DHS Component) |
| USDA | United States Department of Agriculture |
| VPN | Virtual Private Network |

# APPENDIX B

# DEFINITIONS

Appendix B provides the definitions for terms and terminology used throughout this document. The following definitions are derived from relevant policies and guidance.

Access control. Access control refers to mechanisms and policies that restrict access to computer resources. An Access Control List (ACL) specifies what operations different users can perform on specific files and directories (assets). (Source: USDA, Departmental Guidebook (DG) 0100-002, *Departmental Directives Definitions Glossary*)

Accompanied access. A person accessing the facility or information system under escort and continuous monitoring by a USDA credential holder (e.g., LincPass, Site Credential).

Agriculture Department (AD)-1197 Form. Request for USDA Identification (ID) Badge form.

AltLinc. A PIV-I credential that will be issued to USDA's short-term employee population that only requires limited logical and physical access to USDA IT systems and facilities for individuals who are employed for fewer than 6 months. Applicants will be required to undergo a minimum of an FBI fingerprint check with favorable results.

Authorization. The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to the organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation, based on the implementation of an agreed-upon set of security controls. (Source: NIST, *Glossary*, Retrieved May 3, 2021)

Barring. Prevention of entry onto Federal property.

Biometric. A measurable physical characteristic used to recognize the identity of an individual. Examples include fingerprints, and facial images. A biometric system uses biometric data for authentication purposes.

Contractor. An individual under contract to USDA (for the purpose of HSPD-12 implementation).

eAuthentication. The process of establishing an individual's identity and determining whether individual Federal employees or contractors are who they say they are.

Employee. Defined in 5 U.S.C. § 2105 "Employee," within a department or agency. "Employee" means a person, other than the President and Vice President, employed by, detailed or assigned to, USDA, including members of the Armed Forces; an expert or consultant to USDA; an industrial or commercial contractor, licensee, certificate holder, or grantee of USDA, including all subcontractors; or any other category of person who acts on behalf of an agency as determined by the agency head

EmpowHR. A Human Capital Management System, EmpowHR is an integrated suite of commercial and Government applications that can be leveraged to automate common administrative tasks associated with HR management and reduce internal operational costs using industry best practices. EmpowHR is used by several USDA Mission Areas, agencies, or staff offices.

ePACS. An Enterprise Physical Access Control System to centralize and provide a means to distribute identity data related to LincPass credentialed individuals to all USDA PACS.

ePACS Agency Segment Administrator (ASA). An ePACS ASA is the overall Mission Area, agency, or staff office point of contact and liaison between the ePACS Program Management Office (PMO) and the segment's Facility Administrators (FA) and end users. The ePACS ASA is responsible for monitoring the status of a Mission Area, agency, or staff office ePACS segment, and escalating system issues and problems from the FA to the ePACS PMO as needed.

e-QIP. The Electronic Questionnaires for Investigations Processing is a Defense Counterintelligence and Security Agency (DCSA) system that allows for the secure transmission of security questionnaires between Government agencies and DCSA.

Executive Order (EO) 10450. Security Requirements for Government Employees.

Facility Administrator (FA). A Facility Administrator is the overall Mission Area, agency, or staff office POC and liaison between the ePACS ASA and the segment's end users, including Credential Operators and Site Guards. The FA is responsible for escalating system issues and problems from the Credential Operators and Site Guards to the ePACS ASA as needed.

Federal Bureau of Investigation (FBI) Fingerprint Check. FBI National Criminal History Check. This check is an integral part of the T1 and is the minimum requirement for PIV ID credential issuance.

Federal Database (FD)-258 Form. Fingerprint Chart used to conduct contractor FBI fingerprint checks.

Federal Facility or Information System Access. Authorization granted to an individual to physically enter federally controlled facilities, and to electronically (logically) access federally controlled information systems for approved purposes.

Identity Management System (IDMS). One or more systems or applications that manage the identity verification, validation and issuance process. The IDMS software is used by PIV Registrars to enroll Applicants.

Identity-proofing. The process of providing sufficient information (e.g., driver's license, proof of current address) to a registration authority, or the process of verifying an individual's information that he or she is that individual and no other.

Lenel OnGuard. The OnGuard application vendor, Lenel, offers advanced access control, alarm monitoring, digital video, intrusion detection, asset tracking, information security integration, credential production, and employee and visitor management functionality in an enterprise structure for data redundancy and data segregation by Mission Area, agency, or staff office and location.

Limited Access. Limited access to facilities includes unaccompanied access to general common areas and workspace only. Limited access to information systems includes access to applications such as USDA email, Time & Attendance, AgLearn, and Concur.

LincPass. USDA has named their common ID card the LincPass, as it is designed to link a person's identity to an identification card and the card to a person's ability to access Federal buildings and computer systems. The spelling of LincPass is a tribute to President Abraham Lincoln, who created USDA, also known as the People's Department, in 1862.

Logical Access Control System (LACS). A protection mechanism that limits a user's access to information and restricts their type of access to only what is appropriate for them. These systems may be built into an operating system, application, or an added system.

National Capital Region (NCR). This is comprised of the District of Columbia; Montgomery and Prince Georges counties, Maryland; the cities of Alexandria, Fairfax and Falls Church, Virginia; and Fairfax, Arlington, Loudoun, and Prince William counties, Virginia.

Non-Federal employee. Persons who are not employed by USDA (e.g., contractors, affiliates, partners, volunteers, et al.) – If act on behalf of USDA and need access to USDA facilities and systems, have an authoritative identity record in USDA ICAM systems.

Optional Form (OF)-306 Form. Declaration for Federal Employment.

OPM OFI-79A Form. Report of Agency Adjudicator Action on OPM Personnel Investigations.

Person Model. Common name for EmpowHR Non-Employee Processing module. USDA's secure and authoritative database for USDA identities and non-Federal employee information required by HSPD-12. Person Model is a module of EmpowHR that feeds non-Federal employee information to the authoritative PIV issuance system, the General Services Administration (GSA) credentialing system. Sponsorship and Adjudication information for non-Federal employees is entered directly into Person Model.

Physical Access Control System (PACS). Protection mechanisms that limit a user's access to physical facilities or areas to only what is appropriate for them. These systems typically involve a combination of hardware and software (e.g., a card reader), and may involve human control (e.g., a security guard).

PIV Compliant Credential. An identity card ("smart card") also known as LincPass issued to an individual that contains stored identity credentials so that the claimed identity of the cardholder can be verified against the stored credentials by another person or by an automated process.

Public Key Infrastructure (PKI). A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. (Source: DG 0100-002)

Revocation. Referring to the termination of a credential. This refers to both the physical removal of the card from the cardholder's possession and the electronic shut off of physical and logical access.

Routine access. A person that is accessing the facility or information system without an escort or continuous monitoring by a USDA official. The Mission Area, agency, or staff office determination should be based upon the support to successfully complete USDA's mission critical functions and missions. This type of access requires a mandatory PIV ID credential to be issued.

Standard Form (SF)-85. OPM Questionnaire for Non-Sensitive Positions.

SF-85P. OPM Questionnaire for Public Trust Positions.

SF-86. OPM Questionnaire for National Security Positions.

SF-87. Fingerprint Chart used to conduct FBI fingerprint checks for federal appointees and employees and Applicants for Federal employment.

Site Credential. A credential issued locally by the facility to persons that do not need a LincPass but need access to the facility or information system to conduct temporary work.

Short Term Employee. Temporary, Term, Student, or intern with employment less than 6 months that are paid or obtaining some sort of benefit directly from USDA.

Suspension. Referring to the temporary shut off of physical and logical access to the credential without terminating the card issuance.

Tier 1 (T1) Investigation. Formerly National Agency Check with Inquiries (NACI) this is the basic and minimum investigation required on all new Federal employees and many contractors. It consists of a National Agency Check (NAC) with written inquiries and searches of records covering specific areas of a person's background during the past 5 years. Those inquiries are sent to current and past employers, schools attended, references, and local law enforcement authorities.

USDA Credential Matrix. The tool to determine a person's legitimate need for physical or logical access using a PIV or other types of credentials as outlined in HSPD-12 to USDA facilities and information systems, and the requirement to view sensitive information.

Volunteer. Under 7 U.S.C. § 2272, a volunteer is defined as an individual who willingly (without duress or intimidation) offers or agrees to provide his or her time or services without compensation, and who actually performs those services in a manner that contributes to the furtherance of the programs of USDA Mission Areas, agencies, or staff offices.

# APPENDIX C

## AUTHORITIES AND REFERENCES

The processes and procedures outlined in this DM align with the directives and standards that are listed below:

5 CFR Part 315, *Career and Career-Conditional Employment*, Subpart H (Probationary Employees)

5 CFR Part 340, *Other than Full-Time Career Employment (Part-Time, Seasonal, On-Call, and Intermittent)*

5 CFR Part 731, *Suitability*, Subparts D and E

5 CFR Part 752, *Adverse Actions*, Subparts D through F

7 CFR § 2.94, *Chief Security Director, Office of Safety, Security, and Protection*

7 CFR § 2.95, *Director, Office of Homeland Security*

5 U.S.C. § 2105, *Employee*

7 U.S.C. § 2272, *Volunteers for Department of Agriculture programs*

44 U.S.C. § 3552(b)(6)(A), *Definitions; National security System*

*Agriculture Acquisition Regulation* (AGAR)

*Agriculture Acquisition Regulation* (AGAR) 404.13, *Personal Identity Verification*

*Agriculture Acquisition Regulation* (AGAR) 452.204-70, *Personal Identity Verification of Contractor Employees*

CBP, Form I-94, *Arrival/Departure Record – Air and Sea Ports of Entry*

CBP, Form I-94A, *Arrival/Departure Record – Land Border Ports of Entry*

*E-Government Act of 2002*, 44 U.S.C. § 3501, December 17, 2002, as amended

EO 10450, *Security Requirements for Government Employees*, April 27, 1953

EO 12968, *Access to Classified Information*, August 2, 1995

EO 13467, Amending Executive Order 13467 to Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters - 2.3(b) *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, June 30, 2008

*Federal Acquisition Regulations* (FAR), Acquisition.gov

FAR, 48 CFR Subpart 4.13, *Personal Identity Verification*

FAR, 48 CFR Clause 52.204-9, *Personal Identity Verification of Contractor Personnel*

FBI, Form FD-258, *Applicant Fingerprint* Form, November 1, 2020

*Federal Information Security Modernization Act of 2014* (FISMA), 44 U.S.C. § 3551 *et seq.*, December 18, 2014, as amended

GSA, *Fed ID Card* website

GSA, *FIPS 201 Evaluation Program* website

GSA, *GoLearn* website

Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004

NIST, FIPS PUB 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013

NIST, *Glossary* website

NIST, SP 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations*, December 2018

NIST, SP 800-53 Rev 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, includes updates as of December 10, 2020

NIST, SP 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing*, June 2017

NIST, SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*, June 2017

NIST, SP 800-63C, *Digital Identity Guidelines: Federation and Assertions*, June 2017

NIST, SP 800-63-3, *Digital Identity Guidelines*, June 2017

NIST, SP 800-73-4, *Interfaces for Personal Identity Verification-Part 1: PIV Card Application Namespace, Data Model and Representation*, May 2015

NIST, SP 800-76-2, *Biometric Specifications for Personal Identity Verification*, July 2013

NIST, SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, May 2015

NIST, SP 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI),* July 2015

NIST, SP 800-85A-4, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)*, April 2016

NIST, SP 800-85B, *PIV Data Model Test Guidelines*, July 2006

NIST, SP 800-87, Rev. 2, *Codes for the Identification of Federal and Federally-Assisted Organizations*, April 2018

NIST, SP 800-96, *PIV Card to Reader Interoperability Guidelines*, September 2006

NIST, SP 800-116 Rev. 1, *Guidelines for the Use of PIV Credentials in Facility Access*, June 2018

NIST, SP 800-156, *Representation of PIV Chain-of-Trust for Import and Export*, May 2016

NIST, SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, December 2014

OMB, Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003

OMB, Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 5, 2005

OMB, Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007

OMB, Memorandum M-07-21, *Verifying the Employment Eligibility of Federal Employees*, August 10, 2007

OMB, Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, May 21, 2019

OPM, Form OF-306, *Declaration for Federal Employment*, February 2016

OPM, Form OFI-79A, *Report of Agency Adjudicator Action on OPM Personnel Investigations*

OPM, Form SF-75, *Request for Preliminary Employment Data*, August 1998

OPM, Form SF-85, *Questionnaire for Non-Sensitive Positions*, December 2013

OPM, Form SF 85P, *Questionnaire for Public Trust Positions*, December 2017

OPM, Form SF-86, *Questionnaire for National Security Positions*, November 2016

OPM, Form SF-87, *Fingerprint Chart*

OPM, OPM Operating Manual, *The Guide to Personnel Recordkeeping*, June 1, 2011

OPM, Memorandum, *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12*, July 2008

OPM, Memorandum, *Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials* ("*OPM Credentialing Standards*"),December 15, 2020

*Paperwork Reduction Act (PRA) of 1995*, Public Law (P.L.) 104-13, May 22, 1995

*Privacy Act of 1974*, 5 U.S.C. § 552a, December 31, 1974, as amended

USCIS, *Form I-9 Acceptable Documents*

USCIS, Form I-551, *Permanent Resident Card*

USCIS, Form I-766, *Employment Authorization Document*

USCIS, *Systematic Alien Verification for Entitlements* (SAVE) system

USDA, DG 0100-002, *Departmental Directives Definitions Glossary*, September 26, 2018

USDA, DR 3080-001, *Records Management*, August 16, 2016

USDA, DR 3505-003, *Access Control for Information and Information Systems*, July 17, 2019

USDA, DR 3505-005, *Cyber Security Incident Management*, November 30, 2018

USDA, DR 3540-003, *Security Assessment and Authorization*, August 12, 2014

USDA, DR 3640-001, *Identity, Credential and Access Management*, June 8, 2021

USDA, DR 4620-002, *Common Identification Standard for U.S. Department of Agriculture*, June 24, 2021

USDA, ePACS SharePoint site

USDA, Form AD-1197, *Request for USDA Identification (ID) Badge*, September 2005

USDA, *MobileLinc Credential Portal* website

USDA, OCIO, ICAM, *Personal Identity Verification Derived Credentials Issuing Operations Plan*

USDA, OCP, *USDA Contracting Desk Book*, Version 2.20, July 1, 2021, Subpart 404.13, *Personal Identity Verification*

USDA, OHS PDSD web page

USDA, *USDA HSPD-12 LincPass Destruction Guide*, Version 4.1, March 25, 2011

USDA, *USDA HSPD-12 Policies, Procedures, and Forms* web page

USDA, *USDA HSPD-12 Role Holder Training* website

APPENDIX D

USDA CREDENTIAL MATRIX

FIGURE 2 – USDA Credential Matrix

| IT and Physical Access Rights Required | Linc Pass | Alt Linc | Site Badge | Visitor Badge | No Badge |
|---|---|---|---|---|---|
| IT & Unaccompanied Physical Access Required > 6 Months | Yes | No | No | No | No |
| IT & Unaccompanied Physical Access Required < 6 Months and minimum of a tier 1 investigation is adequate for level of access | Yes | No | No | No | No |
| IT & Unaccompanied Physical Access Required < 6 Months and minimum of an FBI fingerprint check is adequate for level of access required | No | Yes | No | No | No |
| No IT Access Required & Unaccompanied Physical Access Required | No | No | Yes | No | No |
| No IT Access Required & Accompanied Physical Access Required (Including Retired USDA Employees) | No | No | No | Yes | No |
| No IT or Physical Access Required | No | No | No | No | Yes |

# APPENDIX E

# EXAMPLES OF CREDENTIAL TOPOLOGIES

## 1. FRONT REQUIREMENTS OF PIV CREDENTIAL

a. Mandatory Items on the Front of the PIV Card

(1) Zone 1F – Photograph. The photograph must be placed in the upper left corner and be a full-frontal pose from top of the head to shoulder. A minimum of 300 dots per inch (dpi) resolution must be used. The background should follow recommendations set forth in NIST SP 800-76-2, *Biometric Specifications for Personal Identity Verification*.

(2) Zone 2F – Name. The full name must be printed directly under the photograph in capital letters. The full name must be composed of a Primary Identifier (i.e., surnames or family names) and a Secondary Identifier (i.e., pre-names or given names). The printed name must match the name on the identity source documents provided during identity proofing and registration to the extent possible. The full name must be printed in the <Primary Identifier>, <Secondary Identifier>, format. The entire full name should be printed on available lines of Zone 2F and either identifier could be wrapped. The wrapped identifier must be indicated with ">" character at the end of the line. The identifiers may be printed on separate lines if each fits on one line. Departments and agencies must use the largest font size of 7 to 10-points that allows the full name to be printed. The font size 7-point allows space for 3 lines and must only be used if the full name does not fit on two lines with font size 8-point.

(3) Zone 8F – Employee Affiliation. An employee affiliation must be printed on the card. Some examples of employee affiliation are "Employee," "Contractor," "Active Duty," and "Civilian."

(4) Zone 10F – Agency, Department, or Organization. The organizational affiliation must be printed as depicted in Figure 3, *Front of PIV Credential*.

(5) Zone 14F – Card Expiration Date. The card expiration date must be printed on the card. The card expiration date must be in a YYYYMMMDD format whereby the MMM characters represent the three-letter month abbreviation as follows: JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, and DEC. The Zone 14F expiration date must be printed in Arial 6 to 9-point bold.

(6) Zone 15F – Color-Coding for Employee Affiliation. Color-coding must be used for additional identification of employee affiliation as a background color for Zone 2F (name). The following color scheme must be used:

(a) Blue – Foreign National

(b) White – Government Employee

(c) Green – Contractor

Foreign National color-coding has precedence over Government Employee and Contractor color-coding. These colors must be reserved and must not be employed for other purposes. Zone 15F may be a solid or patterned line at the Department or agency's discretion.

(7) Zone 18F – Affiliation Color Code. The affiliation color code "B" for Blue, "W" for White, or "G" for Green must be printed in a white circle in Zone 15F. The diameter of the circle must not be more than 5 mm. Note that the lettering must correspond to the printed color in Zone 15F.

(8) Zone 19F – Card Expiration Date. The card expiration date must be printed in a MMMYYYY format in the upper right-hand corner. The Zone 19F expiration date must be printed in Arial 12-point Bold.

b. Optional Items on the Front of the PIV Card – Available through the GSA USAccess Program

(1) Zone 4F – Agency Specific Text Area. If used, this area can be used for printing agency specific requirements, such as employee status.

(2) Zone 5F – Rank. If used, the cardholder's rank must be printed in this area. Data format is at the Department or agency's discretion.

(3) Zone 9F – Header. If used, the text "United States Government" must be placed as depicted in Figure 3. Departments and agencies may also choose to use this zone for other Department or agency-specific information, such as identifying a Federal emergency responder role.

(4) Zone 11F – Agency Seal. If used, the seal selected by the issuing Department, agency, or organization must be printed in the area depicted.

(5) Zone 12F – Footer. The footer is the location for the Federal Emergency Response Official identification (FERO) label. If used, a Department or agency may print "Federal Emergency Response Official" as depicted in Figure 3, preferably in white lettering on a red background. Departments and agencies may also use Zone 9F to further identify the Federal emergency respondent's official role. Some examples of official roles are "Law Enforcement," "Fire Fighter," and "Emergency Response Team (ERT)." When Zone 15F indicates Foreign National affiliation and the Department or agency does not need to highlight emergency response official status, Zone 12F may be used to denote the country or countries of citizenship. If

so used, the Department or agency must print the country name or the three-letter country abbreviation (alpha-3 format).

(6) Zone 17F – Agency Specific Data. In cases in which other defined optional elements are not used, Zone 17F may be used for other Department or agency-specific information.

(7) Zone 20F – Organizational Affiliation Abbreviation. The organizational affiliation abbreviation may be printed in the upper right-hand corner below the Zone 19F expiration date. If printed, the organizational affiliation abbreviation must be printed in Arial 12-point Bold.

c. Optional Items on the Front of the PIV Card – Not Available through the GSA USAccess Program

(1) Zone 3F – Signature. If used, the Department or agency must place the cardholder signature below the photograph and cardholder name. The space for the signature must not interfere with the contact and contactless placement. Because of card surface space constraints, placement of a signature may limit the size of the optional two-dimensional bar code.

(2) Zone 6F – Portable Data File (PDF) Two-Dimensional Bar Code. If used, the PDF bar code placement must be as depicted in Figure 3 (i.e., left side of the card). If Zone 3F (a cardholder signature) is used, the size of the PDF bar code may be affected. The card issuer should confirm that a PDF used in conjunction with a PIV Card containing a cardholder signature will satisfy the anticipated PDF data storage requirements.

(3) Zone 13F – Issue Date. If used, the card issuance date must be printed above the Zone 14F expiration date in YYYYMMMDD format.

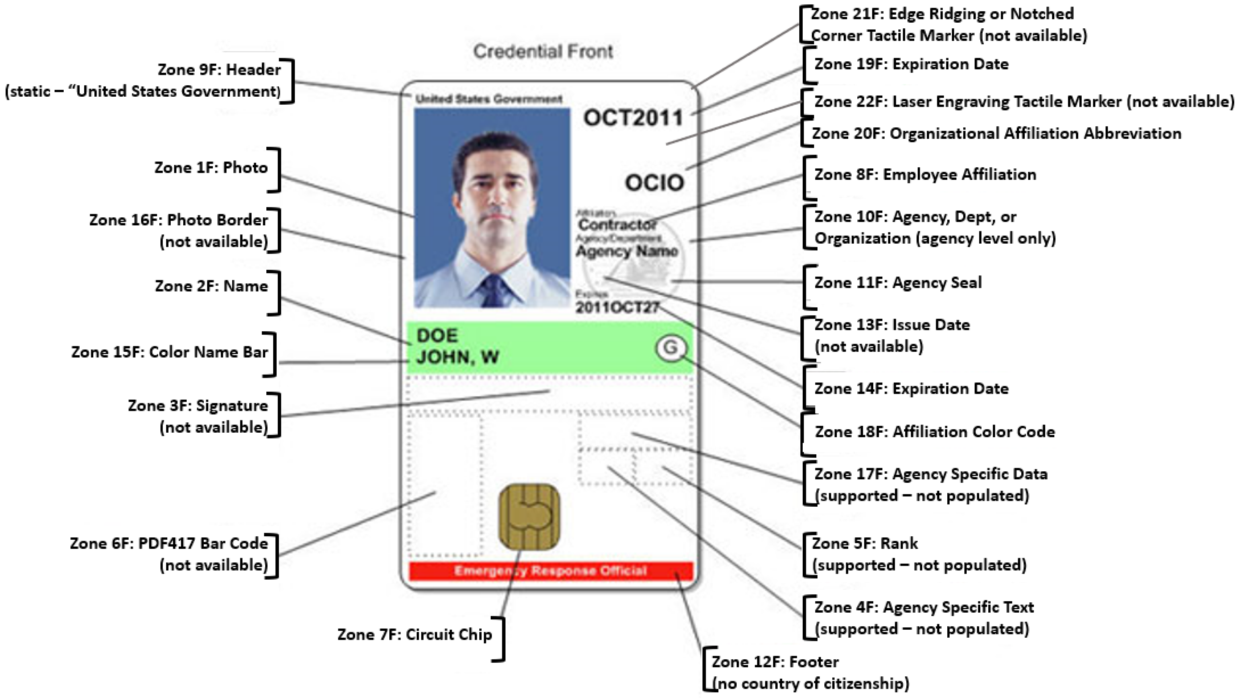
(4) Zone 16F – Photo Border. A border may be used with the photo to further identify employee affiliation. This border may be used in conjunction with Zone 15F to enable Departments and agencies to develop various employee categories. The photo border must not obscure the photo. The border may be a solid or patterned line. For solid and patterned lines, red must be reserved for emergency response officials, blue for foreign nationals, and green for contractors. All other colors may be used at the Department or agency's discretion.

(5) Zone 21F – Edge Ridging or Notched Corner Tactile Marker. If used, this area must incorporate edge ridging or a notched corner to indicate card orientation. Departments and agencies should ensure such alterations are closely coordinated with the card vendor or manufacturer to ensure the card material integrity and printing process is not adversely impacted.

(6) Zone 22F –Laser Engraving Tactile Marker. If used, tactilely discernible marks must be created using laser engraving to indicate card orientation. There must be an opening in the lamination foil where laser engraving is performed. Departments and agencies should ensure such alterations are closely coordinated with the card vendor or manufacturer to ensure the card material integrity and printing process is not adversely impacted.

Figure 3, *Front of PIV Credential*, below provides a graphic copy of the front of a PIV Credential Badge and explanation of the zones.

FIGURE 3 – Front of PIV Credential


Credential Front
United States Government
OCT2011
OCIO
Affiliation
Contractor
Agency/Department
Agency Name
Expires
2011OCT27
DOE
JOHN, W
G
Emergency Response Official
Zone 9F: Header
(static – "United States Government)
Zone 1F: Photo
Zone 16F: Photo Border
(not available)
Zone 2F: Name
Zone 15F: Color Name Bar
Zone 3F: Signature
(not available)
Zone 6F: PDF417 Bar Code
(not available)
Zone 7F: Circuit Chip
Zone 21F: Edge Ridging or Notched
Corner Tactile Marker (not available)
Zone 19F: Expiration Date
Zone 22F: Laser Engraving Tactile Marker (not available)
Zone 20F: Organizational Affiliation Abbreviation
Zone 8F: Employee Affiliation
Zone 10F: Agency, Dept, or
Organization (agency level only)
Zone 11F: Agency Seal
Zone 13F: Issue Date
(not available)
Zone 14F: Expiration Date
Zone 18F: Affiliation Color Code
Zone 17F: Agency Specific Data
(supported – not populated)
Zone 5F: Rank
(supported – not populated)
Zone 4F: Agency Specific Text
(supported – not populated)
Zone 12F: Footer
(no country of citizenship)

2. BACK REQUIREMENTS OF PIV CREDENTIAL

a. Mandatory Items on the Back of the PIV Card

(1) Zone 1B – Agency Card Serial Number. This item must be printed as depicted in Figure 4, *Back of PIV Credential* and contain the unique serial number from the issuing Department or agency. The format must be at the discretion of the issuing Department or agency.

(2) Zone 2B – Issuer Identification Number. This item must be printed as depicted in Figure 4 and consist of six characters for the Department code, four characters for the agency code, and a five-digit number that uniquely identifies the issuing facility within the Department or agency.

b. Optional Items on the Back of the PIV Card – Available through the GSA USAccess Program

(1) Zone 4B – Return Address. If used, the "return if lost" language must be generally placed on the back of the card.

(2) Zone 5B – Physical Characteristics of Cardholder. If used, the cardholder physical characteristics (e.g., height, eye color, hair color) must be printed in the general area illustrated in Figure 4.

(3) Zone 7B – Standard Section 499, Title 18 Language. If used, standard Section 499, Title 18, language warning against counterfeiting, altering, or misusing the card must be printed in the general area depicted in Figure 4.

c. Optional Items on the Back of the PIV Card – Not Available through the GSA USAccess Program

(1) Zone 3B – Magnetic Stripe. If used, the magnetic stripe must be high coercivity and placed in accordance Figure 4.

(2) Zone 6B – Additional Language for Emergency Response Officials. Departments and agencies may choose to provide additional information to identify emergency response officials or to better identify the cardholder's authorized access. If used, this additional text must be in the general area depicted and must not interfere with other printed text or machine-readable components.

(3) Zone 8B – Linear 3 of 9 Bar Code. If used, a linear 3 of 9 bar code must be generally placed as depicted in Figure 4. It must be in accordance with Association for Automatic Identification and Mobility (AIM) standards. Beginning and end points of the bar code will be dependent on the embedded contactless module selected. Departments and agencies are encouraged to coordinate placement of the bar code with the card vendor.

(4) Zone 9B – Agency-Specific Text. In cases in which other defined optional elements are not used, Zone 9B may be used for other Department or agency-specific information. For example, emergency response officials may use this area to provide additional details.

(5) Zone 10B – Agency-Specific Text. Zone 10 is similar to Zone 9 in that it is another area for providing Department or agency-specific information. For Zones 9 and 10, Departments and agencies are encouraged to use this area prudently and minimize

printed text to that which is absolutely necessary. In the case of the Department of Defense, the back of the card will have a distinct appearance. This is necessary to display information required by the Geneva Accord and to facilitate legislatively mandated medical entitlements.

Figure 4, *Back of PIV Credential*, below provides an example of the back of a PIV Credential Badge and explanation of badge zones.

FIGURE 4 – Back of PIV Credential

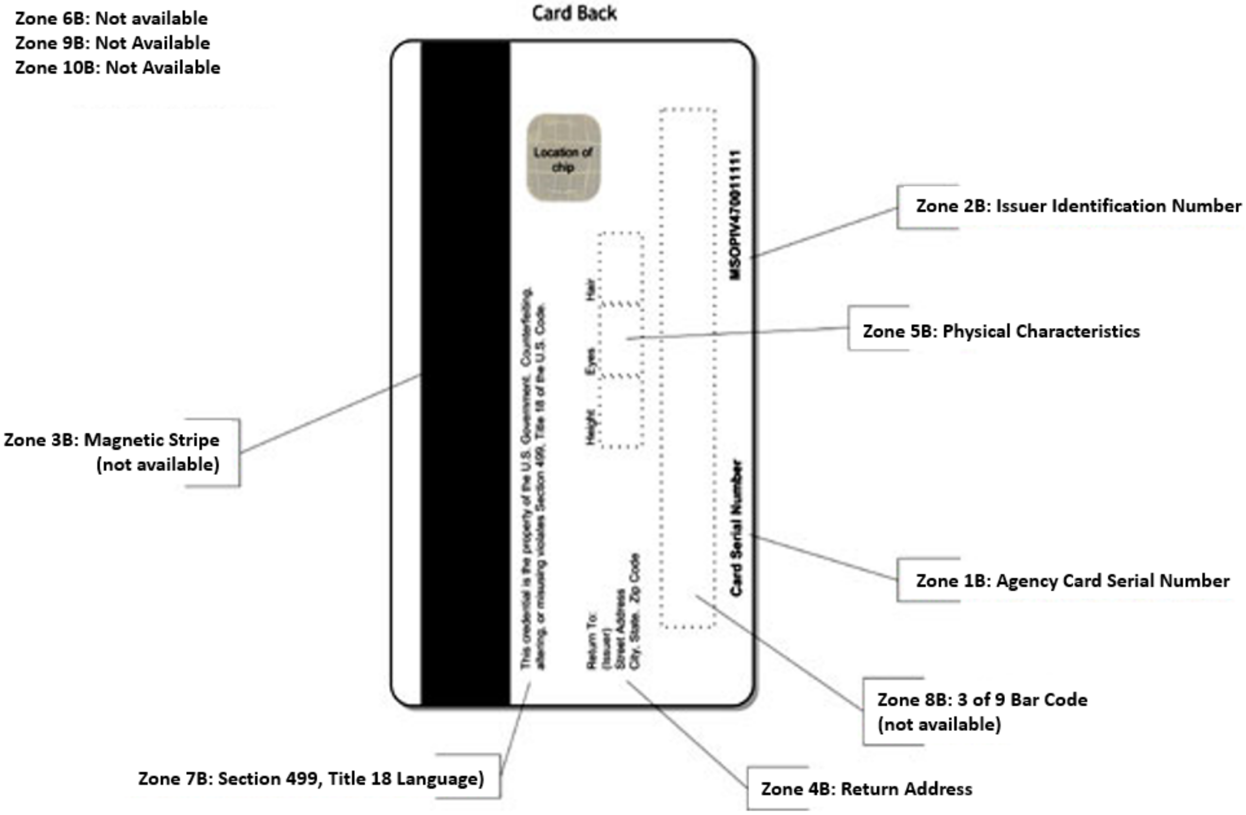
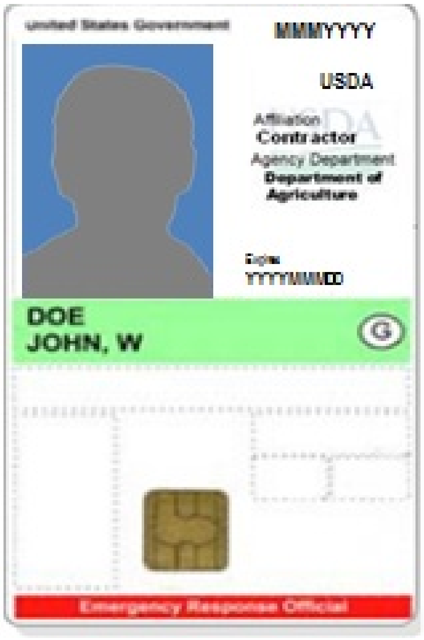

Card Back
Zone 6B: Not available
Zone 9B: Not Available
Zone 10B: Not Available
Location of chip
MSOPIV470011111
Zone 2B: Issuer Identification Number
Hair
Eyes
Height
Zone 5B: Physical Characteristics
This credential is the property of the U.S. Government. Counterfeiting, altering, or misusing violates Section 499, Title 18 of the U.S. Code.
Zone 3B: Magnetic Stripe (not available)
Card Serial Number
Zone 1B: Agency Card Serial Number
Return To:
(Issuer)
Street Address
City, State. Zip Code
Zone 8B: 3 of 9 Bar Code (not available)
Zone 7B: Section 499, Title 18 Language)
Zone 4B: Return Address

Figure 5, *LincPass Topology*, below provides an example of the LincPass topology. The LincPass name bar color coding is explained in the section below the LincPass badge.

FIGURE 5 – LincPass Topology



3. USDA LINCPASS NAME BAR COLOR CODING

a. Coding for Federal Employee – White. An individual employed by, detailed to, or assigned to USDA under the authority of 5 U.S.C. § 2105, *Employee,* and receives Government funding for services rendered.

b. Coding for USDA Affiliation – Contractors: Green. An individual under contract (i.e., prime or sub-contract) to USDA requiring routine unaccompanied access to USDA-controlled facilities and USDA-controlled information systems.

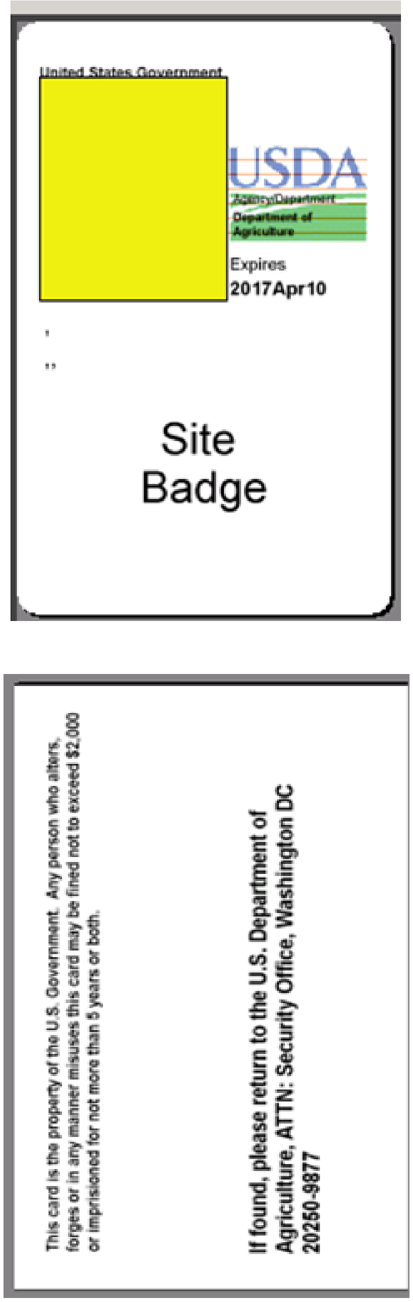
c. Coding for USDA Affiliation – Associate or Dignitary: White. An individual under a grant or agreement to USDA requiring routine unaccompanied access to USDA-controlled facilities and USDA-controlled information systems.

d. Coding for USDA Affiliation – Foreign National: Blue. An individual who is employed by, detailed to, or assigned to USDA but who is not a citizen or permanent resident alien of the U.S. The foreign national color coding takes precedence over the Federal Employee, Contractor, or Associate or Dignitary color designation.

e. Coding for USDA Affiliation—Federal Emergency Response Official (FERO). A FERO will be annotated with a red band in the footer. Mission Area, agency, or staff offices are responsible for determining who should be authorized the coding of FERO.

Figure 6, *Site Credential Topology*, below provides an example of a Site Credential badge topology.

FIGURE 6 – Site Credential Topology

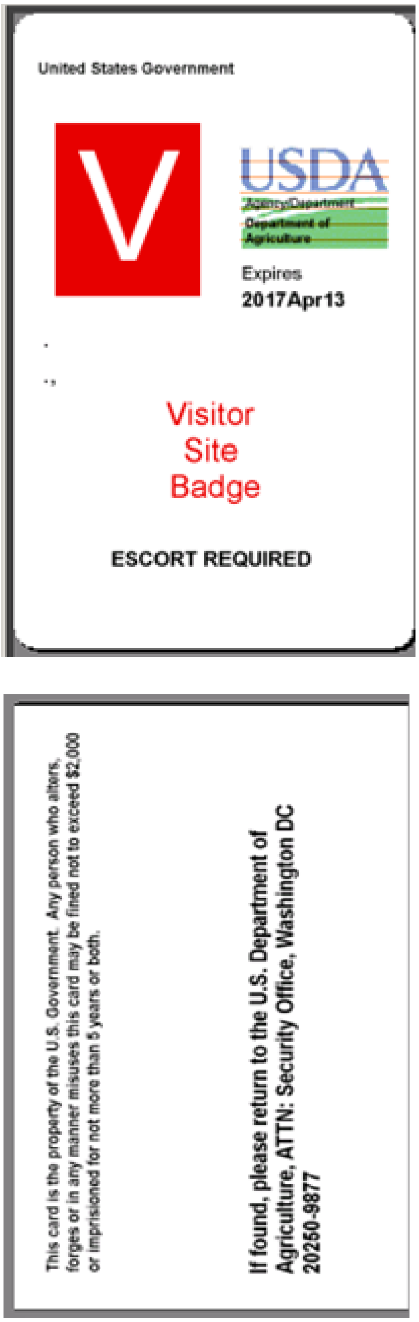


This card is the property of the U.S. Government. Any person who alters, forges or in any manner misuses this card may be fined not to exceed $2,000 or imprisoned for not more than 5 years or both.

If found, please return to the U.S. Department of Agriculture, ATTN: Security Office, Washington DC 20250-9877

Figure 7, *Visitor Site Badge Topology*, below provides an example of USDA Visitor Site Badge topology.

FIGURE 7 – Visitor Site Badge Topology



United States Government

V

USDA

Agency/Department

Department of Agriculture

Expires

2017Apr13

Visitor Site Badge

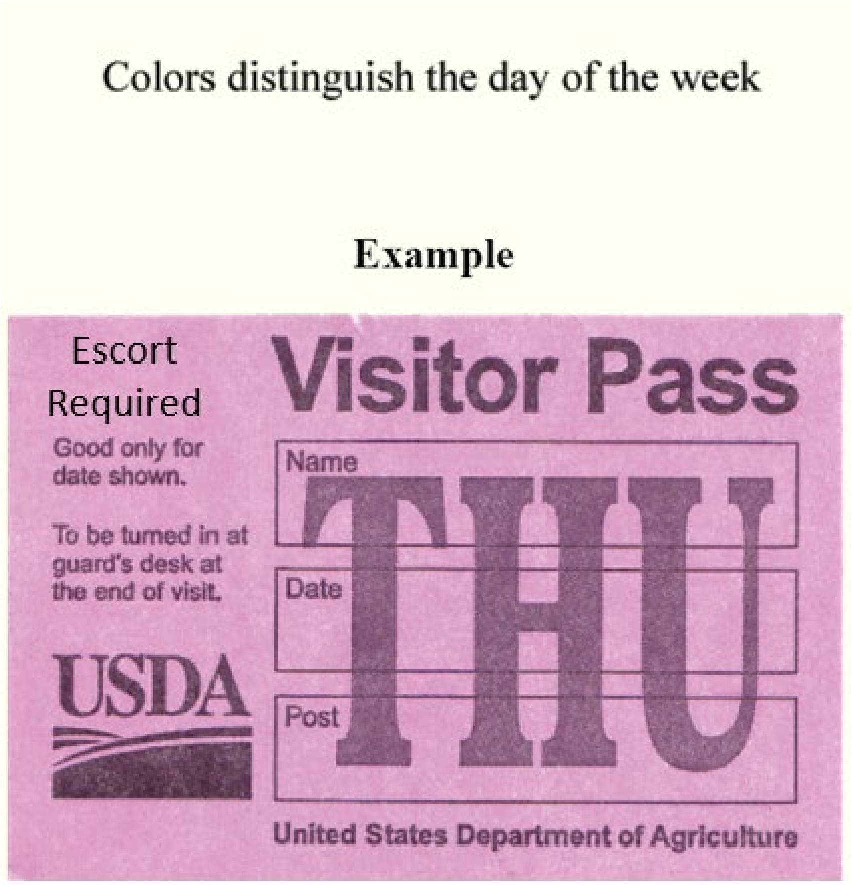
ESCORT REQUIRED

This card is the property of the U.S. Government. Any person who alters, forges or in any manner misuses this card may be fined not to exceed $2,000 or imprisoned for not more than 5 years or both.

If found, please return to the U.S. Department of Agriculture, ATTN: Security Office, Washington DC 20250-9877

Figure 8, *Paper Visitor Pass*, below provides an example of a paper Visitor Pass.

FIGURE 8 – Paper Visitor Pass



Colors distinguish the day of the week

**Example**

Escort Required

Good only for date shown.

To be turned in at guard's desk at the end of visit.

USDA

Visitor Pass

THU

Name

Date

Post

United States Department of Agriculture

4. PIV-I TOPOLOGY

   The PIV-I cards are visually different from a PIV card as shown below. PIV-I credential orientation is landscape vs. portrait orientation of PIV.

5. FRONT REQUIREMENTS OF PIV-I CREDENTIAL

   a. Mandatory Items on the Front of the PIV-I Card

      (1) Zone 1F-I – Photo

      (2) Zone 2F-I – Full Name

(3) Zone 7F-I – Circuit Chip

(4) Zone 9F-I – Header (Static – "United States Government)

(5) Zone 10F-I – Agency, Department, or Organization Affiliation

(6) Zone 11F-I – Agency Seal

(7) Zone 14F-I – Expiration Date

(8) Zone 15F-I – Color Name Bar

(9) Zone 18F-I – Affiliation Color Code

(10) Zone 19F-I – Expiration Date

(11) Zone 20F-I – Organizational Affiliation Abbreviation

b. Optional Items on the Front of the PIV-I Card – Available through the GSA USAccess Program

(1) Zone 4F-I – Agency Specific Text

(2) Zone 5F-I – Rank

(3) Zone 17F-I – Agency Specific Data

c. Optional Items on the Front of the PIV-I Card – Not Available through the GSA USAccess Program

(1) Zone 3F-I – Signature

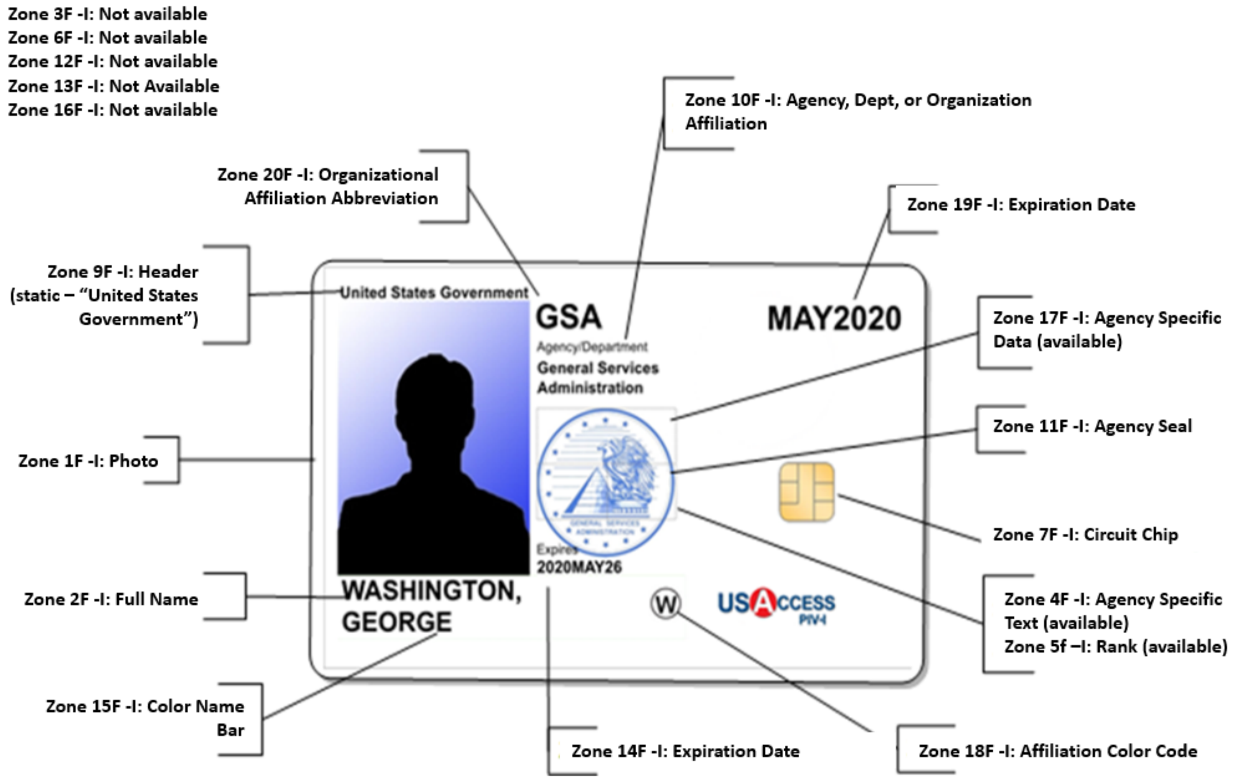
(2) Zone 6F-I – Portable Data File (PDF) Two-Dimensional Bar Code

(3) Zone 12F-I – Footer

(4) Zone 13F-I – Issue Date

(5) Zone 16F-I – Photo Border

FIGURE 9 - AltLinc PIV-I Topology – Card Front


Zone 3F -I: Not available
Zone 6F -I: Not available
Zone 12F -I: Not available
Zone 13F -I: Not Available
Zone 16F -I: Not available
Zone 10F -I: Agency, Dept, or Organization Affiliation
Zone 20F -I: Organizational Affiliation Abbreviation
Zone 19F -I: Expiration Date
Zone 9F -I: Header (static – "United States Government")
United States Government
GSA
MAY2020
Agency/Department
General Services Administration
Zone 17F -I: Agency Specific Data (available)
Zone 11F -I: Agency Seal
Zone 1F -I: Photo
Zone 7F -I: Circuit Chip
Expires
2020MAY26
Zone 2F -I: Full Name
WASHINGTON, GEORGE
W
USAccess
PIV-I
Zone 4F -I: Agency Specific Text (available)
Zone 5f –I: Rank (available)
Zone 15F -I: Color Name Bar
Zone 14F -I: Expiration Date
Zone 18F -I: Affiliation Color Code

6. BACK REQUIREMENTS OF PIV-I CREDENTIAL

a. Mandatory Items on the Back of the PIV-I Card

(1) Zone 1B-I – Serial Number

(2) Zone 2B-I – Issuer Identification Number

(3) Zone 3B-I – Magnetic Stripe

(4) Zone 4B-I – Return Address

(5) Zone 5B-1 – Physical Characteristics

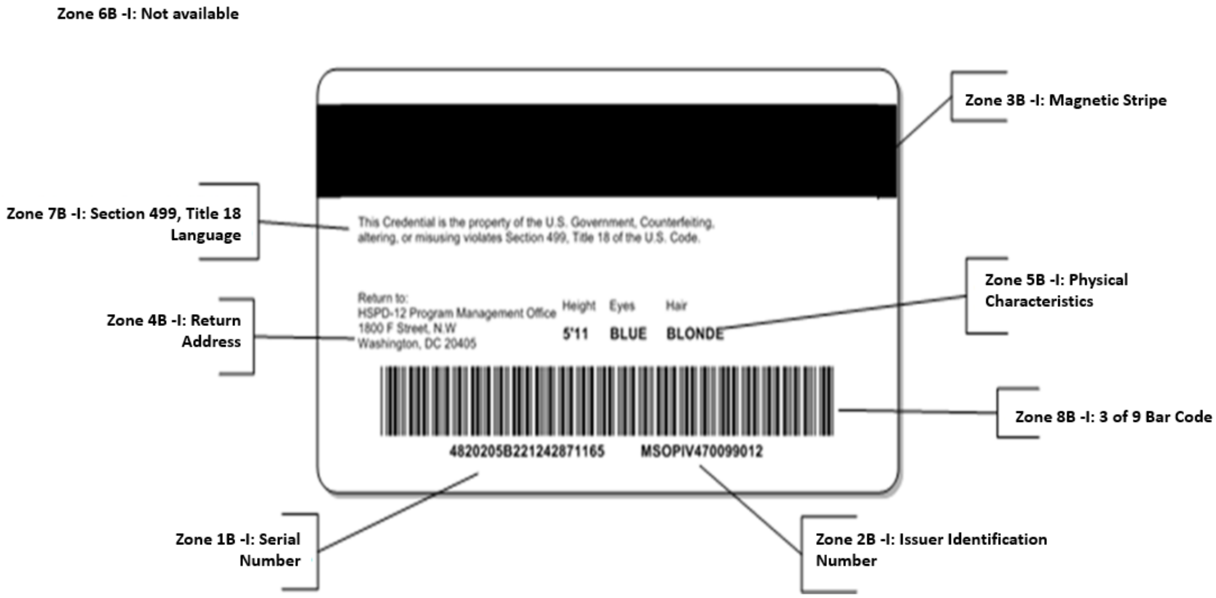
(6) Zone 7B-I – Section 499, Title 18 Language

(7) Zone 8B-I – 3 of 9 Bar Code

b. Optional Items on the Back of the PIV-I Card – Not Available through the GSA USAccess Program

(1) Zone 6B-I – Additional Language for Emergency Response Officials

FIGURE 10 - AltLinc PIV-I Topology – Card Back


Zone 6B -I: Not available
Zone 3B -I: Magnetic Stripe
Zone 7B -I: Section 499, Title 18 Language
This Credential is the property of the U.S. Government, Counterfeiting, altering, or misusing violates Section 499, Title 18 of the U.S. Code.
Zone 5B -I: Physical Characteristics
Zone 4B -I: Return Address
Return to:
HSPD-12 Program Management Office
1800 F Street, N.W
Washington, DC 20405
Height
Eyes
Hair
5'11
BLUE
BLONDE
Zone 8B -I: 3 of 9 Bar Code
4820205B221242871165
MSOPIV470099012
Zone 1B -I: Serial Number
Zone 2B -I: Issuer Identification Number