United States
Department of
Agriculture

Food and Nutrition
Service

3101 Park Center
Drive

Alexandria, VA
22302-1500

To: All FNCS Employees and Contractor Personnel

Subject: FNCS 702 Handbook, Information Systems Security Guidelines and Procedures

Date: August 18, 2014

The FNCS 702 Handbook, Information Systems Security Guidelines and Procedures, has been updated. The updated procedures are included as an attachment to this memo and can be found in the E-Library under FNS Instructors and Handbooks.

The 702 Handbook provides guidance for maintaining the confidentiality, integrity, and availability of FNCS Information System Resources. All procedures were written in accordance of USDA policies in the Cyber Security Department Manual, series 3500, National institute of Standards and Technology (NIST), Federal Information Security Management Act (FISMA) 800-53 publications, Office of Management and Budget (OMB) regulations, and Federal Information Processing Standards (FIPS).

The FNCS 702 Handbook is a key element of the FNCS Information System Security Program (ISSP). As the ISSP evolves, the Office of Information Technology will provide future updates to the 702 Handbook with additional information security guidance.

As an FNCS employee or contractor, you have a responsibility to understand your role in information security. By adhering to the guidance as written in the 702 Handbook, we can avoid potential security vulnerabilities that can obstruct the accomplishment of the FNCS mission.

If you have any questions about the FNCS 702 Handbook, please contact Leo Wong in the Information Security Office at (703) 605-1181.

Rory Schultz
USDA/Food Nutrition Services
Acting Chief Information Officer

FNS Handbook 702
Version 3.0

INFORMATION SYSTEMS SECURITY

GUIDELINES & PROCEDURES

PREPARED BY: INFORMATION SECURITY OFFICE

RELEASE DATE: SEPTEMBER 2014

Document Control

This is a controlled document produced by the United States Department of Agriculture (USDA), Food, Nutrition and Consumer Services, Chief Information Officer (CIO). The control and release of this document is the responsibility of the Information Security Office (ISO) and document owner.

Issue Control	
Document Reference	FNCS 702 v3.0
Document Title	FNCS Information System Security Guidelines and Procedures 702 Handbook, v3.0

Document Owner Details	
Name	Leo Wong
Contact Number	703-605-1181
E-mail Address	Leo.Wong@fns.usda.gov

Revision History			
Revision	**Date**	**Author**	**Comments**
1.0	January 2008	Carol Ware, ISO	Created original version of the 702 Handbook.
1.1 Draft	October 2008	Information Security Office (ISO)	Updated entire document. Added 4 new guidelines
1.2 Draft	October 2009	Bill Ramo	Revised Draft
1.3 Draft	November 2010	Leo Wong	Updated Document
1.4 Draft	August 2011	Vishad Pathak	Updated frequency of review for monitoring least privilege, IT restricted space.
1.5 Draft	October 2011	Vishad Pathak	Updated PII, mobile code usage, and foreign use policies.
1.6 Draft	December 2011	Leo Nguyen	Updated Citrix Policy
2.0	March 2012	Information Security Office	Updated Release
2.1	June 2013	Information Security Office	Annual Update
3.0	August 2013	Information Security Office	Annual Update – Added reference to Child System and

			Application Assessment Policy, V1.0 – Added reference to IR policy – Added Vulnerability Policy

Distribution List			
Name	**Title**	**Agency/Office**	**Contact Information**
Food, Nutrition and Consumer Services	All Personnel	FNCS/All	

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

[**This page intentionally left blank.]**

Information System Security Overview

The purpose of the FNCS Information Systems Security Guidelines and Procedures is to protect agency information and information processing assets from theft, fraud, misuse or unauthorized modification. This Handbook addresses requirements and guidance set forth by the Federal Information Security Management Act (FISMA). It also encompasses minimum security controls as required by the Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems; and defined by the current National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, commensurate with security categorization defined by FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

- Information used by any business enterprise must be safeguarded against tampering, loss, unauthorized disclosure, denial of service, destruction and must be available when and where needed.
- IT Information Security guidance applies to the areas of: administrative, physical and/or environmental, personnel, professional behavior, communications, and computer security (e.g., hardware and software).
- All guidelines within the 702 Handbook are written in accordance with USDA policies within the Department Manual Cyber Security 3500-3599 series and the Department Regulations, and NIST Special Publications.
- FNCS IT systems should not process or contain any Classified, Secret, or Top Secret data. Control measures are in place to protect FNCS data and the supporting IT systems commensurate with the sensitivity of the data. If any classified data should pass through the FNCS network, users are to contact the Information Security Office (ISO) at SecurityOfficers.Mailbox@fns.usda.gov
- Mechanisms shall be integrated into the FNCS architecture to detect and minimize inadvertent and/or malicious modification or destruction of FNCS data.
- All FNCS employees, contractors, state partners and official visitors shall adhere to the guidelines within the 702 Handbook and ensure that information is used only for its intended purpose, retains its content integrity, and is marked properly as required.
- Requests to deviate from FNCS security policies must be approved by the FNCS Chief Information Officer (CIO) prior to implementation.
- For assistance or questions on FNCS Information Systems Security Guidelines and Procedures, please contact the ISO at SecurityOfficers.Mailbox@fns.usda.gov .

Enforcement Statement

Compliance with this Handbook is mandatory. Violations of the Information Systems Security Guidelines and Procedures as stated in the 702 Handbook may lead to immediate removal from the FNCS Network and/or may be the basis for disciplinary action. Supervisors and/or management officials considering disciplinary action must consult with the Labor & Employee Relations Branch in the Human Resources Division prior to taking any action.

Update and Review

Policies will be reviewed, at minimum, on an annual basis. Policies may be reviewed more frequently as necessary.

Information System Security Planning at FNCS

050 Overview

In a world of evolving threats to our information systems, it has become clear that we must continuously ensure we are satisfying a level of information security within FNCS that meets with the information we are expected to protect. System Security Plans (SSP) have become the foundation document in the overall security process since they define the system security features and controls.

SSPs support Capital Planning and Investment Control (CPIC), Federal Information Security Management Act (FISMA) reporting, System Life Cycle efforts, Risk Management activities as well as the Certification and Accreditation of Information Technology (IT) systems. Therefore, it is critical that they be prepared and updated on an ongoing basis with the most current information concerning each agency's information security practices.

060 References

This Guidance is written in accordance with:

- NIST Special Publication 800-53 Rev. 3
- DM 3565-001 USDA Annual Security Plans for Information Technology Systems

070 Guidelines

The FNCS System Security Plan consists of three (3) security control classes: Management, Operational and Technical.

The three classes and control families are described as follows:

071 Management Controls

Management Controls focus on the management of the information system and the management of risk for a system. Management Controls are techniques and concerns that are normally addressed by FNCS Management. Control families for the Management Controls are:

1. Security Assessment and Authorization (CA)
2. Planning (PL)
3. Risk Assessment (RA)
4. System and Services Acquisition (SA)
5. Program Management (PM)

072 Operational Controls

Operational Controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

Control families included in the Operational Controls are:

1. Awareness and Training (AT)
2. Configuration Management (CM)
3. Contingency Planning (CP)
4. Incident Response (IR)
5. Maintenance (MA)
6. Media Protection (MP)
7. Physical and Environmental Protection (PE)
8. Personnel Security (PS)
9. System and Information Integrity (SI)

073 Technical Controls

Technical Controls focus on security controls executed by computer systems. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. Control families included in the Technical Controls are:

1. Access Control (AC)
2. Audit and Accountability (AU)
3. Identification and Authentication (IA)
4. System and Communications Protection (SC)

074 Security Tools

Security tools are used at FNCS to provide effective security protection for FNCS Information resources and are used as part of the comprehensive security process to monitor compliance for some of the aforementioned control families. Some of the security tools utilized at FNCS are:

1. Vulnerability Scanning
2. Firewalls
3. Anti-virus Program
4. Encryption
5. Log Management Tool

The NIST Special Publication 800-53 Revision 3 (page F-1) outlines the recommended security controls that are management, operational and technical security domains for low, moderate, and high baseline systems. The FNCS security program is compliant to FISMA security requirements as well as FIPS 199 regulations for security categorization of Federal information systems and FIPS 200 regulations for the minimum security requirements for Federal information systems.

080 FNCS Information System Security Compliance

The Guidance established within this document authorizes the ISO to promote and execute information security control compliance for all phases of the System Development Life Cycle (SDLC), Capital Planning and Investment Control (CPIC), operations & maintenance, and other IT functions that may impact the effectiveness of maintaining the confidentiality, integrity, or availability of FNCS data.

The table below highlights the relevant sections created to comply with the Management (indicated as “M” on the table), Technical (indicated as “T” on the table) and Operational (indicated as “O” on the table) controls for FNCS System Security Plans.

ID	Security Requirements	Section Series
SA	System and Services Acquisition (M)	Section 100
SC	System and Communications Protection (T)	Section 200
IR	Incident Response (O)	Section 400
AU	Audit and Accountability (T)	Section 500
AC	Access Control (T)	Section 600
IA	Identification and Authentication (T)	Section 600
PE	Physical and Environmental Protection (O)	Section 700
AT	Awareness and Training (O)	Section 800
CA	Security Assessment and Authorization (M)	Section 900
PM	Program Management (M)	Section 1000
RA	Risk Assessment (M)	Section 1200
CP	Contingency Planning (O)	Section 1300
PL	Planning (M)	Section 1600
MA	Maintenance (O)	Section 1700
MP	Media Protection (O)	Section 1800
PS	Personnel Security (O)	Section 1900

Table 1 – FNCS Information System Security Plan Families and Identifiers

081 Compliance Program: The FISMA Scorecard

The FNCS ISO responds to Department requirements to report specific FISMA scorecard variables used to measure and ensure compliance to security controls for each system at FNCS. The scorecard reports on the total score and grade for:

1. Systems Inventory
2. CSAM Controls
3. Systems scheduled for a Certification & Accreditation (C&A)
4. Plan of Actions and Milestones (POA&Ms) and due dates
5. Contingency planning
6. Monthly scanning
7. Monthly patching
8. USDA Information Security Awareness (ISA) Training
9. Specialized IT Training
10. Annual Assessments and Authorization (A&A)
11. Annual Security Plans
12. Privacy Impact Assessment (PIA)
13. Privacy Threshold Analysis (PTA)
14. Systems of Records
15. United States Government Configuration Baseline (USGCB)
16. Whole Disk Encryption
17. Security Incidents
18. Wireless Devices

The FNS Information Security Office (ISO) conducts monthly compliance reviews and reports on security data such as the status for overdue POA&Ms, monthly patches, and scan information. The results of the reviews and reports are communicated via a FISMA scorecard that is reported to USDA. The CIO reviews and approves the FISMA scorecard and reports to USDA. In the event that non-compliance is discovered, the system owners are given an opportunity to create POA&Ms that documents the planned, implemented and evaluated remedial actions to correct the deficiency or non-compliance. POA&Ms are currently entered into the Cyber Security Assessment and Management tool (CSAM).

082 Standard Operating Procedures (SOPs)

FNCS has developed various SOPs detailing the procedure for maintaining security tools used at FNCS, including: vulnerability scanning, patch management, firewalls, anti-virus program, data encryption and log management. These SOPs are necessary to maintain compliance.

083 Security Assessments

FNCS, through the ISO, performs annual security assessments of security controls for FNCS systems. The assessments are required for OMB A-123 Management Controls of financial systems and NIST SP 800-53 of FISMA reportable systems, including financial and non-financial and General Support Systems (GSS).

FNCS may be selected to participate in OIG audits of FISMA controls on an annual basis.

Guidance on Acceptable Use of FNCS Information Resources

100 Overview

Acceptable use provides guidelines on the proper usage of networks. It also details behaviors that are acceptable and unacceptable on the FNCS Network.

This guidance applies to all FNCS Users (i.e., employees, contractors, official visitors (including external clients and third party vendors with access to the network) for both internal and remote access connections to the FNCS Network).

The purpose of this 702 Handbook is to document security policies and procedures, in accordance with Federal government mandated requirements for connecting to the FNCS network from any device. Acceptable Use is to set forth the principles that govern appropriate use of FNCS information resources and is intended to promote the efficient, ethical, and lawful use of the resources. Access to Government Furnished Equipment (GFE) and the FNCS network is a privilege which imposes certain responsibilities and obligations to each FNCS users.

110 References

This Guidance is written in accordance with:

- NIST Special Publication 800-53 Rev. 3
- DN 3300-011 USDA Commercial Wireless Technologies
- DM 3525-000 USDA Internet and E-mail Security
- DR 3300-001, DR 3300-1-A through DR 3300-1-M

120 Guidelines

When using FNCS information resources, FNCS users shall:

- Ensure the ethical use of FNCS information resources in accordance with FNCS guidelines and procedures.
- Acknowledge that FNCS has the right to restrict or rescind network privileges at anytime.
- Utilize all security measures that are in place to protect the confidentiality, integrity and availability of information and systems.
- Refrain from using FNCS information resources for inappropriate activities.
- Adhere to all licenses, copyright laws, contracts, and other restricted or proprietary information.
- Always safeguard user IDs, passwords, and smartcards.
- Access only those information systems, networks, data, control information, and software that you are authorized to use.

- Use any special accounts to which they have been given access (privilege, system, etc.) only for the purposes for which the account was intended. Users should not modify accounts or elevate other accounts with privileged accounts without written approval from the Information Security Office.
-
- Know who the Information System Security Officers (ISSO) are and how to contact them

.

- Determine the sensitivity of the information and programs on their computing resources (e.g., non-sensitive, sensitive but unclassified). Please refer to the Guidance and Protection of SBU Information for more detail. Sensitivity of information is also classified by security categorizations. Refer to NIST SP 800-53 Revision 3, Page 18 for more information or refer to the FIPS 199 guidelines on security categorizations.

- Avoid the introduction of harmful files/data that may contain spy-ware, viruses, etc. into any computing resource.

130 Personal Use

Federal employees are permitted limited use of GFE for personal needs if the use does not interfere with official business and involves minimal additional expense to the Government. This policy also applies to contractor personnel, interns, and other non-government employees through incorporation by reference in contracts or memorandums of agreement as conditions for using GFE and space. This limited personal use of GFE should take place during the employee's personal time, not during official duty time. This privilege to use GFE for non-government purposes may be revoked or limited at any time by appropriate Federal agency or department officials. Below are guidelines on the acceptable and unacceptable personal use at FNCS.

131 Acceptable Personal Use

FNCS Users shall have limited personal use of FNCS information systems if it is determined that such communication:

- Does not adversely affect the performance of their official duties or degrade the performance of the network (e.g., any personal use that could cause congestion, delay or disruption of service to FNCS Information Systems or equipment).

- Does not put Federal Government telecommunication systems to uses that would reflect adversely on FNCS, to include activities that are illegal, inappropriate, or offensive to fellow employees, partners, contractors or the public.

132 Unacceptable Personal Use

Employees are not to connect any personal equipment to GFE; this restriction includes but is not limited to:

- Personal removable media (flash drives, external hard drives, etc.);
- Personal Mobile Devices; and
- Any other type of Personal Electronic Property

Employees are reminded that they should not try to read media such as CD-ROMs using their GFE unless they can confirm the source of the media. Using unfamiliar media on GFE increases the probability of system comprises. Users should always validate the source before using.

Personal use that could cause congestion, delay, or disruption of service to any government system or equipment. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network. “Instant Messaging” and web casting on the Internet and other continuous data streams would also degrade the performance of the entire network.

Create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings regardless of the subject matter.

Use of GFE for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

Create, download, view, store, copy, or transmit sexually explicit or sexually oriented materials.

Create, download, view, store, copy, or transmit materials related to illegal gambling, illegal weapons, terrorist activities, and non-FNCS – owned music, videos and any other illegal activities.

Commercial use or in support of “for-profit” and “non-profit” activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, and sale of goods or services).

Engage in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

Posting agency information (all Intellectual Property) to external newsgroups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one’s official capacity as a Federal Government employee, unless appropriate Agency approval has been obtained.

Any use that could generate any additional expense to the U.S. government.

The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data.

140 E-mail Use

USDA DR 3300-1-F states that electronic mail (e-mail) shall be used for the conduct of official business or limited personal use. Below is guidance on acceptable and unacceptable e-mail use at FNCS.

141 Acceptable E-mail Use

Appropriate e-mail use includes, but is not limited to:

- Limited personal use of the FNCS e-mail system as long it does not interfere with official business nor reflect adversely on FNCS Information Systems.
- Any message containing information exchanged by employees for the purpose of accomplishing government business.
- Access to the FNCS e-mail system by users when they are not at their duty station site, or at another installed site, are permitted only through FNCS approved secured methods, such as VPN or Citrix.
- Securing SBU information prior to transmission. Please see Guidance for the Protection of SBU for further guidance on E-mailing SBU information.
- If you receive Spam email, immediately forward this email to the spam mailbox at: spamabuse@fns.usda.gov .

142 Unacceptable E-mail Use

Inappropriate e-mail use includes, but is not limited to:

- Sharing a User ID and password to obtain access to another user's e-mail for any purpose.
- Opening attached file extensions on FNCS e-mail servers to include, but not limited to: .ade, .adp, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hta, .ins, .isp, .lnk, .mda, .mde, .mdz, mp3, .msc, .msi, .msp, .mst, ocx, .pcd, .pif, .reg, .sct, .shs and vbs. In the event you receive an email attachment that is not listed here and you are unsure if it is safe to open, please send an e-mail to spamabuse@fns.usda.gov.
- Sending an email that is inappropriate, or not authorized for distribution on the FNCS network. An inappropriate email can include but not limited to profanity, sexual content or abusive language
- Users may not send e-mail for work purposes through personal e-mail account without prior approval from a supervisor, unless there is an extenuating circumstance, according to the FNCS COOP plan.

150 Internet Use

USDA DR 3300-1-I states that mission areas and staff offices may utilize the Internet to support departmental and mission area responsibilities.

Below are guidelines for the acceptable and unacceptable Internet use at FNCS.

151 Acceptable Internet Use

Appropriate Internet use includes, but is not limited to:

- Limited personal use of the Internet as long it does not interfere with official business nor reflect adversely on FNCS Information Systems.

  Communication and exchange of data between state and local governments, private sector organizations, and educational and research institutions, both in the United States and abroad.
- View inter-Agency non-sensitive data in support of departmental mission, FNCS missions, or other official purposes.

- Download and store information related to official FNCS business on Government Financed Equipment (GFE) only.

152 Unacceptable Internet Use

Inappropriate Internet use includes, but is not limited to:

- Accessing pornographic, gambling, on-line auction and other inappropriate sites.

- Downloading, streaming, copying, sharing, or sending software, music videos, movies, radio or pictures (whether purchased or not purchased) that are not job related as use of these constitute copyright violations and are a non-business use of limited network bandwidth.

- Using peer-to-peer software and file sharing products not expressly identified for authorized use may not be used on or through FNCS servers and workstations, i.e. non-FNCS Instant Messaging (IM) Software.

- Subscribing to ‘list servers’, ‘user groups’, or ‘bulletin boards’ that do not align to authorized business needs.

160 Telephone Equipment and Services

USDA DR 3300-1-F states that use of Government telephone systems (including cellular telephones and calls over commercial systems which will be paid for by the Government) are in place for the conduct of official business or limited personal use.

Below are guidelines on acceptable and unacceptable telephone use at FNCS.

161 Acceptable Telephone Use

Use of government telephone and mobile phone equipment and services for limited personal use may be authorized if used according to the following acceptable use:

- Use does not adversely affect the performance of official duties by the employee or the employee's organization.
- Use could not have been reasonably accomplished at another time using another means.
- It is provided for in a collective bargaining agreement.
- FNCS Users are authorized to use Government telephone equipment and services to:
    - Call to notify family, doctor, etc., when an employee is injured on the job.
    - Contact family while on official business travel.
    - Make calls to arrange for emergency repairs for their residence or automobile while on official business travel.

162 Unacceptable Telephone Use

Inappropriate telephone use includes, but is not limited to:

- Accepting collect calls from non-government numbers.
- Participating in a monitored or recorded telephone conversation without making the other party aware of the monitoring and/or recording.
- Telephone conversations over a speaker-phone or other audio equipment without listing the names or numbers of persons included on the call.
- International Calls by users are prohibited without prior supervisor approval.

164 Violating FNCS Information Resource Acceptable Use Standards

Violations of the Information Systems Security Guidelines and Procedures as stated in the 702 Handbook may lead to immediate removal from the FNCS Network and/or may be the basis for disciplinary action. Supervisors and/or management officials considering disciplinary action must consult with the Labor & Employee Relations Branch in the Human Resources Division prior to taking any action.

170 International Travel

International travel consists of all travel outside the United States and its Territories.

International travel poses additional risk to GFE technology being utilized while on travel. Generally, access to FNCS network resources and systems from foreign countries is prohibited unless approved by the FNCS senior management in advance.

Users should understand that they are subject to the laws of that country, there is no expectation of privacy in most countries, and wireless devices are particularly vulnerable to interception and malware infection.

Users are expected to remain in compliance with all domestic policies when traveling internationally, especially the policies highlighted below:

- No GFE devices and removable media used domestically shall be used on foreign travel to perform government related work. Only FNCS approved and furnished devices are allowed

To the extent possible approved GFE must provide protection against malware and have up-to-date antivirus, spyware, security patches, and firewall software installed.

Unneeded and unnecessary features shall be disabled in accordance with the agency secure configuration baseline.

All sensitive information stored, transmitted or viewed on GFE and removable media shall be protected in accordance with DR 3440-002, “Control and Protection of Sensitive Security Information,” DM 3550-002, Chapter 10, Part 2, “Sensitive But Unclassified (SBU) Information Protection.

- Approved foreign travel devices including removable media should be configured to encrypt stored data using USDA Regulation DR 3170-001 Appendix B Section 16.0 Policy for the requirements governing data encryption.
- GFE used for international travel shall be prepared as follows:
    - GFE devices and removable media will only be used in the performance of officially sanctioned travel; if the devices are not essential to the mission, the equipment shall not be taken.
    - FNCS shall document approval and acceptance of risk for any GFE, which includes, but not limited to, laptops, Citrix token, mobile devices and removable media, allowed to be used during travel.
    - Approved GFE for use while on travel shall be decommissioned or wiped immediately upon return.
    - The servicing Information Technology (IT) unit shall make a copy of all GFE profiles, including but not limited to, OS, configuration, signatures for system and applications

used on the device. This "snapshot" shall be used to evaluate any possible changes made to the device upon return to the office.

- Agencies and Offices shall consult with Office of Homeland Security Emergency Coordination (OHSEC) for current precautions to be observed for destination countries prior to departure.

- Upon return to FNCS after international travel, the GFE:
  - All equipment must be turned off or not used domestically until it can be examined by the appropriate IT staff to ensure the GFE has not been modified or infected by malicious code.
  - Shall not connect to any FNCS servers or networks for any reason prior to this examination.
  - Shall have device passwords changed upon return to the United States (US).
- Users shall exercise a higher level of due diligence in the protection of GFE while on international travel than would be expected in the domestic environment.
  - GFE and removable media shall not be transported in checked baggage.
  - Whenever possible, GFE shall be powered off and the batteries removed and stored separately from the device when not in use to minimize the opportunity for misuse.
  - Foreign thumb drives, compact disks (CDs), or other media shall not be used in FNCS GFE. If such use cannot be avoided, the GFE shall be assumed to be compromised and shall be cleaned and/or reformatted as soon as feasibly possible.
  - FNCS GFE and removable media shall not be used with or in foreign equipment due to the possibility of compromise.
  - Travelers must ensure physical security of the device while in transit and while on international travel or foreign duty.
  - Public internet kiosks, cafes, and hotel Wi-Fi sites are particularly susceptible to monitoring, data interception, and control by foreign entities. Transmission, storage or printing of sensitive government and personal information is prohibited unless by an area pre-approved for printing. Potential solutions for international printing: (1) USDA in-country office location, (2) U.S. Embassy location, (3) U.S. Consulate location, (3) other U.S.G. in-country office or approved printing location, and (5) portable printer.

- If a GFE is lost or stolen while on international travel, the loss must be reported to FNCS incident response team and the local US embassy or consulate immediately upon detection/discovery.

Guidance on Accessing the FNCS Network

200 Overview

This guidance applies to all devices/technologies (to include but not limited to computers, laptops, printers, personal digital assistants (PDAs), routers, firewalls, servers, switches, access points, Universal Serial Bus (USB) network devices, etc. owned by FNCS or not) that are connected to the FNCS Network. The procedures also apply to internal and remote access connections to the FNCS Network. Personally-owned equipment (POE) is only permitted to access the FNCS and USDA networks via Citrix.

The purpose of this 702 Handbook is document security policies and procedures, in accordance with Federal government mandated requirements for connecting to the FNCS network from any device. These standards are designed to minimize the risk of exposure to damage which may result from authorized or unauthorized use of FNCS resources. Damages include the loss of FNCS SBU information, Personally Identifiable Information (PII), intellectual property, damage to public image and critical FNCS internal systems, etc. The following guidelines shall be observed by all users connecting to the FNCS Network.

210 References

This guidance is written in accordance with:

- NIST Special Publication 800-53 Rev.3
- DM 3535-001 USDA C2 Level of Trust Policy
- DM 3530-000, 001,004 USDA Security Protection
- DM 3525-003 USDA Tele-work and Remote Access

220 FNCS Network Access for Government-Furnished Equipment (GFE)

FNCS Internal Access

- All requests for user level network access shall be made only after the successful completion of the FNS-674 form. Please see Section 234 for details on requesting access to the FNCS Network. Access granted is applicable to only those applications that are necessary for the FNCS user's job. New hires, temporary personnel, contract staff and official visitors to FNCS must complete the USDA Information Security Awareness (ISA) training prior to requesting access to the FNCS Network. New Employees will be given these materials by HR; other employees please e-mail SecurityOfficers.Mailbox@fns.usda.gov to receive instructions for taking this CD or paper-based training. For new hires, communication should be initiated with the regional HR Points of Contact to ensure compliance. For all other hires requiring access, employees and supervisors should contact the Information Security Office (ISO).
- Any equipment connecting to the FNCS Network within FNCS facilities shall conform to FNCS OIT standards. Such devices shall adhere to FNCS software standards and security controls (e.g., operating systems, antivirus software, service packs, hot-fixes, and FNCS approved applications). System configurations shall not be changed, added or modified.
- Any non-GFE brought into FNCS by employees, contractors or official visitors shall *not* be connected directly to the FNCS Network.

- An official warning banner shall be displayed before a user successfully gains access to the FNCS Network. By clicking “ok”, the user has agreed to the terms as outlined in the official banner. Refusal to agree will mean that the user will not be granted access.

Remote Access (VPN)

FNCS VPN access to Information Technology (IT) systems from remote location is provided to FNCS users in a secure and effective manner.

FNCS VPN access is built into all employee furnished GFE laptops and is only permitted through GFE laptops.

- FNCS employees, contractors or official visitors requiring remote access to FNCS Network resources shall conform to all security standards.

- Devices connecting to the FNCS Network shall adhere to FNCS software standards and security controls (e.g., operating systems, antivirus software, service packs, hot-fixes, and FNCS approved applications). System configurations shall not be changed, added or modified. FNCS users are required connect via VPN to the FNCS network to ensure all software patches anti-virus software, etc. are up-to-date.

- An official warning banner shall be displayed before a user successfully gains access to the FNCS Network. By clicking “OK”, the user has agreed to the terms as outlined in the official banner. Refusal to agree will mean that the user will not be granted access.

- Connections to the FNCS network through the VPN will automatically disconnect a user from the network when inactivity is detected for 30 minutes by the VPN server; however, if the user is running Microsoft Outlook, the VPN will continue to stay connected. As a result, users of FNCS VPN are reminded to always lock the desktop of all unattended devices logged into VPN and to shut down Outlook when the application is not needed.

221 FNCS Network Access for Personally Owned Equipment (POE)

Remote Access (Citrix)

FNCS Citrix access is available through most Internet web browsers and may be accessed through GFE, or POE.

- FNCS employees, contractors or official visitors requiring remote access to FNCS Network resources shall conform to all security standards.

- Devices connecting to the FNCS Network via Citrix must have up-to-date antivirus software, OS service packs, and hot-fixes applied. An official warning message shall be displayed before a user enters in their login info to the FNCS Network. By clicking “OK”, the user has agreed to the terms as outlined in the official banner. Refusal to agree will mean that the user will not be granted access.

- POE access to the FNCS network is permitted only via FNCS Citrix.

222 FNCS Network Security Controls

- Firewalls, VPN, router-based Access Control Lists (ACL) and audit logs shall be used to control, restrict, and monitor all network access to any FNCS Network.

- The Firewall, VPN and router-based ACLs should be monitored at least on a quarterly basis by a system administrator. Any discrepancies should be noted and corrected during the review.

- All network traffic between FNCS locations shall be transported on dedicated FNCS/USDA owned circuits and VPN connections meeting data encryption levels set by FNCS encryption standards.

- At any time, FNCS/USDA may monitor and/or audit user activity and/or network traffic.

- Network routers, switches, wireless access points and hubs are points of vulnerability and need to be managed centrally to ensure manageability, security and reliability. Unauthorized FNCS Users are not permitted to extend or re-transmit network services.

- Connections to the FNCS Network shall automatically lock a user from the network when 15 minutes of inactivity is detected by enabling a password protected screen saver.

223 FNCS Network Restrictions

- FNCS offices shall not have Internet connectivity other than the connectivity provided by FNCS/USDA. Users inside the FNCS firewall may not be connected to the FNCS Network at the same time they are connected to any other network.

- FNCS devices or any devices approved by FNCS shall not be used as a vehicle to gain unauthorized access to other devices or networks for any illegal, unauthorized or inappropriate activity.

- FNCS employees and contractors are prohibited from remotely accessing the FNCS network, systems, and any related component of the IT infrastructure from foreign countries unless prior approval is provided by the CIO. Any unauthorized use from a foreign country increases the risk of foreign access to information system access and will result in immediate termination of access to the FNCS network. Additional consequences may be taken into action depending on the severity of the incident. Please reference section 170 for International Travel requirements.

- FNCS employees and contractors are prohibited from installing and using unapproved software and mobile code-based products (e.g., Flash, Java, and ActiveX). Unauthorized software or mobile code installation increases the risk in introducing vulnerabilities onto the FNCS network. Users may request software installation from an approved software list established by OIT and distributed via DSB. If a user needs software or mobile code that is not on the approved software list, the user may submit a service ticket to DSB for OIT review.

- FNCS Users shall only use network Internet Protocol (IP) addresses issued by FNCS. Selecting or manually entering an IP address to configure a computer network device is prohibited.

- The use of private IP addressing behind FNCS firewalls and proxy servers, as well as the use of Network Address Translation (NAT) is prohibited unless authorized.

- An unauthorized deliberate attempt to obtain proprietary (non-public information) FNCS Network information is prohibited. This applies to all FNCS Network locations, and the wide area network (WAN).

- Unauthorized FNCS users are prohibited from downloading, installing or running security programs or utilities that reveal weaknesses in the security of a system. FNCS users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner (remotely or internally) to the FNCS Network.

224 How to Request Access to the FNCS Network

After completing the required Information Security Awareness (ISA) training, complete the FNS User Access Request form, FNS-674. This form can be accessed through the Intranet (E-forms) or by contacting the Service Desk (IT Customer Support).

- *If you currently have access to the FNCS Network and need to request access to the STARS, eDRS, SNAP QCS or FPRS Systems, request a level 2 e-Authentication User ID. To learn more about e-Authentication, click here.*

- Attach the ISA training certificate to form FNS-674 and submit to your supervisor for signature. Submit both documents to the Service Desk. Regional Security representatives will be notified through the Information Security Office.

  Upon approval:

  - Users will be notified when access has been granted.

  - Users must report to their corresponding OIT Security Office to obtain an FNCS network user ID and temporary password.

  - Users must contact the Service Desk and request to have user profiles and Outlook set-up.

  - Users are provided with and required to read the Rules of Behavior. Pending the type of access provided, the FNS-674 form is required to be signed.

  - Users may refer to Appendix B of this document for instructions on how to fill out FNS 674 access forms.

225 How to log on and off the FNCS Network (Internal and Remote)

- After receiving an FNCS network user ID and password, the user is required to change the temporary password immediately. Please see the Access Control Procedure on creating acceptable passwords.

- Prior to logging onto the FNCS network, the user is prompted to read and acknowledge the Official warning banner. By selecting “ok”, the user has agreed to the terms as outlined in the official banner. Refusal to agree will mean that the user will not be granted access.

- Users must connect Government-Furnished Equipment (GFE) to the FNCS Network every 30 days for a minimum of 120 minutes to ensure the device receives updates to virus definitions, operating systems and hot fixes. Computers which are identified as not updated on a 30 day window will not be allowed to join the network.

- To log off the FNCS network, the user must be fully logged onto the FNCS network. Select the Ctrl-Alt-Del keys simultaneously, when the task manager dialog box is open, choose "log off". Also, a user can click the "Start" menu of the Windows Task bar and select the "Log off" button.

226 How to lock a workstation

While a user is successfully logged onto the FNCS network, their network sessions must be locked if they leave the work area. Select the Ctrl-Alt-Del keys simultaneously, when the task manager dialog box is open, choose "lock computer" or on the task bar, select the "lock computer icon". All FNCS users are encouraged to shut down their computers at the end of each day. For workstations using a PIV card, the user must pull out their PIV card to lock station. Each workstation needs to be locked when a user leaves their workstation.

227 Separation from FNCS

All users are required to send an E-mail to the Security Officers Email Address, SecurityOfficers.Mailbox@fns.usda.gov, when access to a particular computing resource is no longer required for reasons that may include project completion, work assignment transfers, retirement, termination, or resignation.

All FNCS supervisors will have their employee's complete form FNS 677, Final Salary Payment Report. FNCS employees can request to have their Outlook contacts saved to a CD by the IT Staff.

All FNCS separating contractors' CORs will complete form FNS 744, Government Contractor's Employee Separation Checklist (GCESC). The COR will ensure that the checklist is completed with all applicable signatures on the last day of employment.

228 Process for Accessing another User's Data

Users who require access to another user's FNCS data may submit a request for access with a valid business justification.

Request should be submitted with business justification to the Director of Human Resources for federal employees or to the Contracts Director for contractors.

If you are not the employee/contractor's COR, the COR should also be CC'ed or be the one to initiate the communication.

The CISO and CIO should also be CC'ed on the communication; the CISO will make sure the request is submitted to the Service Desk once all approvals are in place.

229 Collaborative Computing Devices

FNCS must ensure that information system prohibits remote activation of computing devices with expectations identified in the department policy under DM 3530-003 and DM3530-005.

230 Public Key Infrastructure Certificate

FNCS must ensure that public key certificate are issued under identity access and management policy DM 3530-003 and DM3530-005 and approved by the department.

Guidance on the Protection and Use of Wireless technologies

300 Overview

Wireless is a technology that permits the active transfer of information between separated points without physical connection. Currently, FNCS permits the use of wireless technologies to connect to the FNCS Network. Users who connect to FNCS wirelessly must comply with the organizations rules and regulations regarding wireless technologies.

310 References

- This guidance is written in accordance with: DM 3300-005 Policies for Planning and Managing Wireless Technologies in USDA
- DN 3300-01 Wireless Communications

320 Wireless Technology Guidelines

Wireless technology guidelines are intended to help everyone use the FNCS's Wireless network responsibly, safely, and efficiently thereby maximizing the availability of these facilities to all employees.

321 Current State of Wireless Technologies at FNCS

- Currently, FNCS does not support a wireless networking infrastructure. GFE with Wi-Fi capabilities may be used to access Citrix and VPN.

- FNCS has approved the use of the following wireless devices/technologies:

    - Smart phone/Personal Digital Assistant (PDA) – Only approved users

    - Government Issued Air Card or MiFi – Only approved users

All wireless services and devices are to be procured through OIT via the Designated Agency Representative (DAR) and the Telecommunications Mission Area Control Officer (TMACO) only.

322 Home/Commercial Use

Anyone using a home/commercial wireless network to connect to the FNCS Network will comply with all USDA Wireless policies for securing information. When using a home/commercial wireless network to connect to the FNCS Network, users must access the FNCS network via VPN or Citrix. If a user is connected via a wireless network or FNCS approved wireless device, the user is not to be simultaneously connected to the local FNCS network.

Guidance on Incident Response and Reporting

400 Overview

FNCS must be able to respond to computer security incidents in a manner that protects its information and helps to protect the information of other Agencies that may be impacted by the incident.

A security incident is defined to be any adverse event that threatens the security of information resources. Adverse events include compromises of confidentiality, integrity, and availability of FNCS IT and telecommunications resources. This guidance will assist FNCS users (employees, contractors or official visitors) to properly identify, declare and report security incidents.

Refer to the Incident Response Procedures, V1.0 for the detailed incident response procedure. The document represents the formal documented FNS information security policies and addresses purpose, scope, roles responsibilities, and compliance as they pertain to information security.

410 References

This guidance is written in accordance with:

- NIST Special Publication 800-53 Rev.3
- NIST Special Publication 800-61 Rev. 2
- NIST Special Publication 800-86
- DM 3505-000 USDA Computer Incident Response Procedures Manual

420 Loss of Personally Identifiable Information (PII)

Personally Identifiable Information (PII) refers to information that can be used to distinguish or trace an individual's identity. PII can include information or combinations of information such as social security numbers (in complete or truncated form), place of birth, date of birth, mother's maiden name, biometric record, fingerprint, iris scan, DNA, medical history, medical conditions, financial information, credit card numbers, bank account numbers, etc. USDA is committed to protecting PII for both employees, contractors and customers.

The following are procedures on how to notify the appropriate authority of any suspected incident in a timely manner:

- During business hours, if there is an actual loss or potential loss of PII, please contact the security officers' mailbox at SecurityOfficers.Mailbox@fns.usda.gov or call the OIT Service Desk: 888-OIT-4FNS.
- After normal business hours, please contact the USDA toll-free PII Incident Hotline at 1-877-PII-2YOU. The hotline is available 24 hours a day, 7 days a week.

421 All Other Incidents

All other incidents should follow the Incident Response procedures as communicated from the Information Security Office and follow the 702 Handbook for Incident Response Standard Operation Procedure.

Guidance on Audit & Accountability of the FNCS Network

500 Overview

An audit of FNCS Information Systems consists of a systematic examination to determine whether or not activities and their associated results comply with Information Systems Security standards and guidelines.

The purpose of this guidance is to provide details for conducting and implementing the security audits on FNCS Information Systems. Auditing is the process of identifying problems, and deficiencies in an information system for the purpose of correcting such issues. Auditing is necessary to protect information resources from harm or misuse.

Below are common security threats including but not limited to:

- Access to confidential data
- Unauthorized access to computers
- Password disclosure
- Detection of Viruses
- Denial of Service (DoS)
- Open ports, which may be accessible to the public
- Use of other IP addresses, not assigned by FNCS

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources.
- Assess, analyze, or investigate security incidents.

For systems requiring audit logging and monitoring (typically determined by the business), FNS requires that at a minimum, failed login events are logged and monitored.

510 References

This policy is written in accordance with:

- NIST Special Publication 800-53 Rev.3
- DM 3535-001 USDA C2 Level of Trust Policy

520 Audit and Accountability Guidance

It is the responsibility of members from the Information Security Office, System Administrators, and System Security Officers to:

- Create and maintain an auditable events list for each Information System within FNCS.
    - Manage the selection of auditable events to be included in audit logs.
    - Review audit logs at least once a week or when unusual or suspicious activity occurs.

- Protect audit records and audit mechanisms from unauthorized access, modification or deletion.

- The following list is representative of events for auditing and logging on existing hosts, network devices, and web server that would provide acceptable auditable events:

    - Date and time of the event, e.g. Time stamps are synchronized, every hour, with a defined system clock;
    - Event origin (software/hardware)
    - Where the event occurred;
    - Type of event;
    - User's identity, if applicable;
    - Outcome (success or failure) of the event.

- Allocate audit storage space to handle the FNCS audit mechanism.

- Provide information system alerts for designated personnel when audit record storage has reached 75% of its capacity.

- Authorize and properly trained to post public content onto the Information system to ensure that information does not contain non-public content. These individuals are responsible for ensuring that all information to be posted on the Information system has been thoroughly reviewed and approved prior to posting. If any non-public information is incorrectly posted, it must be removed from the Information System immediately upon discovery. This control only applies to an information system that has publicly accessible content.

- Provide capabilities to perform monitoring, analysis and reporting of incidents.

- Respond to alerts for potential or confirmed security incidents.

- Review audit reports to assist in security incident investigations.

- Perform audit reviews on a daily basis.

- Archive audit logs and maintain for a minimum of three (3) years.

Guidance on Access Control for FNCS Information Systems

600 Overview

In computer security, access controls include authorization, authentication and audit. Access control protects information by managing access to all entry and exit points, both logical and physical. Perimeter and logical security measures protect against unauthorized access to sensitive information stored on the FNCS network or applications.

The purpose of this guidance is to maintain information security by preventing unauthorized access to FNCS Information systems and data. This guidance is reviewed and updated at least annually. The Access Control Guidance is written to:

- Communicate the need for access controls within FNCS.
- Establish specific requirements for protecting against unauthorized access.
- Define FNCS user privileges, password restrictions and login limitations.
- Provide guidelines for Identification and Authentication.

610 References

This policy is written in accordance with:

- NIST Special Publication 800-53 Rev.3
- DM 3535-001 USDA C2 Level of Trust Policy

620 FNCS Access Control Guidance

- FNCS mainly uses Microsoft Active Directory to manage all information systems that establish, activate, modify, review, disable, and remove user accounts. eAuthentication accounts are also used to manage user accounts for externally, and some internally, accessible web applications.

- Accounts that are created, modified, disabled and terminated are to be reviewed as determined by the system owner. All FNCS information systems must manage information system accounts by reviewing accounts for compliance with account management requirements at least annually.

- Automated mechanisms should be employed to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals must be notified.

- Accounts inactive for more than a month are automatically disabled.

- System Owners may restrict access to system objects such as: files, directories, devices, databases and programs based on the identity of the users and/or groups to which they belong, these controls are Discretionary Access Controls.

- FNCS shall establish separation of duties that allow appropriate information system authorization based on individual or role.

- An FNCS user may request access to information based on a need-to-know basis. This will be determined by the executive or manager deemed to be the system owner of the asset.

- FNCS shall implement least privilege (most restrictive settings) that grants users only those accesses required to perform their duties. User listings which show least privilege settings for administrators will be updated on an annual basis or as needed after a major update.

- FNCS shall establish a limit of three (3) concurrent sessions on high impact systems as defined by FIPS 199 security baseline categorizations. Currently, no high impact systems exist at FNS.

- FNCS shall establish object reuse capabilities to ensure storage objects/devices that store SBU information are rendered inaccessible before the object/device is used for other purposes. All FNCS laptops and workstations will be re-imaged when the device is no longer used by the FNCS employee or contractor.

621 FNCS Recertification of Access Controls

- All system user access lists must be reviewed and recertified at a minimum of once a year by the System Owner, and/or as needed by the System Owner based on risk. This review includes all user privilege levels to any or all portions of a system.

- Recertification forms can be found on the Intranet (E-Library). Once a recertification is completed, the signed form must be submitted to the Information Security Office (ISO) and signed by the ISSM.

640 FNCS Password Guidance

641 General User - Password Guidelines

General users do not have administrative rights on a system or application.

- Passwords to any system used for FNCS business are confidential and must not be shared.

- General user accounts shall have passwords with a maximum sixty (60) day age limit and a minimum one (1) day age limit.

- User passwords must be twelve (12) or more characters in length containing upper and lower case, alphanumeric, and special character combinations (at least one of each).

- Dictionary words used for passwords are prohibited.

- User accounts are locked after five (5) failed attempts. If this occurs, call the Service Desk or submit a work order via the IT Customer Support Web portal to report that your account is locked. Follow instructions given by the Service Desk.

- As a routine courtesy, the system will notify the user in advance when passwords will expire.

- When prompted, change your password within the allocated time given. A history of 24 previously used passwords are maintained, please do not repeat passwords.
- Do not automate passwords through use of function keys, scripts or other methods that store passwords on systems.
- Do not store passwords within near proximity of the workstation, such as underneath the keyboard, behind the monitor, under the desk, etc.
- Please refer to Appendix C for Password Hints.

642 Privileged User - Password Guidelines

Privileged users are users who have administrative type access for all or part of an operating system or application, e.g. System or LAN Administrator.

- Passwords to any system used for FNCS business are confidential and must not be shared with others.
- Privileged account holders will have at least two (2) accounts, one for privileged use and one for common network use such as e-mail and Internet access.
- Privileged accounts will not be e-mail or Internet enabled.
- Privileged user accounts shall have passwords with a maximum sixty (60) day age limit and a minimum one (1) day age limit.
- User passwords must be twelve (12) or more characters in length, containing alphanumeric and special characters.
- Dictionary words used for passwords are prohibited.
- User accounts are locked after three (3) failed attempts. If this occurs, call the Service Desk or submit a work order via the IT Help Desk Tracking System, Alloy, to report that your account is locked. Follow instructions given by the Service Desk.
- As a courtesy, the system will notify the Network user prior to the expiration of passwords.
- When prompted, change password within the allocated time given.
- Do not repeat passwords since the system maintains a history of the last 24 passwords.
- Passwords cannot be shared between privileged users.
- Do not automate passwords through use of function keys, scripts or other methods that store passwords on systems.
- Once privileged users leave or their accounts are terminated, their access accounts are disabled.

- Please refer to Appendix C for Password Hints.

643 Password guidelines for Government-Furnished Wireless PDAs

- User passwords must be eight (8) or more characters in length, containing alpha, numeric and special characters.
- The number of incorrect password attempts are currently set to seven (7), if this limit is exceeded, the device is wiped. If this occurs, contact the Service Desk.
- Government Furnished Wireless PDAs must have the USDA mandated security configuration settings and software installed. These settings are FIPS 140-2 compliant and users are not allowed to modify or delete these settings.
- Lock the device after five (5) minutes of inactivity.

644 Acceptance of PIV Credentials

Multifactor authentication for remote access to FNCS Information Systems, is used for privileged and non-privileged accounts, such that one of the factors is provided by a device separate from the system gaining access and the device meets USDA policy for multifactor security requirements.

645 Device Identification and Authentication

FNCS must ensure that information systems uniquely identify and authenticate components in inventory that support the ability to connect to outside systems before establishing a remote and/or network connection.

Guidance on IT Restricted Space and Physical Access Control

700 Overview

The United States Department of Agriculture, Food, Nutrition and Consumer Services houses and/or processes information relating to the privacy of US citizens, payroll and financial transactions, proprietary information and life/mission critical data. It is essential that this information be protected from the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction.

FNCS must protect information resources through layered physical security, high logical data security and effective security procedures and administration. Successful IT security protection dictates the physical control of restricted space that contains major FNCS computer and telecommunications resources.

This procedure will define the physical security standards for all IT restricted space(s) located at FNCS facilities. This procedure includes the physical access control requirements for Computer Facilities, Telecommunications/Local Area Network (LAN) Rooms, IT equipment storage rooms, Web Farms, Sensitive Compartmented Information Facility (SCIF) and isolation zones.

710 References

This policy is written in accordance with:

- NIST Special Publication 800-53 Rev.3
- DM 3510-001 USDA Physical Security Standards for IT Restricted Space
- GSA Facilities Standards P100

720 Physical Environment

FNS leases restricted space from General Services Administration (GSA). FNS policy and procedures for Physical and Environmental Protection adheres to policies and standards provided through the GSA Facilities Standards, P100, and the USDA Physical Security Standards for Information Technology Restricted Space, DM 3510-001. Property Management Branch receives delegated authority for protection of the FNS secured space through GSA.

721 Roles and Responsibilities

The key roles and responsibilities for carrying out the provisions of this Handbook are outlined below.

722 The FNCS CIO will:

- Inform the Property Management Branch of their duties on maintaining and managing user access to IT restricted space(s).
- Approve and implement this procedure.
- Review and approve all modifications to this procedure.

720 The FNCS Supervisors and point of contacts (POC) will:

- Provide contractors and non-FNCS employees with form FNS 767 to complete when access to IT restricted space is requested.
- Ensure form FNS 767 is complete, approved and forwarded to the appropriate System Owner for approval.

721 The System Owners will:

- Authorize user requests for data center access by approving form FNS 767.
- Forward form FNS 767 to the Information Security Office (ISO) at SecurityOfficers.Mailbox@fns.usda.gov
- FNCS System Owners are:
  - OIT Director of Technology or their representative

722 The Information Systems Security Program Manager (ISSPM) will:

- Approve form FNS 767 after the System Owner and Supervisor approval.
- Forward form FNS 767 to the Property Management Branch for final processing.
- Conduct reviews of all FNCS IT restricted space and ensure they are compliant to physical security requirements as outlined in DM 3510-001 USDA Physical Security Standards for Information Technology Restricted Space.

723 The Physical Security Branch will:

- Maintain all user access requests to IT restricted space by generating monthly reports of user access sending them to Operational Security. Operational Security performs audits for unauthorized access.
- Remove access to users who have been inactive for 90 days.
- Remove all access for users who have been terminated: FNCS employees, contractors and others who are no longer at FNCS.
- Ensure that all user access requests to IT restricted spaces meet the appropriate security standards required to receive access.
- Block access to IT restricted space for those individuals who lack the required security authorization.
- Perform user recertification, quarterly. See section 725 for details on recertification.

724 FNCS Users will:

- Request access to IT restricted space by completing Form FNS 767.
- Notify the ISO when access to IT Restricted Space is no longer needed.

- Escort guests who request access to IT Restricted Space and ensure they have signed-in via the IT restricted space sign-in sheet. Guests include but are not limited to:
  - Fire detection personnel
  - Alarm system personnel
  - Air Conditioning maintenance personnel
  - UPS maintenance personnel
  - Hardware maintenance personnel
  - Software maintenance personnel
  - Other Vendors

- In the event that the automated system is not functional (power outages, etc.), the restricted space needs to maintain a log of user access via a manual process such as a sign-in sheet.

725 IT Restricted Space and User Access Recertification Process (Property Management Branch)

Step 1: The Facility Management Branch will produce a site-specific list of all users who have access to FNCS IT restricted space.

Step 2: The Technology Division will review and determine which users need access to IT restricted space at least on an annual basis or as needed

Step 3: The annual recertification of user access will be performed only for those users deemed necessary to continue accessing IT restricted space.

Step 4: The Facility Management Branch and the appropriate point of contact from the Technology Division will take appropriate actions to modify or terminate user access as indicated by the results of the recertification process.

Step 5: FNCS Management will review and verify results of the recertification and ensure the Facility Management Branch has the appropriate corrective action plans in place.

Step 6: The Information Security Office will retain all recertification documents for five (5) years.

Guidance on FNCS Computer Security Awareness and Training

800 Overview

The Federal Information Security Management Act (FISMA) mandates general training of employees to ensure that they are aware of their security responsibilities; specialized training of agency employees with significant security responsibilities; and reporting of agency statistics on security awareness and training efforts.

This procedure will detail plans to develop, conduct and implement computer security awareness and training as required by USDA and FISMA. This procedure will also provide guidance on

reporting and monitoring training and creating an information security training program for specialized information security professionals at FNCS.

This procedure is applicable to all FNCS employees, contractors and official visitors who engage in FNCS business.

The procedure is reviewed and updated at least annually.

810 References

This policy is written in accordance with:

- NIST Special Publication 800-53 Rev.3
- NIST Special Publication 800-16
- NIST Special Publication 800-50
- DM 3545-001 Computer Security Training and Awareness Policy

820 Information System Security Awareness

The FNCS Information Security Office (ISO) will conduct computer security awareness campaigns by distributing interactive electronic-based training.

Other informal security awareness promotion will be conducted on a frequent basis in the form of emails, posters, videos and hard copy reading materials, all designed to encourage information system security awareness at FNCS.

830 Information Security Awareness (ISA) Training

ISA training is currently implemented annually by USDA.

ISA training consists of an interactive, electronic-based training module that provides computer security information and assessments of that information.

Basic security awareness training must be provided and completed annually.
All FNCS employees, contractors and official visitors, regardless of their job duties are required to complete this training with a passing score. If the employee does not pass with a score of at least 70%, the employee may take the training two more times with different versions of the test.

Currently, the ISA training is available on AgLearn. All users must request an eAuthentication ID then register with AgLearn to access the security training modules. For more information on eAuthentication follow this link, http://www.eauth.egov.usda.gov/index.html. For additional information on AgLearn, click here, http://www.aglearn.usda.gov/ .

831 ISA Training Requirements

Information Security Awareness Training requirements are to be included in all new procurement requests, specifications, statement of work (SOW), grants and cooperative agreements. The security requirements will detail the appropriate level of training needed based on the job duties, access and need-to-know.

ISA training requirements are to be included in new employee orientation at FNCS. All FNCS new-hires are required to complete this training prior to receiving access to the FNCS Network. The ISA training certificate must accompany the Form FNS-674, User Access Request Form.

The FNCS ISO will participate in the annual review and redesign of the security awareness program and vendors to ensure the training is accurate.

Information systems security professionals are encouraged to request additional training as needed for their job functions at FNCS.

832 ISA Specialized Training Requirements

In accordance with NIST Special Publication 800-16, *Information Technology Security Training Requirements*, the Department mandates that all IT Professionals with specific information security responsibilities are required to complete IT Security Specialized Training.

As an IT Professional with specific information security responsibilities, once you have been identified, you will need to complete the annual IT Security Specialized Training. Failure to complete this training by the deadline may result in the temporary removal of your individual rights, roles, and responsibilities where those individual attributes impact the security of the system or application.

833 ISA Training Records

Individual training records, including security awareness training certificates and specific information systems security records are retained for a minimum of one year.

Guidance on System Certification and Accreditation (C&A)

900 Overview

OMB Circular A-130, Appendix III and the Federal Information Security Management Act (FISMA) requires that all federal agencies institute an agency-wide information security program to provide information security for information and information systems that support the operations and assets of the agency. This includes those systems provided or managed by another agency, contractor, or other source. All USDA agencies shall institute a comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting a specified set of security requirements for the system. These actions are referred to as system certifications. Certification supports the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets or individuals based on the implementation of an agreed-upon set of security controls. This decision is referred to as system accreditation.

All USDA IT systems require certification and accreditation prior to the system becoming operational. The Designated Accrediting Authority (DAA) makes formal accreditation determinations. This action supports the regulatory requirement that every USDA system must have official approval to operate. Please see the USDA definition of a "System".

910 References

This Guidance is written in accordance with:

- NIST Special Publication 800-53 Rev.3
- NIST Special Publication 800-37
- USDA Certification and Accreditation Guide, Appendix A
- USDA DM 3540-001 Risk Assessment Methodology
- FIPS Publication 199

920 Roles and Responsibilities

This sections details the responsibilities of all teams and individuals who are impacted by or involved in system C&As. System owners will be responsible for developing Phase I C&A documents.

921 The CIO will:

- In coordination with the System Owner, determine when a C&A is needed for a system after a major change has occurred.

- Act as the Certifying Official for FNCS. As appropriate, the CIO may delegate this responsibility to a Security Officer, but must continue to recognize their accountability in that delegation.

922 The System Owner will:

- Represent the user community and IT system throughout the systems' life cycle.
- Ensure the system is delivered and operating in accordance with the security controls documented in the security plan.
- Uphold training requirements by ensuring system users and security support personnel receive security training.
- Work with the IT Project Manager (ITPM) throughout the C&A process.
- Create POA&Ms for deficiencies along with milestone dates and submit to the ISSM/ITPM.

923 The IT Project Manager (ITPM) will:

- In coordination with the ISO, maintain the C&A schedule for all existing systems.
- Notify the Systems Owners of upcoming C&As.
- Oversee the system maintenance, operation and disposal.
- Submit the completed C&A documents to the ISO templates to System Owners for each phase of the C&A.
- Perform a preliminary review of the C&A documents.
- Provide updates to the ISO on the system's C&A progress.
- Report suggested changes to C&A documents from the ISO to the System Owners.
- Work with ISO to ensure security controls based on NIST 800-53, are included in system documentation.

924 The Designated Accrediting Authority (DAA) will:

- Accredit systems for operation.
- Act in the role of Business Owner to a system being certified.
- Assume the responsibility for the residual risks of operation of the systems.
- Approve security requirements documents, memoranda of agreement (MOA), memoranda of understanding (MOU) and any deviations from security policies.
- Commitment memos will be issued by the system owner to the Department on C&A completion dates.

925 The Certification Team will:

- (The ITPM and ISSM determine if this team is needed for the C&A).
- Identify, assess and document the risks associated with the operating system.
- Coordinate C&A activities and consolidate the final C&A package.
- Assess the vulnerabilities in the system.
- Determine if the security controls are correctly implemented and effective.
- Identify the level of residual risk to the system.

926 The Security Test and Evaluation Team (ST&E) will:

- Receive approval by the Certifying Official (CO) prior to commencement of the C&A.
- Consist of individuals independent of the IT infrastructure and business function.
- Members of the ST&E team have not been involved in development of the system.
- Members of the ST&E team have not been involved in other certification activities such as writing the System Security Plans (SSP) and conducting the risk assessments.
- Perform the security control assessment on the system to validate the results of the risk assessment.
- Create POA&Ms for deficiencies found, if any, during the evaluation.
- Validate that the controls listed in the SSP are present and in operation.
- Update the SSP, if needed.
- Update the Risk Assessment, if needed.

927 The ISSM will:

- Monitor the physical, personnel, incident handling, security awareness and training needs of a system on a daily basis.
- Identify the pending system or environment changes that may necessitate re-certification and re-accreditation of the system.
- Serve as the principal technical advisor to the ITPM for all security-related issues.

Guidance on Certification and Accreditation (C&A) of Information Systems at FNCS

930 General Information

1. C&A's are initiated upon the creation of a new system application.

2. All systems going through a C&A must undergo FIPS 199, Privacy Impact Assessment, Privacy Threshold Analysis, Configuration Management Plan, Contingency Plan and must address each control in the System Security Plan.

3. If a system undergoes a major change, it may need to undergo a full C&A by direction of the CIO.

4. C&As are performed for both General Support Systems (GSS) and Major Applications.

5. Refer to the Child System and Application Assessment Policy, V1.0 for determining if a system is a parent or a child. The document represents the formal documented FNS information security policies and addresses purpose, scope, roles responsibilities, and instructions of assessment and the categorization of an application.

6. Systems may use a modified C&A process if their system categorization rating is "low" in all three of the assessment categories; confidentiality, availability and integrity.

7. The C&A process consists of three phases:
   - Phase 1: Pre-certification
   - Phase 2: Certification and Accreditation
   - Phase 3: Post Accreditation

8. Cyber Security Assessment and Management

   - The Cyber Security Assessment and Management Tool (CSAM) is a web-based tool which is used to achieve FISMA compliance for in-scope systems. The CSAM tool performs the following functions within the C&A process:

   - CSAM provides risk-based policy and implementation guidance. The tool references controls mentioned in NIST Special Publications 800-53 and 800-53A in which users can document test cases and results for financial and other high-impact systems.

   - The user documents the applicable, inherited, and hybrid controls for the applicable system. After this process is complete, the concurrency reviewer adds any revisions and comments to the classification of controls. Once the comments are addressed, Phase 1 is complete.

   - When Phase 2 is initiated, documents such as the System Security Plan, Risk Assessment, and the Security Assessment Report (refer to section 933 for more information) are updated within the CSAM tool. Any certification findings are reported. Before initiating Phase 3, the final accreditation decision is uploaded within CSAM as well.

- The CSAM tool allows for the monitoring of current and upcoming in-scope applications which require an update of C&A documentation.

931 Phase 1 Pre-certification (Initiation, Acquisition/Development Phase of the SDLC)

The following steps details what is needed in the pre-certification phase of a C&A:

Step 1: **Define the Scope**

A. The Certification Team gathers all available system information needed to define the scope of the C&A and provide a detailed description of the system. Key C&A participants agree on the scope and schedule the C&A Activities.

B. Determine the security categorization for the system and document this by using Table 1-1 as a guide to determining the risk levels (low, moderate, high) for each level of concern for Confidentiality, Availability and Integrity. *If the security categorization rates this system as a low impact system, only complete phase 1 of the certification.*

C. Select the team that will perform the security control assessment and inform the CO. The CO approves the security control assessment team and ensures they are independent of FNCS OIT.

932 Level of Concern for Confidentiality, Integrity and Availability (CIA)

Level of Risk			
	LOW	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C §3542]	The unauthorized disclosure of information could be expected to have a **limited adverse effect** on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective repairs.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.	The unauthorized disclosure of information could be expected to have a **severe** or **catastrophic** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.
Integrity Guarding against improper information modification, destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C. §3542]	The unauthorized modification or destruction of information could be expected to have a **limited adverse effect** on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of integrity could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized modification or destruction of information could be expected to have a **serious adverse effect** on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of integrity could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.	The unauthorized modification or destruction of information could be expected to have a **severe** or **catastrophic** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of integrity could be expected to cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.

Level of Risk			
	LOW	**MODERATE**	**HIGH**
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C. §3542]	The disruption of access to information could be expected to have a **limited adverse effect** on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of availability could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective repairs.	The disruption of access to information could be expected to have a **serious adverse effect** on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of availability could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.	The disruption of access to information could be expected to have a s**evere or catastrophic** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of availability could be expected to cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.

Table 2 – Level of Concerns for CIA – FIPS 199

Step 2: **Identify Security Controls and Construct a Compliance Matrix (High, Moderate, and Low Systems)**

A. Identify all security controls for the system. Include those already specified in the SSP.

B. Review system privacy implications in preparation for the Privacy Impact Assessment (PIA) and Systems of Records Notice (SORN), if applicable.

C. Ensure all security controls are compliant with USDA Cyber Security Polices, 3500 series, OMB A-130 and NIST SP 800-53(FISMA).

D. Include management, operational, technical, environmental and physical controls.

E. List each security control and reference where the security control was derived and whether the control was implemented.

No.	Security Control	Compliance			Comments
		Yes	No	Other	
Management Controls					
1.	**(Example)** The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls. **NIST SP 800-53, Rev. 2, Appendix F CA-1**	**Y**			

Table 3 – Security Controls and References

Step 3: **Conduct a PIA and, if required, complete a Systems of Records Notice (SORN) (High, Moderate and Low) Systems**

A. Determine the impact that this system may potentially have on an individual's privacy.

B. Complete the PIA and SORN if needed.

Step 4: **Review the SSP for (High, Moderate and Low) Systems**

A. Ensure the existing SSP accurately follows the methodology as documented in NIST 800-18, Guide for Developing Security Plans for IT Systems.

B. Review all documents and ensure they have the most current system configurations.

C. Review the Interconnection Service Agreement (ISA), if applicable.

Step 5: **Review the Initial Risk Assessment (High, Moderate and Low) Systems**

A. The risk assessment will list all apparent threats and vulnerabilities.

B. Ensure the risk assessment is compliant with the USDA Risk Assessment Methodology, DM 3540-001 and NIST SP 800-30.

C. Compare the initial risk assessment to the security requirements during development of the system.

D. Update the risk assessment each time there is a change to the security controls that may cause further risk to the system.

Step 6: **Review the Interconnection Security Agreement (ISA)**

A. The ISA is initially drafted during the Initiation Phase of the SDLC.

B. An ISA must be completed for each system that connects to the new systems.

Step 7: **Negotiations with the C&A Participants**

A. All participants involved in the C&A process should meet to review all of the documentation created thus far. Those involved will be the DAA, CO, Program Manager, System Owner and Certification Teams.

B. The Security Categorization should be verified for accuracy.

C. At this time the SCCM should be reviewed to ensure all Security Controls accurately reflect the security requirements for this system.

933 Phase 1 C&A Documents

The following documents are created during or prior to Phase 1 of the C&A process. Some documents may not apply based on the result of the Security Categorization:

- Scope
- Security Categorization Document — SCD
- System Security Plan — SSP
- Contingency Plan — CP/DRP
- Contingency Exercise Handbook
- Disaster Recovery Test Plan — DRTP
- Rules of Behavior — RoB
- Plans of Actions & Milestones — POA&Ms
- Security Controls Compliance Matrix — SCCM
- Privacy Impact Assessment — PIA
- System of Record Notice — SORN
- Initial Risk Assessment — RA
- Configuration Management Plan — CMP
- Privacy Threshold Analysis — PTA
- eAuthentication Risk Assessment
- Interconnection Security Agreement — ISA
- Concept of Operations — CONOPS

- Appendix S – Hardware Listing
- Appendix T – Software Listing

For more information on the C&A documents, see Appendix D

934 Phase 2 Certification and Accreditation

The following steps detail what is needed to perform a certification and accreditation:

Step 1: **Conduct a Security Control Assessment (Acquisition/Development Phase of the SDLC)**

A. The Security Control Assessment Team evaluates the effectiveness of security controls through hands-on testing. FNCS uses a third-party Contractor to perform Security Control Assessments.

B. The Security Control Assessment consists of three steps:

1. Create Security Assessment Plan
   - Derive test objectives from the Security Controls
   - Create test procedures for each objective

2. Execute the test procedures
   - Perform technical testing
   - Interview Staff on the security controls
   - Review System documentation
   - Observe System Operations
   - Test and execute a Contingency Plan

3. Document the test results
   - Document the test results
   - Recommend countermeasures for identified findings

Step 2: **Update the Risk Assessment (High & Moderate) Systems**

A. The results of the Security Control Assessments are used to review and update the risk assessment and determine any risk that may remain.

B. Updates to the Risk Assessment will be in the form of an addendum to the original Risk Assessment.

C. Refer to the USDA Risk Assessment Methodology http://www.ocio.usda.gov/directives/doc/DM3540-001.pdf and NIST SP 800-30 to ensure all areas of the risk assessment are completed.

D. Updates to the Risk Assessment should include the following steps:

- Review the list of threats to include: hackers, malicious insiders, attacks against the system facility and natural disasters.

- Assess vulnerabilities for each system and evaluate the likelihood that the identified threat may exploit vulnerability.
- Assess the possible impact to the system and agency if the vulnerability was exploited.
- Determine if there is a likelihood that the threat will exploit the vulnerability and the impact that would result.
- Evaluate the risks of all identified vulnerabilities to determine an overall level of risk for the system or application.

Step 3: **Update the System Security Plan (SSP), ISA and PIA**

A. The SSP should be updated to reflect the results of the Security Control Assessment and final risk assessment.

B. During this phase, there should be updates to the PIA and ISA.

C. Update the Document Certification Findings

Step 4: **Document Certification Findings** In this step, the following certification activities are to be completed.

A. The Certification Team documents all findings in the Security Evaluation Report (SER). The SER includes all findings from the Security Control Assessment and Risk Assessment.

B. The Certification Team creates and submits the certification package. The certification package is forwarded to the CO for review. The package includes:
   - SCCM
   - Security Control Assessment
   - ISA
   - PIA
   - SORN
   - Risk Assessment
   - System Security Plan (SSP)
   - Security Evaluation Report

C. The CO evaluates the risks and issues in the SER and reviews the other documents in the certification package.

D. When the CO has completed the review, a certification statement is created and states the extent to which the system meets its security requirements.

E. At this time, the CO provides a recommendation for an accreditation decision.

F. The certification statement and SER are forwarded to the Associate Chief Information Officer for Cyber Security (ACIO-CS) via the ISSPM for a mandatory concurrence.

G. If the ACIO-CS concurs, the CO forwards the certification package to the DAA with the accreditation decision.

Step 5: **Accreditation Decision** In this step, the accreditation decision occurs:

A. Based on the evaluation of the residual risk, the COs recommendation and the ACIO-CS concurrence.

B. The DAA will grant system accreditation or deny it.

C. The accreditation decision is documented in the final accreditation package which consists of the accreditation letter and supporting documentation.

935 Phase 2 C&A Documents

The following documents are created and/or updated during Phase 2 of the C&A process.

- Certification Package:
  - SCCM
  - Security Assessment Report
  - Plan of Action and Milestones
  - ISA
  - PIA, if applicable
  - SORN, if applicable
  - Risk Assessment
  - System Security Plan
  - Security Evaluation Report
- Certification Statement
- Final Accreditation Package:
  - Accreditation Letter
  - Supporting documents
  - Rationale for the accreditation decision
- IT Contingency Plan and Disaster Recovery Plan (DRP)
- Trusted Facilities Manual (TFM)

For a detailed description of each document, see Appendix D.

936 Phase 3 Post-Accreditation

Once an ATO is obtained following successful completion of the C&A process; the new C&A system will enter the continuous A&A process going further. A C&A will only be needed if the system is undergoing major changes warranting a full security assessment. Once the A&A process has been fully implemented, the decision to complete a full C&A will be made by the DAA, with the support of the CIO.

Guidance on Assessment and Accreditation (A&A) of Information Systems at FNCS

Security Assessment and Authorization

950 Overview

The Office of the Chief Information Officer (OCIO), Agriculture Security Operations Center (ASOC), Oversight Compliance Division (OCD) provides oversight for the United States Department of Agriculture's (USDA) Assessment and Authorization (A&A) program, formerly known as the Certification and Accreditation (C&A) program. The program is based on guidance provided in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision (Rev.) 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach; mandates identified in the Federal Information Processing Standards (FIPS) Publication (Pub)199, Standards for Security Categorization of Federal Information and Information Systems; FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems; and USDA enhancements created to accommodate the Department's environment.

The intent of the Continuous A&A process is to evaluate Information Technology (IT) systems against documented specific information security requirements, verify information security control test results, summarize the residual risk, and involve the Department's senior management (the System Owner and the Authorizing Official (AO)) in the security lifecycle of the system. Each system will go through the Continuous A&A process every year, but only 1/3 of their controls will be tested each year.

This guide is designed to lead System Owners and certification and risk assessment teams through the USDA's Continuous A&A process. It provides a basic understanding of the process steps and examples of what information to input (system information and documents) into the Cyber Security Assessment Management System (CSAM).

(USDA Six Step Risk Management Framework (RMF) Process Guide, 2012)

960 References

This Guidance is written in accordance with:

- NIST SP 800-37 Rev 1
- FIPS Publication 199
- FIPS Publication 200

This sections details the responsibilities of all teams and individuals who are impacted by or involved in system C&As. System owners will be responsible for developing Phase I C&A documents.

970 The CIO will:

- In coordination with the System Owner, determine when a Continuous A&A is needed for a system after a major change has occurred.

- Act as the Certifying Official for FNCS. As appropriate, the CIO may delegate this responsibility to a Security Officer, but must continue to recognize their accountability in that delegation

971 The System Owner will:

- Represent the user community and IT system throughout the systems' life cycle.
- Ensure the system is delivered and operating in accordance with the security controls documented in the security plan.
- Uphold training requirements by ensuring system users and security support personnel receive security training.
- Work with the IT Project Manager (ITPM) throughout the Continuous A&A process.
- Create POA&Ms for deficiencies along with milestone dates and submit to the ISSM/ITPM.

972 The IT Project Manager (ITPM) will:

- In coordination with the ISO, maintain the Continuous A&A schedule for all existing systems.
- Notify the Systems Owners of upcoming Continuous A&As.
- Oversee the system maintenance, operation and disposal.
- Submit the completed A&A documents to the ISO templates to System Owners for each phase of the Continuous A&A.
- Perform a preliminary review of the Continuous A&A documents.
- Provide updates to the ISO on the system's Continuous A&A progress.
- Report suggested changes to Continuous A&A documents from the ISO to the System Owners.
- Work with ISO to ensure security controls based on NIST 800-37 rev 1, are included in system documentation.

973 The Designated Accrediting Authority (DAA) will:

- Accredit systems for operation.
- Act in the role of Business Owner to a system being certified.
- Assume the responsibility for the residual risks of operation of the systems.
- Approve security requirements documents, memoranda of agreement (MOA), memoranda of understanding (MOU) and any deviations from security policies.

974 The Authorization Team will:

- Identify, assess, and document the risks associated with the operating system.
- Coordinate Continuous A&A activities and consolidate the final Continuous A&A package.

- Assess the vulnerabilities in the system.
- Determine if the security controls are correctly implemented and effective.
- Identify the level of residual risk to the system.

975 The Security Test and Evaluation Team (ST&E) will:

- Receive approval by the Certifying Official (CO) prior to commencement of the Continuous A&A.
- Consist of individuals independent of the IT infrastructure and business function:
    - Members of the ST&E team have not been involved in development of the system.
    - Members of the ST&E team have not been involved in other certification activities such as writing the System Security Plans (SSP) and conducting the risk assessments.
- Perform the security control assessment on the system to validate the results of the risk assessment.
- Create POA&Ms for deficiencies found, if any, during the evaluation. POA&Ms will be created after discussing potential weaknesses with System Owner and their representative.
- Validate that the controls listed in the SSP are present and in operation.
- Update the SSP, if needed.
- Update the Risk Assessment, if needed.

976 The ISSM will:

- Monitor the physical, personnel, incident handling, security awareness and training needs of a system on a daily basis.
- Identify the pending system or environment changes that may necessitate re-certification and re-accreditation of the system.
- Serve as the principal technical advisor to the ITPM for all security-related issues.

977 Additional Continuous A&A Guidance

FNCS follows the six step approach to achieve an Authority to Operate (ATO) and to effectively manage risk for their systems. FNCS uses the Cyber Security Assessment and Management (CSAM) as its automated FISMA management tool and the system of record to capture system information throughout the A&A process. At USDA, all system information, documentation, and assessment results require recording in CSAM

978 General Information

1. Continuous A&As are performed every year

2. Only 1/3 of the controls and the USDA selected “Key” controls will be tested
3. Continuous A&As will be performed every year
4. Systems may use modified Continuous A&A process if their system categorization rating is “low” in all three of the assessment categories; confidentiality, availability and integrity
5. The Continuous A&A process consist of six (6) steps:
    - 5.1. Step 1- Categorize the Program/System
    - 5.2. Step 2 - Select Security Controls
    - 5.3. Step 3 – Implement Security Controls
        - 5.3.1. Step 3a – Implement Security Controls
        - 5.3.2. Step 3b – Concurrency Review
    - 5.4. Step 4 – Assess Security Controls
        - 5.4.1. Step 4a – Assess Security Controls
        - 5.4.2. Step 4b – Submit the Package for Final Concurrency Review
    - 5.5. Step 5 – Authorize Information System
    - 5.6. Step 6 – Monitor Security Controls

979 Step 1: Categorize the Program/System

Step 1 of the RMF focuses on the collection of general system information, completing the Privacy Threshold Assessment (PTA), Privacy Impact Assessment (PIA) and completion of the FIPS 199 system categorization. This collected information includes the mission, environment, boundary definition, architecture, and information the system transmits or processes. The system owner is responsible for completing the categorization and may require the participation of the information system security officer or others as needed.

Requirements for All Systems/Programs	Potential Additional Requirements
• Collect general system information • Create CSAM entry and enter information • Create PTA and upload to CSAM • Perform security categorization • Enter remaining information in CSAM System Identification (Purpose, attributes, funding, etc.) and Narratives (System description and Technical description)	• Perform PIA and upload to CSAM • Perform E-Authentication Risk Assessment and upload to CSAM (under Appendix G5: E-Auth Risk Assessment OMB M04-04)

Table 4 – RMF Step 1 Requirements (Categorization)

Below is the overall process for RMF Step 1.

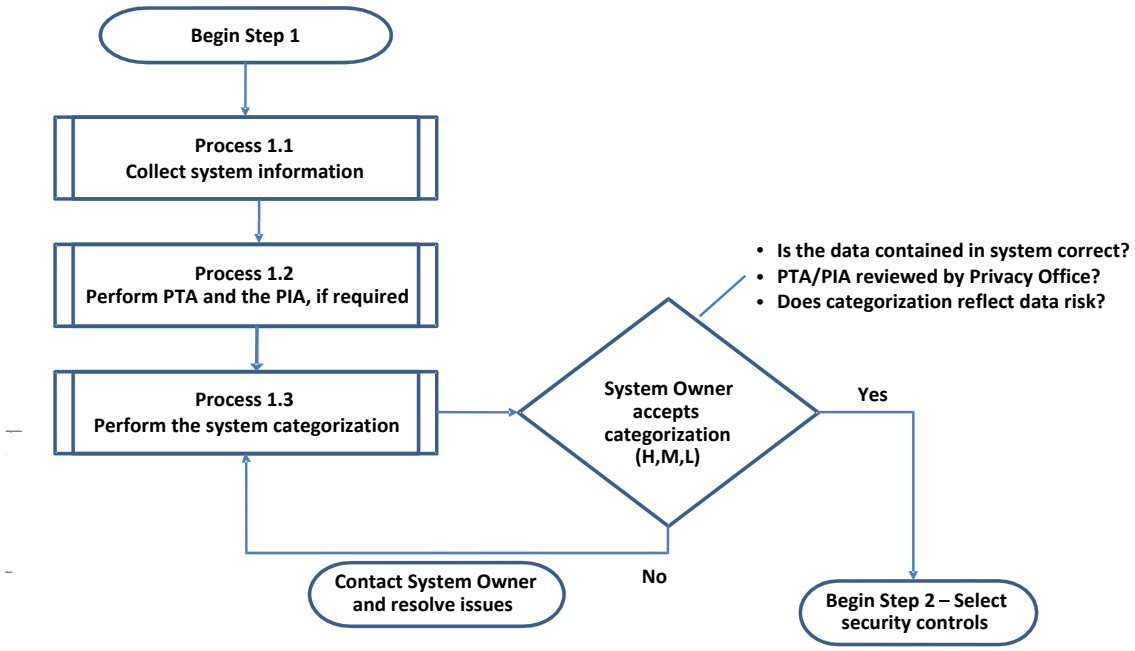

Figure 1 – RMF Step 1 Process (Categorization)

980 Step 2: Select Security Controls

Just as FIPS 199 and NIST 800-60, Rev. 1 are mandatory for the categorization of information systems, FIPS 200 and NIST 800-53, Rev. 3 are mandatory for the selection of the corresponding security control baselines. Once the FIPS 199 security categorization of the information system is documented in CSAM, the corresponding set of controls (high, moderate or low) will automatically be selected for the information system within CSAM. This security control baseline must then be tailored within CSAM to include the selection of inherited controls and the documentation of the implementation of each control

Requirements for All Systems/Programs	Potential Additional Requirements
• Identification of all common/inherited controls • Compliance descriptions identified for every control including tailoring • Create any needed compensating controls • Develop Contingency Plan (CP), CP test training and testing documents	• 508 Compliance • System of Record Notice (SORN) • Configuration Management Plan(CMP) • Incident Response Plan (IRP) • Disaster Recovery Plan (DRP) • Interconnection Security Agreement (ISA) (Optionally this could be in the form of a Memorandum of Understanding (MOU) or Service Level Agreement (SLA))

Table 5 – RMF Step 2 Requirements (Select Security Controls)

Below is the overall process for RMF Step 2.

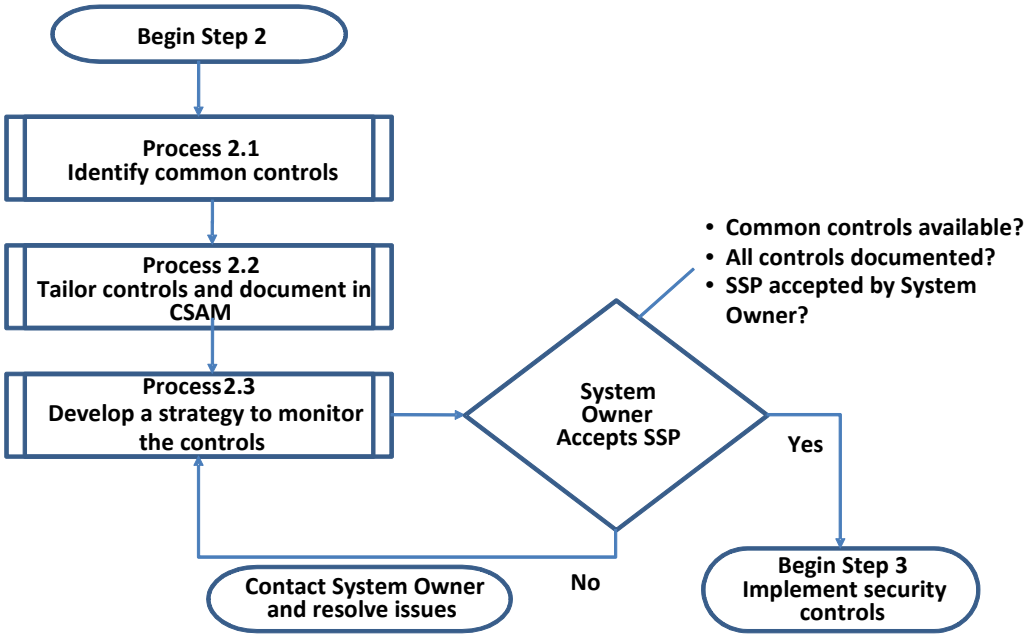

Figure 2 – RMF Step 2 Process (Select Security Controls)

Step 2 focuses on completion of the compliance descriptions in CSAM for all security controls. The documentation includes the identification of all common controls, selection and documentation of the remaining controls, and any tailoring or compensating controls.

At USDA, identification of the controls the system can inherit is the responsibility of both the common controls provider and the system owner and/or ISSO/ISSPM. In the case of Department Program Management controls, this may involve the Department's CIO and/or CISO. The common controls provider must publish what controls are inheritable in CSAM and may also have them listed in other documents that are required by the data centers and/or other service providers. The controls are then formally documented as an appendix to the ISA which is then confirmed by signature by the common controls and/or data center provider.

981 Step 3a: Implement Security Controls

Step 3 focuses on the implementation of security controls during system development and/or after the system has been completed. Implementation of the security controls is the responsibility of the System Owner and/or the common controls provider where controls are inherited. Once the controls are implemented, the SSP compliance descriptions, CP, CMP and IRP should be finalized to capture the true "as-built" implementation. A CMP, IRP, and CP may need to be developed for the system unless these are covered under another plan elsewhere in the hosted environment.

Requirements for All Systems	Potential Additional Requirements
• Finalize SSP compliance descriptions • Finalize CP	• 508 Compliance • Finalize CMP, IRP and DRP (If required)

Table 6 – RMF Step 3 Requirements (Implement Security Controls)

Below is the overall process for RMF Step 3a.

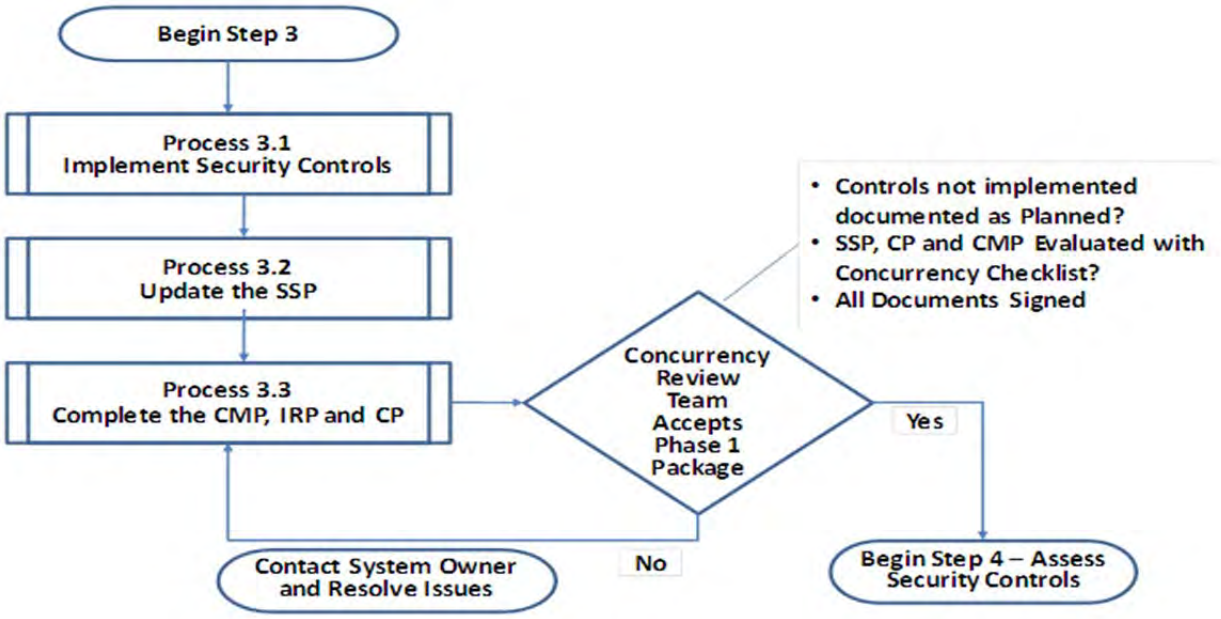

Figure 3 – RMF Step 3 Process (Implement Security Controls)

982 Step 3b: Concurrency Review

When the SSP is complete, it needs to be submitted for Step 3 concurrency review. The user submits an email to the concurrency review team at Cyber.Communication@usda.gov stating the package is ready for review in CSAM.

This concurrency review is primarily for the security plan and the categorization; however, the supporting documents (CP, CMP, ISA, PTA, and/or PIA) that are present at the time of the review will also be reviewed. If the concurrency review team finds any issues with the documentation, they will notate the issues in the concurrency review checklists and return the checklists to the agency. The key items for the Step 3 review are the system categorization and the security plan. Since Issues with the remaining documents do not have a significant effect on testing they can be addressed concurrently with performing Step 4 testing. The checklists utilized for concurrency review are located in Appendix C.

The result of the concurrency review is either passage of the system to Step 4 (Assess Security Controls), or the documentation is returned for further refinement with a checklist of items to remediate. Agencies cannot proceed to Step 4 until notified via concur memo that the system has successfully completed the Step 3b concurrency review. If the documentation is returned with a remediation checklist noting issues identified with the security plan, system categorization or other documents to be addressed, the system must be re-submitted to the concurrency review manager for verification that the issues have been adequately addressed.

Upon satisfactory completion of concurrency review, the concurrency review manager will ensure that the RMF Step 3 concur memo is issued. Once the RMF Step 3 concur memo is issued, the SSP shall not be modified without first discussing the changes with the COE liaison and the concurrency review team. The SSP should not be unilaterally modified by the System Owner until after the Program/system is authorized to operate

983 Step 4: Assess Security Controls

The purpose of this step is to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This step also addresses specific actions to be taken or planned to correct deficiencies in the security controls, and to reduce or eliminate known vulnerabilities in the information system.

Please note that the RMF Step 4 (Assessment) for moderate/high systems must be performed by a different (independent) entity than the one utilized for RMF Steps 1-3 (Documentation and Implementation).

The term independent assessor is defined as follows:

- An independent assessor is one who is impartial and not influenced by the system owner or their direct staff during the conduct of the assessment of security controls or the reporting of the results.
- Independent assessors and/or assessment teams may be in-house permanent teams or outsourced as needed. However the services are performed, strict measures must be put in place to obtain an impartial assessment result.
- To obtain impartiality, the system owner should not be directly involved in the management of, or contracting for, the assessment services. If this cannot be done, the system owner must put in place strict measures and/or contracting language to ensure that they cannot influence said assessment services.
- The assessor (contractor’s company) cannot be directly or indirectly involved in the development, management, or operation of the security controls to be assessed.
- If a system is working through RMF steps 4 through 6 for the first time, assessment of this system must be performed by a different contractor than the one that performed RMF steps 1 through 3.
- An independent assessor or ISO team must ensure that Plans of Actions and Milestone (POA&M) are developed for information that document the planned remedial actions to correct weakness or deficiencies noted during assessment and to reduce and eliminate known vulnerabilities in the system.

Tasks Performed by Certifier	System Owner Requirements
• Develop Security Assessment Plan • Assess security controls • Analyze findings / quantify results • Develop/update Plans of Action and Milestones (POA&Ms)	• Provide certification coordination with Certifier • Ensure support system administration personnel are available during testing • Ensure system is ready for testing

Table 7 – RMF Step 4 Tasks (Assess Security Controls)

Below is the overall process for RMF Step 4.

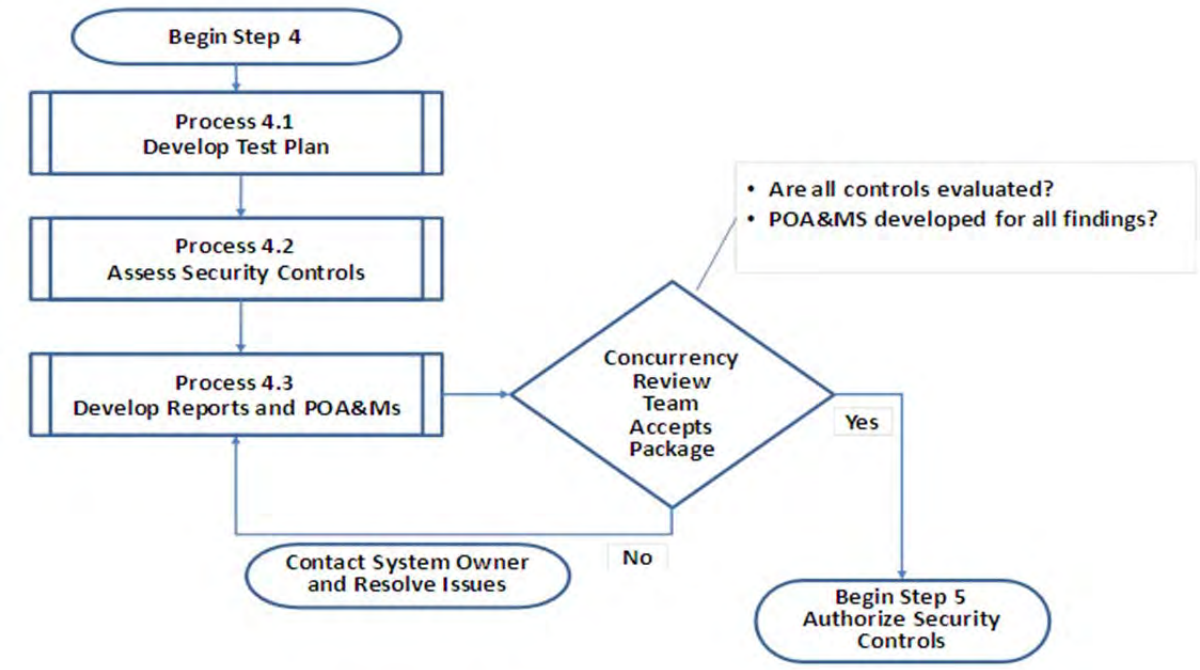

Figure 4 – RMF Step 4 Process (Assess Security Controls)

984 Step 4b Submit the Package for Final Concurrency Review

The system owner/ISSPM/CISO sends an email to the concurrency review team at Cyber.Communication@usda.gov stating the package is ready for review in CSAM. The concurrency review team will review the system's Step 4 documentation against the concurrency review checklists for compliance with NIST and Departmental standards. This concurrency review covers all Continuous A&A package documents. At the conclusion of the concurrency review process, the System Owner/Authorizing Official will receive either a concur memorandum from

OCD with a recommendation to proceed to authorization or one or more checklists listing items that must be remediated and re-reviewed prior to the issuance of a concur memorandum

985 Step 5 Authorize Information System

During Step 5, the required evidence is produced to provide the AO with the information needed to make an informed risk based decision. The residual risk report documents the risk determined for the vulnerabilities found during assessment of the security controls. The subsequent POA&Ms include costs and remediation plans.

Tasks Performed by System Owner (SO)	Authorizing Official (AO)
• Remediate AO identified issues if necessary to achieve ATO • E-mail ATO letter to Cyber.CSAM@ocio.usda.gov and request to update the restricted ATO field in CSAM	• Review/validate risk, POA&M and ATO constraints with System Owner • Generate authorization recommendation or denial with System owner involvement

Table 8 – RMF Step 5 Tasks (Authorize Security Controls)

During authorization, the certification official or ISSPM gathers the key Continuous A&A package documents (Step 4 concur memorandum, POA&M, Security Assessment Report, and SSP) for the AO/DAA to make a decision concerning the authority to operate (ATO). The AO/DAA weighs any remaining vulnerabilities and risks of system operation and then determines what residual risk to accept, what remedial actions are required (i.e., POA&Ms), and whether or not to issue an ATO.

Below is the overall process for RMF Step 5.

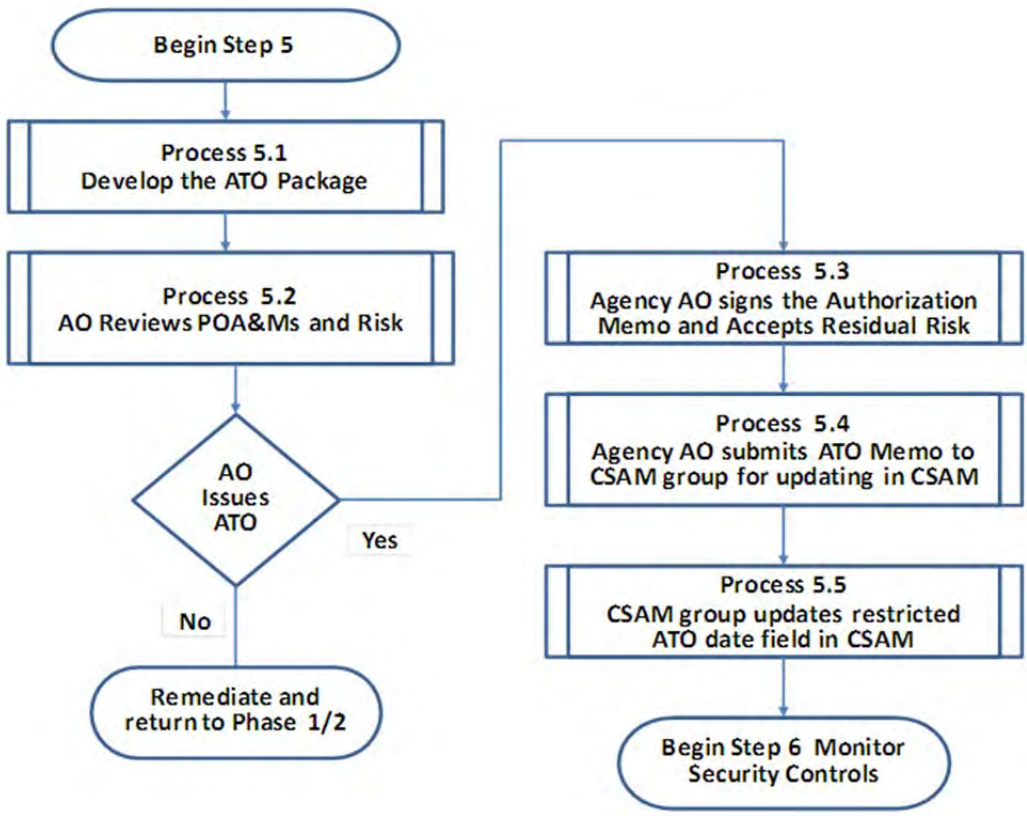

Figure 5 – RMF Step 5 Process (Authorize Security Controls)

986 Step 6 Monitor Security Controls

Once the system is authorized for operation, it is ready to enter the continuous monitoring phase. Continuous monitoring consists of three tasks: (1) configuration management and control; (2) security control monitoring; and (3) status reporting and documentation.

The purpose of this step is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the AO when changes occur that may impact the security of the system. Continuous monitoring activities ensure that secure system management, operation, and maintenance preserve an acceptable level of residual risk.

The activities in this step are performed continuously throughout the life cycle of the information system.

Tasks Performed by System Owner (SO)	Authorizing Official (AO)
• Review system changes and start re-accreditation if major change occurs • Remediate POA&Ms • Document updates to SSP, CP, CMP, IRP • Continual scanning of information systems for vulnerabilities • Review the system and complete the "System Annual Review Memo" found in Appendix B of this document annually.	• Review/validate risk, POA&M, system changes, and documentation with System Owner annually

Table 9 – RMF Step 6 Tasks (Monitor Security Controls)

Below is the checklist for Step 6, Monitor Security Controls.

- Validate that the vulnerability scanning is being accomplished and configuration management issues remediated in a timely fashion.
- Validate that progress is being made on POA&Ms items and milestones are updated in CSAM. Existing Plans of Action and Milestones (POA&M) are updated at least quarterly based on the finding from security controls assess and continuous monitoring activities
- Validate that key controls and the set of controls defined for assessment in that fiscal year are tested annually (reference Appendix E for the sets of controls to assess).
- Annually complete the "System Annual Review Memo" found in Appendix B - Templates to this document.

Below is the overall process for RMF Step 6.

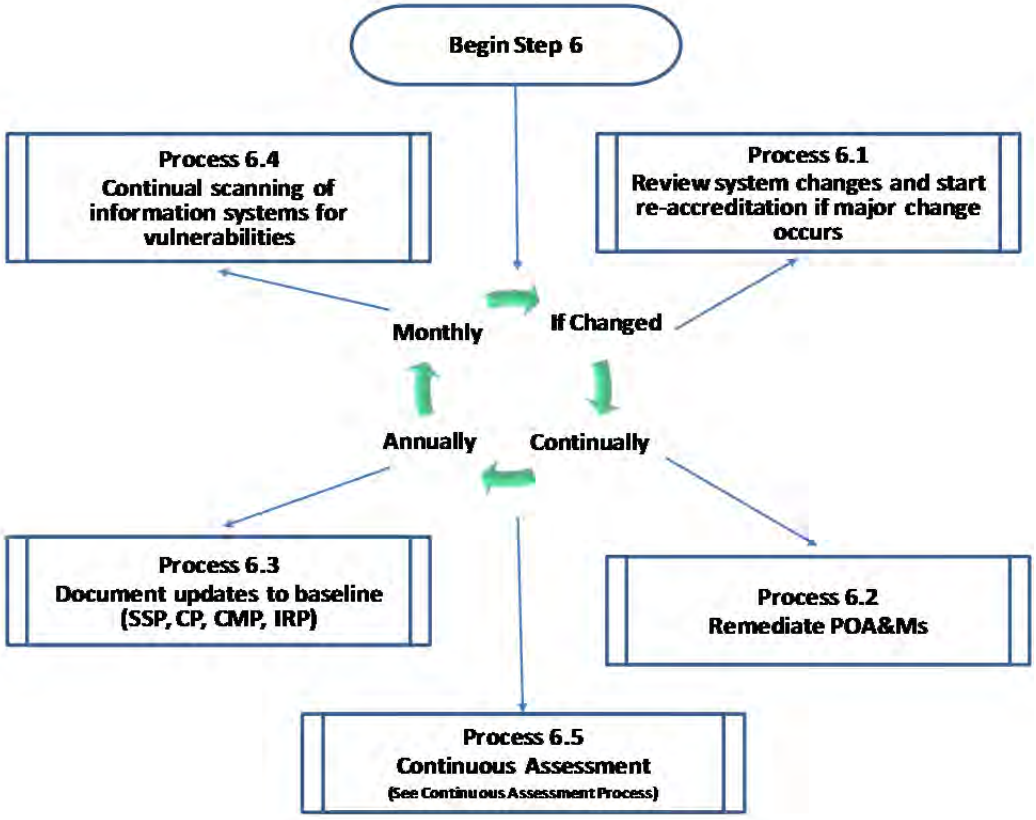

Figure 6 – RMF Step 6 Process (Monitor Security Controls)

Guidance on the Information Systems Security Program (ISSP) for FNCS

1000 Overview

On January 23, 2002, Congress enacted Public Law, 107-347, E-Government Act of 2002. The Federal Information Security Management Act (FISMA) of 2002, Title III, of this law requires that each agency have effective information security controls over Information Technology (IT) to support Federal operations and assets and provide a mechanism for improved oversight of Federal agency information security programs. This Act was designed to strengthen OMB Circular A-130, Appendix III that initially established specific requirements for all agency security programs. As technology has grown more complex and open, the need for effective Federal information security programs in each agency and staff office is essential. In USDA, this program is referred to as the Information Systems Security Program (ISSP).

USDA has undertaken an aggressive role in support of E-Gov to include ensuring that IT systems have been certified and accredited or otherwise authorized as being properly secured. All of these actions require that each agency ISSP be responsive and responsible in supporting security requirements. The material in this guidance is designed to outline the responsibilities of FNCS' ISSP and to specifically define the security roles of the Agency Administrator or Head, Chief Information Officer (CIO) and Information Systems Security Program Manager (ISSPM). These positions are vital components in securing FNCS information technology assets by providing effective agency management and oversight of its ISSP.

1010 References

This Guidance is written in accordance with:

DM 3545-002 USDA Information Systems Security Program (ISSP) Policy

1020 Purpose

The purpose of this guidance is to establish, organize, implement and maintain an ISSP that ensures IT security compliance within FNCS.

Establishment of the ISSP ensures that security is adequately addressed in all phases of the System Development Life Cycle (SDLC), CPIC process, operations, maintenance activities and other IT functions. The FNCS agency ISSP will include the following responsibilities:

- Create a Security Plan for the FNCS Security Program.
- Categorize sensitivity of information and information systems in accordance with FIPS 199.
- Conduct regular risk assessments for IT systems and computing devices.
- Implement effective risk mitigation strategies.
- Manage the formal Certification and Accreditation (C&A) of all agency IT systems.
- Monitor security controls throughout the System Life Cycle.
- Use the Capital Planning and Investment Controls (CPIC) process to formulate and plan security costs for all systems.
- Monitor the system Configuration Management (CM) process of all systems.
- Maintain agency annual Program and System Security Plans.
- Manage an effective Security Awareness and Training Program.

- Manage the agency Security Incident Response Program.
- Conduct annual self-assessments of the agency IT systems using NIST 800-53.
- Monitor IT systems using audit trails, control logs and other mechanisms.
- Establish an electronic inventory of all IT systems and computing devices.
- Maintain an IT system inventory in the FNCS approved systems.
- Disseminate Department policy and procedures to all agency personnel.
- Respond to regular and ad hoc reporting requirements and audits by internal or external agencies.
- Monitor agency compliance to USDA, OMB, NIST and other governing bodies' policy for security.

1030 FNCS ISSP Structure

FNCS has elected an alternative structure for the ISSP. An alternative structure is useful in agencies that have more than 1,000 IT users. Currently, FNCS has approximately 1,500 users that are made up of employees and contractors. The FNCS Information Security Office (ISO) is responsible for implementing FNCS' ISSP. Within the hierarchy of OIT, the ISO will be located under the Office of the Chief Information Officer.

The Alternative structure of an ISSP consists of a three-tier management approach, ISSPM, ISSM and ISSO:

- The duties of the ISSPM, ISSM and ISSO shall be designated as the agency sees fit, as long as all responsibilities are designated in writing and effectively executed.
- The Associate CIO for Cyber Security (ACIO CS) must be notified in writing, that an Alternative ISSP is being implemented at FNCS.
- The FNCS CIO has formally designated one (1) Information Systems Security Program Manager (ISSPM) via the "Designation of ISSPM and Deputy ISSPM" form.

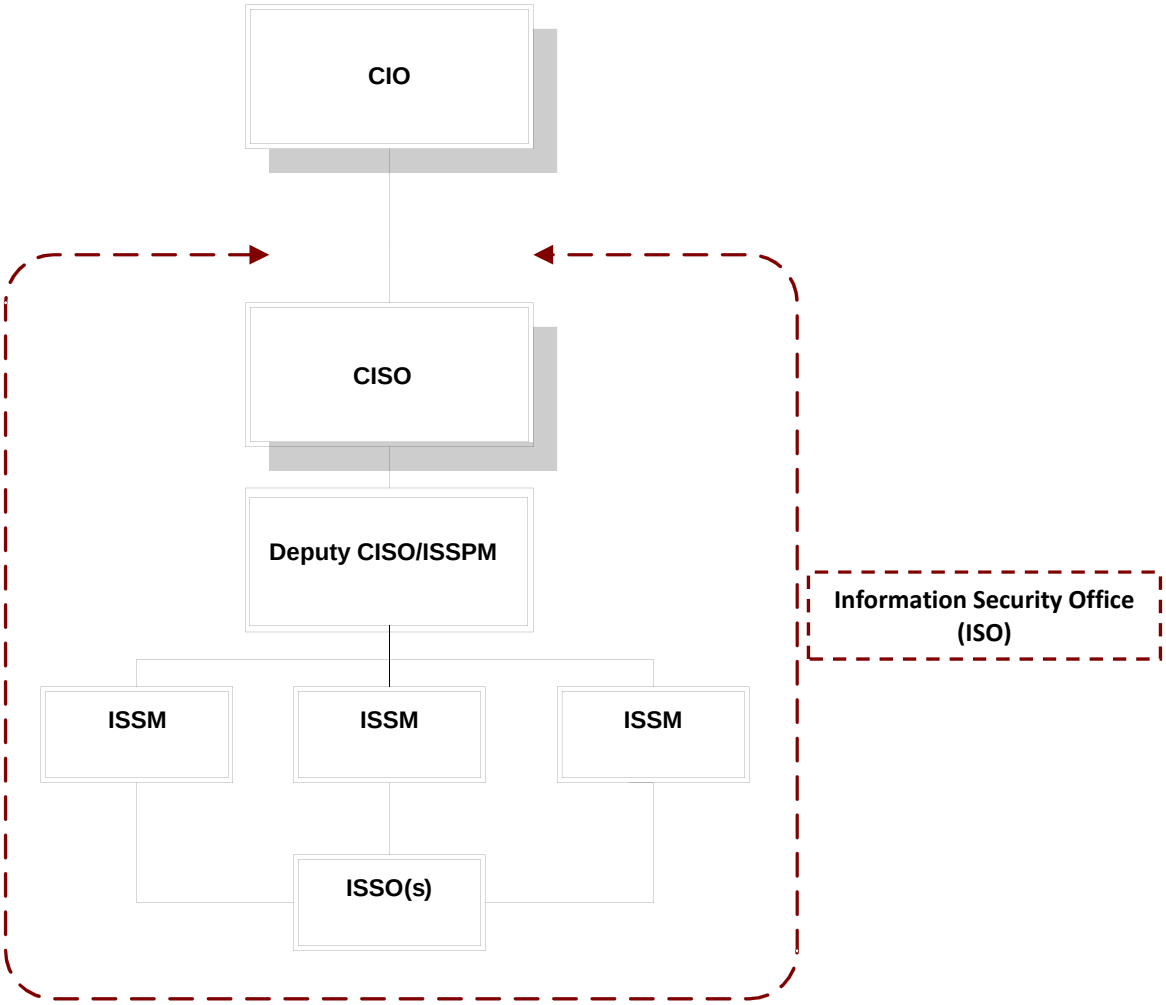

Figure 7 – OIT Information Security Office Management 4-Tier Structure

1040 Management Structure of the ISSP

The Chief Information Security Officer (CISO) and Deputy CISO/ISSPM:

The duties and responsibilities of a CISO and Deputy CISO are diverse, comprehensive and complex. This position is responsible for understanding and mitigating the Agency's information system risks. This position is also responsible for leading investigatory and compliance work. The CISO, Deputy CISO/ISSPM, and some ISSM positions, as defined by OIT leadership, should be considered High Risk Public Trust positions as defined by 5 CFR 731. As a result, FNCS must ensure that the individuals in these positions have the appropriate level of background investigation completed. Additionally, FNCS is responsible for determining the National Defense sensitivity level of these positions as defined in 5 CFR 732 and obtaining the appropriate level of security clearance. Individuals in these positions will have a direct reporting relationship with the

USDA Agriculture Security Operations Center (ASOC) and will require a level of clearance meeting with the USDA ASOC's minimum security clearance requirements. Information Systems Security Manager (ISSM):

The ISSM is responsible for managing the tactical efforts of a business, functional, or operational entity within an agency. Their responsibilities include the daily operational security issues of the business area and overall management of the "front line" security requirements for the business area. This individual may often be called upon to assist in the resolution of certain system security issues.

Information Systems Security Officer (ISSO)

The System Owners shall appoint as many Information Systems Security Officers (ISSOs) as necessary to comply with this guidance. This person is responsible for the day-to-day security administration for one or more information systems. Theirs is an operational security effort regarding the system(s) for which they are responsible. The ISSOs will be responsible for coordinating audit and certification/accreditation activities. The ISSOs will work closely with and report directly to the ISSM assigned to their system.

1050 ISO Roles and Responsibilities:

1051 The CIO will:

1. Act as or designate the FNCS Chief Information Security Officer (CISO).
2. Support the strategic requirements of the ISSP.
3. Ensure adequate funding, training and resources are provided to the ISSP to support the agency mission.
4. Facilitate the resolution of high-level security matters within the agency by acting as a proponent for ISSPM.
5. Serve as the Certifying Official for FNCS security requirements (i.e., Annual Security Plans, FISMA, C&A and other formal reporting requirements, waiver requests and certification of agency IT Systems).
6. Determine the need for C&As with the System Owner.
7. Communicate to the ACIO CS in writing, the designated ISSPM.
8. Designate a Contingency Planning Coordinator (CPC).
9. Other responsibilities for the CIO are written in the procedures for C&A, IT Contingency Planning, SSP, SDLC, CPIC and IT Restricted Space and Physical Access Control.

1052 The CISO/Deputy CISO/ISSPM will:

1. Manage the agency ISSP including the activities and training from USDA Enterprise training vehicles of the ISSM/ISSOs.

2. Support the strategic security program requirements to include: planning, budget analysis, Department policy review and internal policy formulation, agency FISMA, POA&M and audit reporting requirements, agency Security Architecture and agency IT CPIC.

3. Consolidate individual security reports from all functional and operation business areas into one agency combined report (i.e., monthly scans, patches, incidents) for higher level management, including ACIO CS.

4. Monitor progress of the ISSM/ISSOs to ensure that they meet the necessary program security requirements of NIST 800-53 and departmental policy directives.

5. Serve as the principle consultant to the agency CIO and senior management, including the ACIO CS, on the Agency's security posture, policy, procedures and strategic planning

6. Submit all system SSPs to the Office of Cyber Security by the last working day of April each year. Include POA&Ms for security weaknesses not corrected from the prior year submissions.

7. Coordinate agency Incident Response with the ISSM/ISSOs to include all associated actions necessary to mitigate the risk to business area systems.

8. Oversee the implementation of agency security policies, procedures and guidelines and ensure compliance.

9. Participate in monthly Information Technology Management Group (ITMG) and Information Security Sub-Council (ISSC) meetings.

10. Monitor server room access list with ASD; verify and approve list quarterly.

11. Host monthly ITMG & ISSC sub-meetings with ISSMs, ISSOs, and Privacy Officer to disseminate information.

12. Communicate with the OIT/Security liaisons in other agencies and USDA.

13. Lead the development of the agency security architecture for all IT systems, including data encryption standards.

14. Oversee the C&A process. Oversee Contingency and Disaster Recovery Plans for each site, in coordination with COOP.

15. Approve updates to SSPs.

16. Enter all POA&Ms into the USDA approved tool.

17. Create and disseminate updated security document templates to the ITPM, System Owners and Contractor/Development Teams.

18. Lead special projects, e.g. CSAMS development, 702 handbook updates, etc.

19. Ensure that ISSM/ISSOs are designated to provide adequate security to business, functional or operational entities.

20. Ensure that the designated ISSPM is a permanent member of all system development, telecommunications planning and the System Development Life Cycle (SDLC) planning teams.

21. Ensure that the ISSPM receives role-based and specialized security-based training.

1053 The ISSM will:

1. Serve as point of contact (POC) for all information security matters and provide subject matter expert guidance to agency personnel.
2. Manage C&A process every three years or when major system changes occur.
3. Ensure all systems follow and complete the C&A process prior to actual operation.
4. Review Privacy Impact Analysis (PIA) annually in coordination with the Privacy Officer.
5. Review Systems of Record Notice (SORN) annually in coordination with the Privacy Officer.
6. Create and disseminate updated security document templates to the ITPM, System Owners and Contractor/Development Teams.
7. Disseminate/Issue departmental security policy and procedures.
8. Create and monitor compliance with the agency Communication Plan.
9. Ensure FISMA compliance in the System Development Life Cycle (SDLC), operations, maintenance and other IT functions of all FNCS systems.
10. Ensure FISMA compliance in telecommunications planning.
11. Attend system status meetings as the subject matter expert for security.
12. Perform internal self-assessments and audits of IT systems to ensure compliance with federal and departmental policy and procedures, includes Annual OMB A-123 self-assessments, FISMA and annual on-site security reviews.
13. Participate in general and role-based security training to enhance knowledge and skill level.
14. Enforce system security controls that protect agency information using authentication techniques, cryptography, firewalls, logical and physical access controls and comprehensive departmental incident response procedures with all system administrators (SA) and system owners.
15. Assist in the categorization of information systems and determine sensitivity levels in coordination with system owners.
16. Lead the development of disaster recovery, contingency plans and other emergency plans for IT systems. Ensure all plans are NIST compliant.
17. Lead the effort to test disaster recovery and contingency plans as directed by the ISSPM.
18. Monitor physical spaces to ensure that the security requirements of IT restricted spaces are upheld.
19. Assist in the planning of IT restricted space which includes advising the

ISSPM when IT restricted space does not comply with security requirements.

20. Assist in managing a Security Awareness program that is compliant with departmental policy.
21. Participate in the development of FNCS architecture for IT systems.
22. Monitor and coordinate patch management and scanning techniques for all systems.
23. Participate in identification and mitigation of all system vulnerabilities.
24. Evaluate system environments for security requirements and control including: IT Security architecture, hardware, software, telecommunications, security trends and associated threats and vulnerabilities.
25. Implement system security controls that ensure the protection of Sensitive but Unclassified (SBU) information.
26. Coordinate the provision of security controls for Portable Electronic Devices (PEDS) and other wireless technology.
27. Participate in the Overall Agency Security Plan and coordinate with Information ISSOs to ensure that current system specific plans are in place for all IT systems.
28. Coordinate or participate in risk assessments of all systems and mitigate vulnerabilities.
29. Monitor Configuration Management (CM) practices to ensure that security controls are maintained over the life of the IT systems, and formulate and prepare an electronic agency inventory for business area computing devices.
30. Plan and document security costs for IT investments and systems.
31. Prepare and update reports to ensure that systems comply with mandated internal and external security reporting requirements, including monthly OMB A-123 Reporting and CPIC.
32. Monitor quarterly LAN/Application user recertification for all systems.
33. Proactively participate in new CS initiatives including, but not limited to, computer investigations and forensics.
34. Prepare and coordinate system owner Incident Responses with the agency ISSPM to include all associated actions necessary to mitigate the risk to systems.
35. In coordination with the ISSO, conduct annual NIST 800-53 self-assessments and create POA&Ms.
36. Participate in special projects as directed by the ISSPM.

1054 The ISSO will:

1. Be knowledgeable of Federal, Departmental, and agency security regulations when developing functional and technical requirements; serve as a POC for system users with security issues.

2. Manage security controls to ensure confidentiality, integrity and availability of information; build security into the system development process and define security specifications to support the acquisition of new systems; develop testing processes that ensure adequate testing of security controls, either by recreating production environment or by developing tests that provide the same effect.

3. Review and sign off on system procurement requests to ensure that security has been considered and included.

4. Assist with security controls and associated costs in the CPIC Process.

5. Perform monthly patching.

6. In coordination with the ISSM, conduct annual NIST 800-53 self-assessments and create POA&Ms.

7. Participate in the Risk Management meetings.

8. Prepare and update reports to ensure that the system(s) complies with mandated internal and external security reporting requirements, including monthly Patching & Scanning Certification and monthly FISMA scorecard.

9. Provide artifacts and data to the ISSM for monthly A-123 reports, annual A-123 Audits and annual on-site security reviews.

10. Create POA&Ms as needed after scans and patch reports.

11. Ensure adherence to system security controls that protect Sensitive But Unclassified (SBU) information using authentication techniques, encryption, firewalls, and access controls.

12. Report all incidents to the ISSPM in following Incident Response Procedures.

13. Participate in the C&A process, including updates to the overall Agency and System Security Plans (SSP) for the program; serve as a key advisor in risk assessments of all systems and mitigate vulnerabilities; adhere to CM practices to ensure that security controls are maintained over the life of IT systems; update the electronic agency inventory for all agency computing devices.

14. Develop Disaster Recovery/Contingency Plans (DR/CP) and other emergency plans for systems, and update annually. Develop, test, and maintain system contingency plans, backup and storage procedures; document all procedures according to departmental and agency standards; conduct annual executable or table-top DR tests and create POA&Ms; Update system SORN annually in coordination with ISSM and Privacy Officer. Update SSP, Risk Management Plan (RMP) and CMP annually Audit and monitor application, system and security logs for security threats, vulnerabilities and suspicious activities; report suspicious activities to the agency ISSPM; Participate in identification and mitigation of all system vulnerabilities.

15. Grant access and password requests after receiving authorization from system owners or from authorization officers designated by system owners.

16. Update the CCB Charter annually and as needed, and CCB minutes as needed.

17. Support and facilitate the security awareness, training and education program; follow up with users for annual CSAT and Privacy training;

18. Participate in monthly Security Office/Privacy meetings.

19. Assist the ISSM in any other security related duties, as required; participate in special projects as directed by the ISSPM.

Guidance on Risk Management at FNCS

1200 Overview

Protection of information assets and maintaining the confidentiality, integrity and availability of FNCS information assets and telecommunications resources are vital in meeting FNCS program delivery requirements. Implementation of security measures such as a risk management program, effective security controls, certification and accreditation of IT systems and updated security plans are vital components in our response to this situation.

Risk "is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence".

This guidance provides the strategies used to implement an FNCS Risk Management (RM) Program. RM includes a structured approach to assessing risk, identifying vulnerabilities, reporting, accepting risk, implementing appropriate mitigation strategies and continuous evaluation and assessment of information resources. Procedure is updated and reviewed annually.

1210 References

This Guidance is written in accordance with:

- NIST Special Publication 800-53 Rev. 3
- NIST Special Publication 800-30
- USDA DM 3540-000 Risk Management Program
- USDA DM 3540-001 Risk Assessment Methodology

1220 FNCS Risk Management

1221 Risk Assessment Guidelines

Risk assessments evaluate the sensitivity and criticality of the system or application data to the vulnerabilities, threats, impacts, and potential countermeasures that may exist in its environment.

A risk assessment includes the following activities:

- Conduct System Characterization
- Conduct Vulnerability and Control Analysis
- Conduct Threat Analysis
- Conduct Impact Analysis
- Develop Risk Mitigation Strategies
- Determine Risk Levels
- Develop Business Cases
- Report Residual Risks

Risk assessments are performed for new system development and major system modifications.

Risk assessments are performed on systems and major applications every three (3) years.

USDA has established a risk assessment methodology. For the complete methodology on assessing risk, please refer to the USDA DM 3540-001 Risk Assessment Methodology

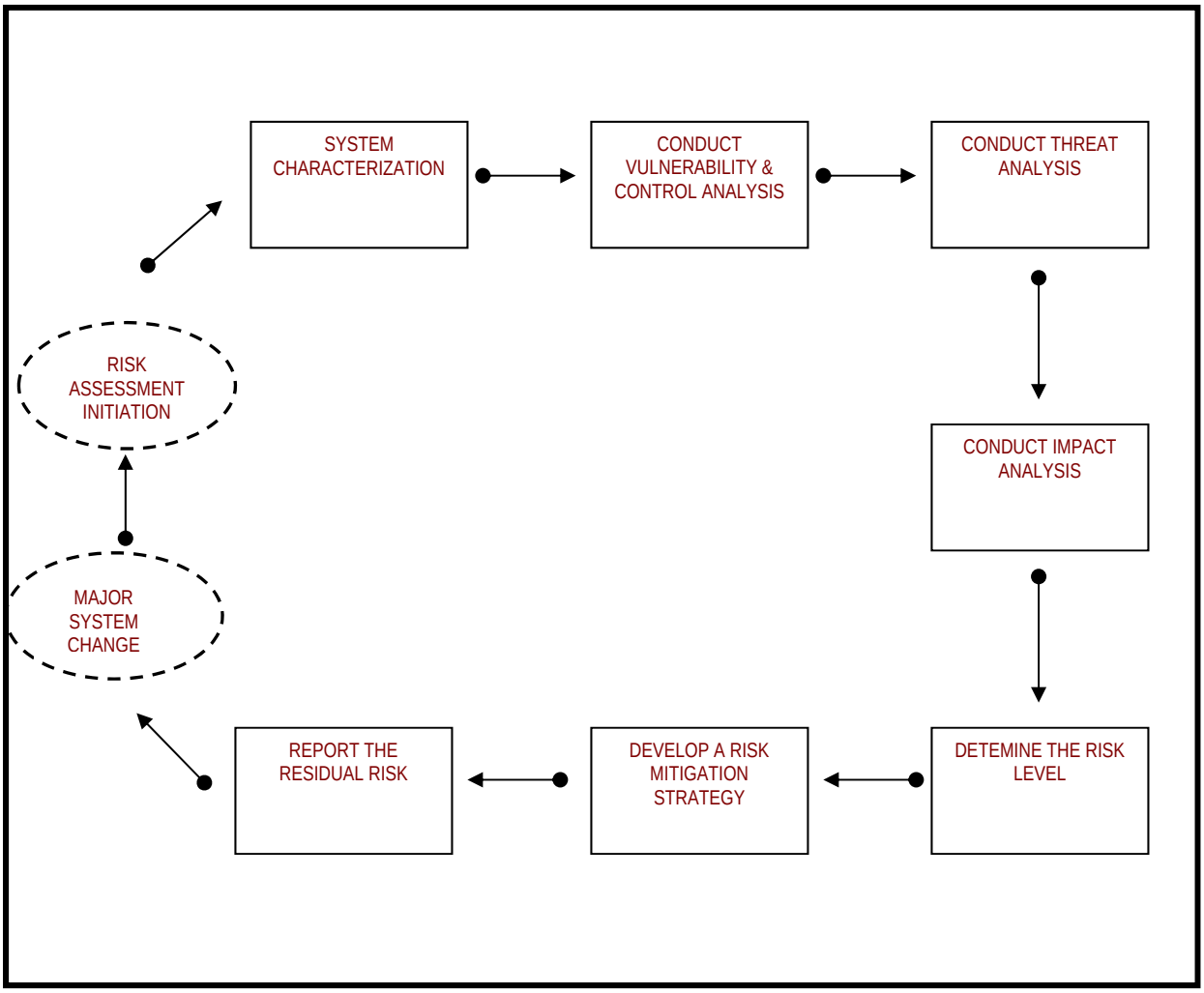

Figure 8 – General USDA Risk Assessment Methodology

Step 1:

1. Identify system mission, review system architecture and determine system boundaries, interfaces and data flow.
2. Determine data categories and sensitivity.
3. Understand system users.
4. Review system security policies.

Step 2:

1. Conduct manual assessments.
2. Conduct automated scans, penetration tests and security control assessments.
3. Review previous security plans and risk assessments.

Step 3:

1. Determine threat types.
2. Develop a listing of threat sources.
3. Determine probability of threat occurrence.

Step 4:

1. Consider data categories.
2. Determine mission impact severity in terms of confidentiality, integrity and availability.

Step 5:
1. Determine threat probability of occurrence.
2. Determine impact criticality.

Step 6:
1. Review threat list.
2. Determine impacts.
3. Implementation countermeasures.
4. Develop a threat mitigation list based on available resources.

Step 7:
1. Document remaining risk(s) and a plan for future action.
2. Include residual risk in Certification and Accreditation package.

1222 Risk Mitigation Guidelines

The process for risk mitigation is as follows:

- Review each potential threat and the action(s) that are necessary to reduce or eliminate the threat such as adding access controls to critical assets.
- Determine the cost of mitigating the threat to the organization.
- Decide whether the financial output is possible for each threat. For instance, what hardware or software measures will add protection and is the cost justifiable.
- Implement the solution that reduces or mitigates the threat.
- Risk mitigation is a systematic methodology used by senior management to reduce mission risk.
- Risk mitigation can be achieved through any of the following risk mitigation options:

    1. **Risk Assumption**. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
    2. **Risk Avoidance**. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified).
    3. **Risk Limitation**. To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising vulnerability (e.g., use of supporting, preventive, detective controls).
    4. **Risk Planning**. To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls.

5. **Research and Acknowledgment**. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.

6. **Risk Transference**. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

1223 Risk Evaluation and Assessment Guidelines

Within the SDLC Operations/Maintenance phase, each system is a part of the continuous monitoring process. FNCS continuous monitoring includes the monitoring of risks identified in risk assessments and evaluating risks that were discovered and accepted. This is an ongoing process.

1230 Risk Acceptance Guidelines

A Risk Management Acceptance report is to be completed and submitted to the ISSPM when vulnerabilities are found within a system and the System Owner accepts the risk (vulnerability). This includes discovery of vulnerabilities through:

- Recognition by a user or system administrator.
- An equipment or network scan.
- An annual self-assessment.
- The Certification and Accreditation (C&A) and security control assessment process.

Please see the Appendix E for the Risk Management Acceptance Form and instructions.

1240 FNCS Risk Management Program Team

- The Risk Management Team will provide communication, support and mitigation techniques for all FNCS Systems.

- The risk management program requires each team member to manage:

  - Vulnerability mitigation
  - Patch management
  - Virus maintenance
  - POA&M and/or possible waiver information

- Weekly meetings facilitated by an ISO ISSM and the Deputy CISO allow each member to report on vulnerability scans, patch and virus reports and discuss how the results have impacted the business continuation and risk minimization for each portion of the FNCS GSS Net network.

- Collectively, the Risk Management Team will create a weekly all-inclusive report on risk management results to be submitted to the ISO for approval.

1241 Vulnerability Identification and Remediation Procedures

As part of FNS's Continuous Monitoring Process, vulnerability identification and remediation is crucial to keeping FNS data safe and secure. This procedure is meant to outline how the agency identifies, validates, and reports the vulnerabilities as well as setting the requirements for

remediating those vulnerabilities as required by NIST SP 800-53 Control RA-5: Vulnerability Scanning.

1242 Identification, Validation, and Reporting

FNS's Information Security Office is responsible for identifying, validating, and reporting vulnerabilities with the organization. FNS utilizes an Enterprise Vulnerability Scanning and Risk Management Appliance, in conjuncture with other security tools, to scan FNS's network. Scans are scheduled to run continuously.

The Enterprise Vulnerability Scanner produces a vulnerability score for every asset scanned. This score is converted to a Risk Score for that asset on a "0-100" scale. A Risk Score of "0" represents a low risk to the organization while a score of "100" represents a severe threat. This is to create a more standardized and simplistic representation of the severity of any given asset to management and system administrators.

As we move towards continuous monitoring, the FNS Information Security Office (ISO) reports on the security posture of the organization through the Executive Situational Awareness Briefing (ESAB) on a predefined schedule. This briefing is intended to illustrate the current state of the security of the organization's IT infrastructure. This includes identifying the top vulnerable workstations, internal servers, and our DMZ environment, patch deployment compliance, and software version trends. The ESAB reports on the network segments it has visibility on and has limited capability on reporting on cloud infrastructure such as but not limited to National Information Technology Center (NITC), National Technology Information Service (NTIS), and the USDA's Enterprise Virtual Private Network (EVPN). The ESAB will serve as the means for ISO to report IT Security weakness to FNS Office of Information Technology (OIT) management. Based upon the severity of an asset's weakness, ISO will then create tickets through the OIT ticketing system and assign them to the responsible parties for remediation. It is the responsibility of ISO to validate vulnerabilities identified and expel any false positives from the ESAB report.

1243 Remediation of Identified Vulnerabilities

The remediation of an asset's vulnerabilities is determined by the type of asset and the severity of the Risk Score. An asset is defined by one of the following types: Demilitarized Zone (DMZ) Server, High Value Target (HVT), an Internal Server, or User Workstation. A DMZ server is defined as asset hosted within the DMZ network segmentation and public facing. An Internal server is any asset that manages access to a centralized resource or service in a network. A HVT is defined as a resource with access to a mission critical data within the organization. Finally a General User is an asset operated by non-high-value target.

An asset's Risk Score is categorized the following severity categories: High, Moderate, Low, and Very Low. A system identified on the ESAB Top 10 list with a High Risk Score must have steps to be remediated in place within 30 days; a Moderate Risk Score must have steps to be remediated in place within 60 days; a Low Risk Score must have steps to be remediated in place within 90 days; finally, a Very Low Risk Score must have steps to be remediated in place with 180 days. Vulnerabilities identified exceeding the threshold listed will be the System Owner and their representatives' responsibility for remediating. They will work with ISO to create and update POA&Ms in the USDA's Cyber Security Assessment Management (CSAM) for tracking purposes. If the vulnerability cannot be remediated, a risk acceptance must be drafted and signed by the

responsible parties. Vulnerability scores less than the Very Low threshold will be considered informational and not need immediate remediation.

The following scale is used to determine the severity of an asset based on the asset's Risk Score:

	DMZ Servers	High Value Target	Internal Servers	User Workstation
High (30 days)	65+	70+	70+	-
Moderate (60 Days)	50-64	55-69	55-69	-
Low (90 Days)	30-49	44-54	44-54	50+
Very Low (180 days)	18-29	25-44	25-44	30-49

Table 10 – Vulnerability Assessment Risk Score Matrix

Guidance on IT Contingency Planning and Disaster Recovery

1300 Overview

IT Contingency Planning is necessary to ensure that IT systems continue to be operational in the event of major or minor interruptions or a large-scale disaster. Use of formal Contingency and Disaster Recovery Plans (DRP) also ensures that FNCS offices have effective and efficient recovery solutions for their systems.

IT Contingency Planning includes activities designed to recover and sustain critical IT services following an emergency. The IT Contingency Plan and Disaster Recovery Plan are tested, minimally, annually. These arrangements fit into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning. This guidance will cover developing, testing, training, reporting and updating IT systems contingency and disaster recovery plans.

USDA has formed a *Contingency Plan Working Group (CPWG)* that meets to discuss current issues with agency-wide IT Contingency and Disaster Recovery Plans and to provide recommendations for change to USDA Cyber Security. So far, the CPWG has recommended and has been approved to standardize the IT Contingency Plan. Other recommendations to Cyber Security include:

- Standardized Disaster Recovery Plans
- Standardized Business Impact Analysis (BIA)
- Standardized Disaster Recovery Test Plan
- Standardized After Action Report

This procedure is reviewed and updated at least annually.

1310 References

This Guidance is written in accordance with:

- NIST Special Publication 800-53 Rev. 3
- NIST Special Publication 800-34
- NIST Special Publication 800-84
- USDA DM 3570-000 IT Contingency Planning
- USDA DM 3570-001 Disaster Recovery and Business Resumption Plans

1320 Roles and Responsibilities

1321 The CIO and CISO will:

- Establish and manage the IT Contingency Planning Program within FNCS.
- Ensure sufficient resources exist to develop, maintain and implement IT Contingency Plans and DRPs for each system.
- Designate a Contingency Planning Coordinator and provide training for a Contingency Planning Coordinator and an opportunity for certification.

- Advise Senior Management on Cyber Security reviews and comments on existing Contingency and DRPs.
- Ensure all plans are developed using a USDA approved tool.
- Ensure alternate sites are in place as a back-up operations facility where trained personnel are in place to run systems or applications as needed.
- Ensure all contingency and disaster recovery plans are closely related to the COOP and other Contingency Plans.
- Ensure DRPs are tested at least bi-annually or when a major change occurs to a system.
- Ensure all system recovery procedures are developed, published and tested.
- Provide specialized training for the disaster recovery teams and coordinate general disaster awareness training for all employees.
- Ensure all Contingency and Disaster Recovery plans are reviewed, approved and stored in the USDA recommended database.

1322 The Contingency Plan and Disaster Recovery Coordinator and Stakeholders will:

- Document such appointments in writing and include specific responsibilities in each appointee's job description.
- Serve as the IT contingency planning expert resource for the agency
- Prepare an agency Contingency Program proposal annually for management consideration and approval which describes and schedules contingency activities to ensure compliance with department and agency requirements documented in BIAs with continual improvement as needed from year to year.
- Ensure the following specific activities are included in the Contingency Program proposal and facilitate completion of the activities during the program year:
    - Test-Exercise such that all plans are tested annually,
    - Annual plan review and update of every plan,
    - Review an update recovery strategies annually,
    - BIA review and update at least every two years,
    - Annual contingency training for agency staff and
    - Bi-Annual Refresher training.
- Provide contingency program reports to agency management as needed.
- Ensure new applications and GSS components are brought into the Contingency Program

1323 The System Owner will:

- Review and update the Contingency and Disaster Recovery Plans, annually.

- In conjunction with the ITPM, ensure new personnel receive training for their roles on Disaster Recovery.
- Perform scheduled table top tests, functional exercises and failover tests.
- Perform scheduled system integration tests.
- Ensure the Alternate Site Coordinator has updated contingency and disaster recovery plans along with recovery and reconstitution procedures.

1324 The ITPM and ISSM will:

- Include development, review and updates of contingency and disaster recovery plan in the project management plan.
- Document results of the tests and provide mitigation strategies for deficiencies (POA&Ms).
- Include costs of contingency plan creation, update, testing and training in the project management plan.
- Work in coordination with the Contingency Planning Coordinator to review/approve all contingency and disaster recovery plans.

1330 Contingency Plan and Disaster Recovery Guidelines

- Each system will have a Business Impact Analysis (BIA) performed to identify and prioritize critical IT resources. The BIA also determines the level of system support needed to restore mission critical core business functions.
- Identify preventive controls. Determine which measures are necessary to reduce the effects on a system in the event of a disruption.
- Develop disaster recovery plans that include all of the guidance and supporting procedures needed to restore the system. Recovery and reconstitution procedures are developed at this time. These procedures will address the recovery and reconstitution of the system to a known secure state after a disruption or failure occurs.
- All disaster recovery personnel will maintain an up-to-date (hard copy and/or electronic) DRP in a place easily accessible in the event of a disaster.
- The ISO will provide a schedule for all FNCS system contingency and disaster recovery plans to be tested. All results to be captured in After Action Reports along with mitigation strategies documented in POA&Ms. All contingency plan test results will be reviewed by Cyber Security.
- Each system will have an alternate storage site where the system's data back-ups are stored.
- Each system will have a designated alternate site where recovery procedures and trained personnel are located to operate the system in the event of a disaster. The alternate site will have an Alternate Site Coordinator for each system.

- FNS's telecommunication and e-mail services are provided by Networx. Currently, FNS has a Service Level Agreement (SLA) with AT&T. The details of the timeframe of resumption of system operations can be found in the SLA.

1331 Contingency Training

Contingency training must be provided to information system users consistent with assigned roles and responsibilities when new employees start at FNCS or after a major change to a system occurs and annually thereafter.

1332 Contingency Plan Testing

The ISO will provide a schedule for all FNCS system contingency and disaster recovery plans to be reviewed and updated annually or after major systems changes have occurred.

Guidance on FNCS System Security Plans (SSP)

1400 Overview

Information security has escalated as a result of high-level attention from both the press and media. Recent terrorist attacks have only highlighted the need to ensure that we have the highest level of information security practices. IT System security plans have become the foundation document in the overall security process because they define the system security features and controls.

The SSP provides a summary of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The SSP may also reference other key security-related documents for the information system such as a risk assessment, plan of action and milestones, accreditation decision letter, privacy impact assessment, contingency plan, configuration management plan, security configuration checklists, and system interconnection agreements as appropriate.

It is critical that FNCS SSPs are prepared and updated on an ongoing basis with the most current information concerning each agency's information security practices.

1410 References

This Guidance is written in accordance with:

- NIST Special Publication 800-53 Rev.3
- NIST Special Publication 800-18
- USDA DM 3565-001 Annual Security Plans for Information Technology (IT) Systems
- Federal Information Processing Standards (FIPS) 199
- Federal Information Processing Standards (FIPS) 200

1420 Roles and Responsibilities

1421 The CISO will:

- In coordination with the ISSPM, ensure the CIO signs the transmittal cover letter attesting the completeness and correctness of the plans.
- Ensure all personnel are familiar with annual SSP requirements.
- In coordination with the System Owner, determine which major changes warrant updates to the SSP.
- Develop and maintain an inventory of all IT systems.
- Determine data sensitivity and identify all GSS and applications.
- In coordination with the ISSPM, prepare detailed plans for the overall security program, GSS and applications. Submit to USDA's Cyber Security for review and evaluation.

- In coordination with the ISSPM, submit all SSPs to the Office of Cyber Security by the last working day in April each year; Plans will include a POA&M for security weaknesses not corrected from the prior year submissions. Submit the package electronically and in hard copy to the Office of Cyber Security.
- Ensure that copies of the SSPs are maintained in the ISO.
- Ensure that all IT systems have adequate security controls based on the sensitivity of data, mission critical and value of the data in the system.
- In coordination with the System Owner, determine the need to update the SSPs based on major changes to the system.

1422 The ISSPM will:

- In coordination with the CISO, submit all SSPs to the Office of Cyber Security by the last working day in April each year; Plans will include a POA&M for security weaknesses not corrected from the prior year submissions. Submit the package electronically and in hard copy to the Office of Cyber Security.
- Act as the Subject Matter Expert (SME) on all SSP requirements.
- Approve updates and newly developed SSPs.
- Prepare a security plan for the overall FNCS System Security Program.
- Participate in the development of exception requests.
- Ensure all SSPs are submitted to the CIO with a cover letter for signature attesting the accuracy and completeness of the plans.

1423 The System Owner will:

- Have a thorough knowledge of USDA policy and FNCS procedures for creating and updating SSPs.
- Develop SSPs in coordination with the system administrator, ISSM, ITPM and functional end users.
- Maintain the SSP and verify that the system is deployed and operated according to the agreed-upon security requirements.
- Update the SSP whenever a significant change occurs.
- Assist in identifying, implementing and assessing common security controls.
- Ensure that system users and support personnel receive the required security training.

1424 The ITPM will:

- Have a thorough knowledge of USDA policy and FNCS procedures for creating and updating SSPs.

- Assist the system owner in the creation of the SSP.
- Perform a preliminary review of the SSP and SSP checklist prior to being released to the ISSPM.
- In coordination with the ISSM, ensure SSPs are reviewed and updated annually or as determined when a major change has occurred.

1430 USDA Definitions of System and Major Applications

Please see the following link for the USDA Definitions of a system

- USDA Definitions Document

1431 SSP Guidelines

- An Information System Inventory is required for the General Support System (GSS) all FNCS systems. The systems inventory consists of all systems categorized in accordance with FIPS 199. Please refer to the FIPS 199 for details on system categorization. The System Categorization is documented and submitted to the ISSPM.
- All systems, whether Major Application or GSS are required to have a security plan. Initial SSPs are drafted in the Initiation phase of the SDLC.
- During and prior to completion of the C&A, the security plan is reviewed, updated and formally accepted by the ISSPM.
- All new software or hardware to be considered for inclusion in the NetGSS environment must receive CCB approval.
- All SSPs are reviewed and updated based on upcoming certification and accreditation dates as noted in the CSAM tool. CSAM has the capability of holding SSP documents within the “Appendices” section. For updated templates, contact the Information Security Office. These documents will reference C&A items such as:

  a. Risk Assessment

  b. Plan of Action and Milestones (POA&M)

  c. Accreditation decision letter

  d. Privacy impact assessment

  e. Contingency plan

  f. Configuration management plan

  g. Security configuration checklist

  h. Results of penetration testing

i. All system interconnection agreements (MOUs)

j. Management, Operational and Technical controls based on SP 800-53.

Guidance on the FNCS Systems Development Life Cycle (SDLC)

1500 Overview

The Systems Development Life Cycle (SDLC) is a conceptual model used in project management that describes the stages involved in an information system development project, from an initial feasibility study through maintenance and final disposition.

The inclusion of security requirements early in the SDLC will result in less expensive and more effective security than adding it after a system is operational. This guidance presents a framework for incorporating security into all phases of the SDLC process, from initiation through disposal. This document will provide information to select and acquire cost-effective security controls by explaining how to include information system security requirements in appropriate phases of the SDLC.

It is important to involve other members to be a part of the development team, dependent on the complexity of the system. Other roles may include, but are not limited to: Designated Accrediting Authority (DAA), Certifying Official (CO), member of OIT, Configuration Management Team, Design and Engineering staff and the facilities group.

1510 References

This Guidance is written in accordance with:

- NIST Special Publication 800-53 Rev.3
- DM3575-001 Security Controls on the Systems Development Life Cycle
- NIST Special Publication 800-64

Please see the USDA definition of a system:
http://www.ocionet.usda.gov/ocio/security/sys_definition.html .

1520 Roles and Responsibilities

1521 The CISO will:

- Be responsible for the organization's information system planning, budgeting, investment, performance and acquisition.
- Provide advice and assistance to senior organization personnel in acquiring the most efficient and effective information system to fit the organization's enterprise architecture.

1522 The Information System Security Program Manager (ISSPM) will:

- Be responsible for developing enterprise standards for information security.
- Play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize information security risks to the organization.
- Coordinate and perform system risk analyses, analyzes risk mitigation alternatives, and build the business case for the acquisition of appropriate security solutions that help ensure mission accomplishment in the face of real-world threats.

- Support senior management in ensuring that security management activities are conducted as required to meet the organization's needs.

1523 The ISSM will:

- Ensure all security requirements are met throughout the life of a system.

1524 The ITPM will:

- Ensure security requirements are budgeted for and met throughout the life of a system.
- Work in collaboration with the ISSPM to ensure security needs are incorporated in the system lifecycle.

1525 The System Owner will:

- Play an essential role in security and be intimately aware of functional system requirements.

1526 The Privacy Officer will:

- Ensure that the system meets existing privacy policies regarding protection, dissemination (information sharing and exchange) and information disclosure.

1527 The Legal Advisor will:

- Advise the team on legal issues related to security during the lifecycle.

1528 The Records Management Officer will:

- Work with the ISSPM and the ITPM to ensure that the system security documents are compliant with all applicable laws and regulations.

1529 Contractor/Development Team will

- Ensure all development is compliant with all security requirements within each phase of the SDLC.

1530 SDLC Required Security Documentation and Responsible Teams

Security Requirement Documentation	Responsible Team/Individual
System Categorization	Contractor/Development Team
Preliminary Risk Assessment	Contractor/Development Team
Privacy Impact Assessment (PIA)	Contractor/Development Team
System Security Plan (SSP)	Contract Development Staff, System Owner and ITPM
Interconnection Service Agreement (ISA)	System Owner
Configuration Management Plan	Contractor/Development Team
Risk Assessment	Contractor/Development Team
Security Functional Requirements Analysis	ISSM
Security Assurance Requirements Analysis	ISSM
Cost Considerations and Reporting	System Owner/ITPM
Security Planning	ISSM
Security Control Development	ISSM
Development Security Control Assessment	Security Control Assessment Team
Other planning components	ITPM
Inspection and Acceptance	QA/CM
System Integration	Contractor/Development Team
Security Certification	CIO
Security Accreditation	DAA
IT Contingency Plan	Contractor/Development Team, System Owner, ITPM
Disaster Recovery Plan (DRP)	Contractor/Development Team, System Owner, ITPM

Configuration Management Control	Contractor/Development Team
Continuous Monitoring	ISSM, ITPM, System Owner
Re-Certification	CIO
Re-Accreditation	DAA
Information Preservation	Records Management Officer
Media Sanitization	IB
Hardware and Software Disposal	IB

1540 SDLC Phases

There are eight (8) basic phases of the SDLC as defined by FNCS Office of Information Technology, Systems Development Lifecycle Guide (SDLC Guide), they are:

1. Initiation
2. Requirements Gathering/Analysis
3. Design
4. Development
5. Integration &Testing
6. Implementation
7. Operations/Maintenance (O&A)
8. Disposition

Within each phase of the SDLC security requirements are put in place and tested, please see Tables 11 and 12 for the SDLC Phases and Security Requirements.

1541 SDLC Phases and Security Requirements

Initiation	Research Gathering and Acquisition/ Development	Implementation	Operations/ Maintenance	Disposition
Needs Determination: • Perception of a Need • Linkage of Need to Mission and Performance Objectives • Assessment of Alternative to Capital Assets • Preparing for investment review and budgeting	Functional Statement of Need • Market Research • Feasibility Study • Requirements Analysis • Alternatives Analysis • Cost-Benefit Analysis • Software Conversion Study • Cost Analysis • Risk Management • Acquisition Planning • Acquisition Approval Request (AAR)	• Installation • Inspection • Acceptance testing • Initial user training documentation	• Performance measurement • Contract modifications • Operations • Maintenance	• Appropriateness of disposal • Exchange and sale • Internal organization screening • Transfer and donation • Contract closeout

Table 11 – SDLC Phases and Processes

Initiation	Research Gathering and Acquisition/ Development	Implementation	Operations/ Maintenance	Disposition
• System Categorization • Preliminary Risk Assessment • Privacy Impact Assessment (PIA) • System Security Plan (SSP) • Interconnection Service Agreement (ISA) • Configuration Management Plan (CMP)	• Risk Assessment • Security Functional Requirements Analysis • Security Assurance Requirements Analysis • Cost Considerations and Reporting • Security Planning • Security Control Development • Security Control Assessment • Other planning components	• Inspection and Acceptance • System Integration • Security Certification • Security Accreditation • IT Contingency Plan • Disaster Recovery Plan(DRP) • Configuration Management Control	• Configuration Management and Control • Continuous Monitoring • Re-Certification • Re-Accreditation • Configuration Management Control	• Information Preservation • Media Sanitization • Hardware and Software Disposal • Configuration Management Control

Table 12 – SDLC Phases and System Security Considerations

1542 SDLC Phases and Detailed Security Requirements for each Phase

1543 Phase 1: Initiation

The purpose of the Initiation Phase is to conduct initial assessment of a potential OIT system/application development effort. This Phase helps establish a framework for project success, and includes establishing processes for defining, planning, controlling and communicating about the project.

Deliverables in this Phase include:

- Business Case (FNS758; FNS755)
- Project Management Plan (optional)
- Acquisition Plan / Strategy
- Acquisition Approval Request
- Alternative Analysis
- Cost Benefit Analysis
- Integrated Project Team Charter (optional)
- Security and Privacy Document

- Project Process Agreement (optional)
- Privacy Impact Analysis (optional)
- Privacy Threshold Analysis (optional)

A critical governance body is established in this Phase: the Integrated Project Team (IPT). The IPT should consist of the following core members: Project Lead; Developers; Business Leads; Technical Representative; Security Representative; and COTR. Associate members should include Governance, Network, Telecommunications, Records, O&M, and the Contracting Officer. The IPT is documented in this Phase and functions from Initiation through the Implementation Phase.

The Initiation Phase includes activities, reviews and approvals as identified in the below flowchart.

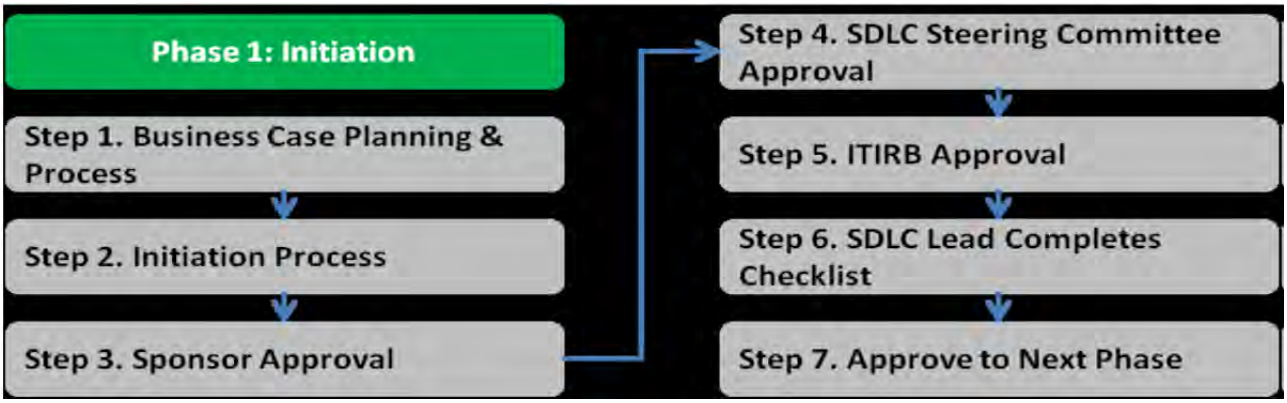

Figure 9 – SDLC Phase 1 Initiation Overview

Upon successful completion of the "Approve to Next Phase" step, the project progresses to the Requirements Gathering and Analysis Phase.

1544 Phase 2: Requirements Gathering and Analysis

This Phase transforms the needs and high-level requirements specified in earlier Phases into unambiguous (measurable and testable), traceable, complete, consistent, and stakeholder-approved requirements. Defining requirements helps ensure development of the required capability on-time and within budget.

Deliverables in this Phase include:

- Privacy Threshold Analysis (PTA)
- Privacy Impact Analysis (PIA)
- System of Records Notices (SORN)
- Electronic Information System Questionnaire for Records Management Scheduling
- System Requirements Specification (SRS)
- Concept of Operations
- Requirements Traceability Matrix
- Project Process Agreement (PPA)
- Project Management Plan
- Integrated Project Team Charter

The Requirements Gathering and Analysis Phase undergoes activities, reviews and approvals as identified in the below flowchart.

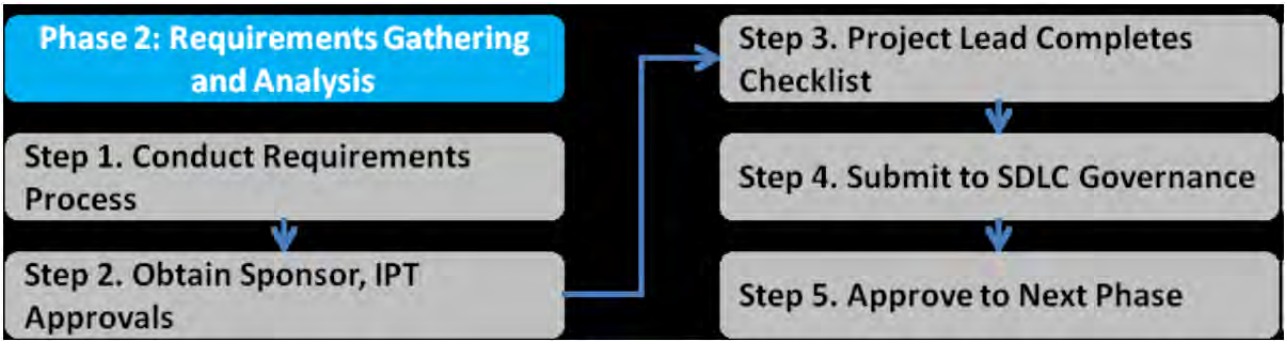

Figure 10 – SDLC Phase 2 Requirements Gathering and Analysis Overview

Upon successful completion of the "Approve to Next Phase" step, the project progresses to the Design Phase.

1545 Phase 3: Design

The purpose of the Design Phase is to transform requirements into complete and detailed system design specifications. The physical characteristics of the system are designed during this Phase, the operating environment is established, major subsystems and their inputs and outputs are defined, and processes are allocated to resources. The concept is further developed to describe how the business will operate once the approved project is implemented (i.e. becomes a "system"), and to assess impact on employee and customer privacy. Additionally, security authorization (formally known as certification and accreditation) activities begin with the identification of security requirements and the completion of a high level vulnerability assessment. Deliverables in this Phase include: • Procurement Documents (e.g. Statement of Work (SOW) / Performance Work Statement (PWS) / Statement of Objectives (SOO))

- System Design Document
- Configuration Management Plan
- Security Business Impact Assessment
- Security Contingency Plan
- Disaster Recovery Plan
- Domain Name Request

The Design Phase undergoes activities, reviews and approvals as identified in the below flowchart.

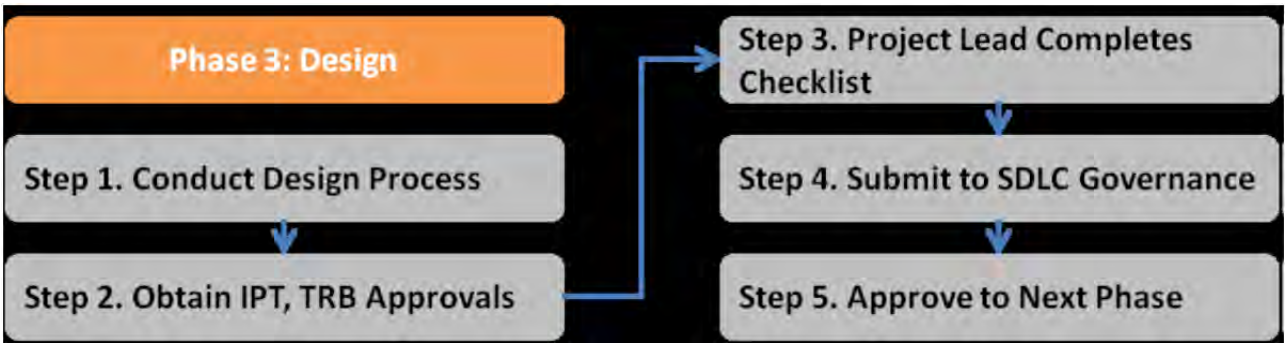

Figure 11 – SDLC Phase 3 Design Overview

Upon successful completion of the "Approve to Next Phase" step, the project progresses to the Development Phase.

1546 Phase 4: Development

The purpose of the Development Phase is to convert the system design prototyped in the Design Phase into a working system that addresses all documented system requirements. Further, everything requiring user input or approval must be documented in this Phase. Deliverables in this Phase include: • Test Plan

The Development Phase undergoes activities, reviews and approvals as identified in the below flowchart.

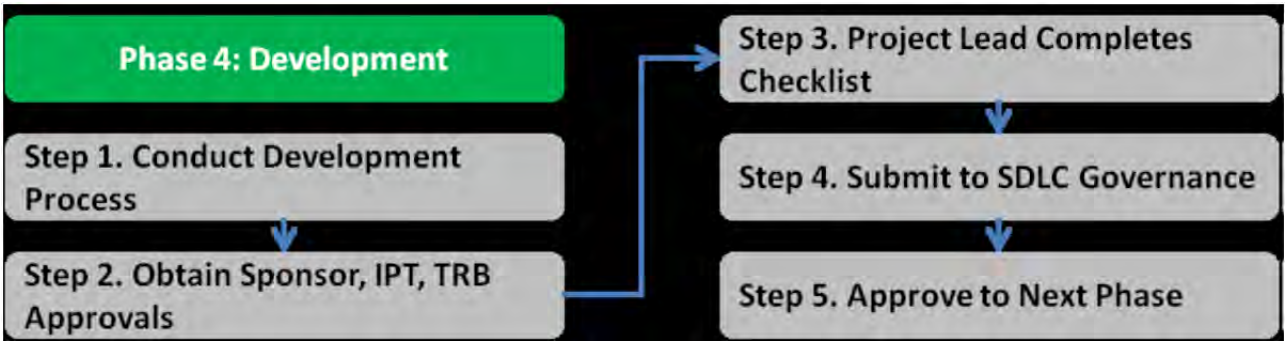

Figure 12 – SDLC Phase 4 Development Overview

Upon successful completion of the "Approve to Next Phase" step, the project progresses to the Integration & Testing Phase.

1547 Phase 5: Integration & Testing

The purpose of the Integration & Testing Phase is to lay the foundation for a smooth and successful implementation. Key activities in this Phase include: • Attaining user input or approval as defined in the prior Phase (Development)
- Preparing detailed logic specifications for each system module
- Testing and integrating units into larger components
- Preparing the technical environment for the system

This Phase focuses on achieving proof that the system meets all requirements, functions according to design parameters, and satisfies all business, technical, and management stakeholders. Additionally, prior to installing and operating the system in a production environment, the system must undergo security authorization activities, as necessary. Deliverables in this Phase include: • Transition Plan

- Operations/Maintenance Manual
- UAT sign-off
- App Scan Results
- Training Manual
- User Manual
- Test Results
- Section 508 VPAT and/or Certification
- Security Risk Assessment Report
- System Security Plan
- Security Assessment Plan (Security Test & Evaluation Plan)

The Integration & Testing Phase undergoes activities, reviews and approvals as identified in the below flowchart.

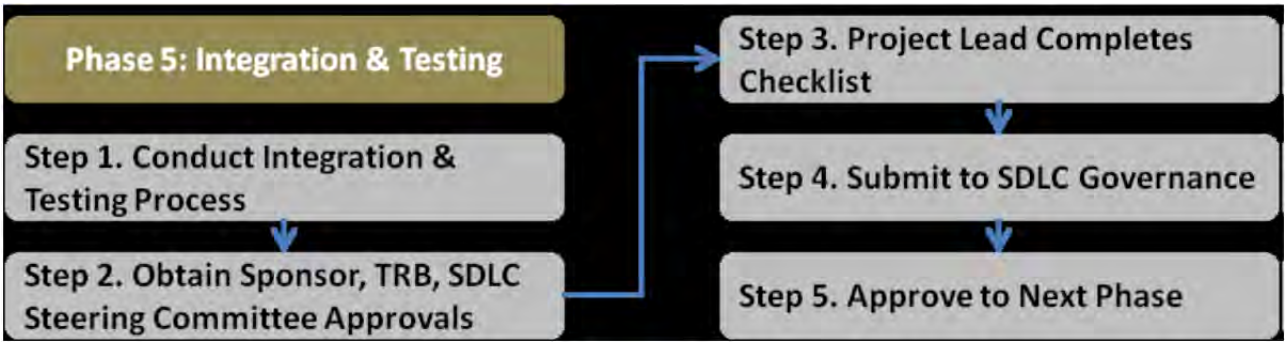

Figure 13 – SDLC Phase 5 Integration & Testing Overview

Upon successful completion of the “Approve to Next Phase” step, the project progresses to the Implementation Phase.

1548 Phase 6: Implementation

The purpose of the Implementation Phase is to deploy and enable operations of the new information system in the production environment. Successful completion of the Implementation Phase should comprise both system deployment and training on the system.

Deliverables in this Phase include:

- Installation Document
- Compliance Certification
- Operations Readiness
- Life Cycle Cost
- Project Closeout
- Performance Measures
- Authority to Operate/Concurrency Review
- Application Guide

- Source Code

The Implementation Phase undergoes activities, reviews and approvals as identified in the below flowchart.

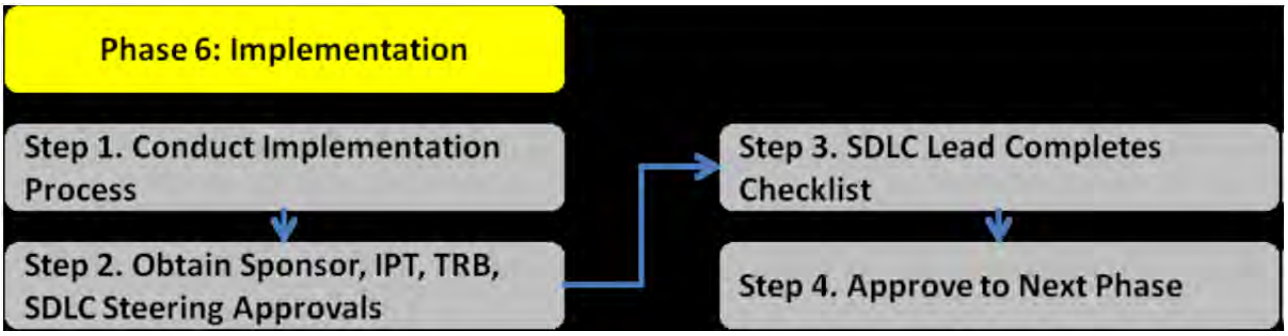

Figure 14 – SDLC Phase 6 Implementation Overview

Upon successful completion of the "Approve to Next Phase" step, the project progresses to the Operations / Maintenance (O&M) Phase.

1549 Phase 7: Operations / Maintenance (O&M)

The purpose of the Operations / Maintenance (O&M) Phase is to ensure the information system is fully functional and performs optimally until the system reaches its end of life. The system is monitored for continued performance in accordance with user requirements, and needed system modifications are incorporated. The operational system is periodically assessed through In-Process Reviews to determine how the system can be made more efficient and effective. Operations continue as long as the system can be effectively adapted to respond to an organization's needs. When modifications or changes are identified as necessary, the system may reenter the planning Phase.

Deliverables in this Phase include:

- System Post Implementation Review Report
- Operational Analysis
- Annual Updates Required:
- Systems Security Plan
- Contingency Plan
- Disaster Recovery Plan
- System Risk Management Plan
- Life Cycle Cost
- Authority to Operate (Every 3 Years)

The O&M Phase undergoes activities, reviews and approvals as identified in the below flowchart.

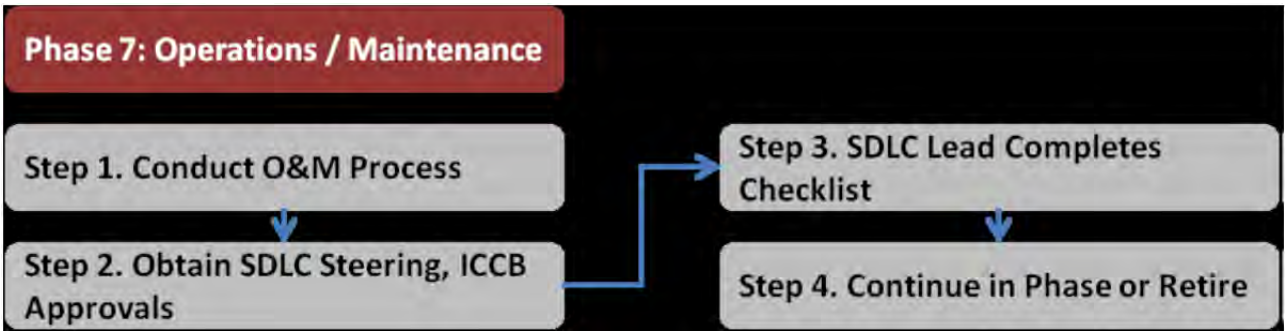

Figure 15 – SDLC Phase 7 Operations & Maintenance Overview

Upon advancement to the "Continue in Phase or Retire" step, the project is determined to continue operating or advance to the Disposition Phase.

1550 Phase 8: Disposition

The purpose of the Disposition Phase is to shut down the operational system in a controlled manner. The disposition activities allow for the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be retrieved in the future, if necessary. Particular emphasis is given to proper preservation of the data processed by the system, so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access.

Deliverables in this Phase include:

- System Disposition Plan
- System Disposition Checklist
- Post-Termination Review Report

The Disposition Phase undergoes activities, reviews and approvals as identified in the below flowchart.

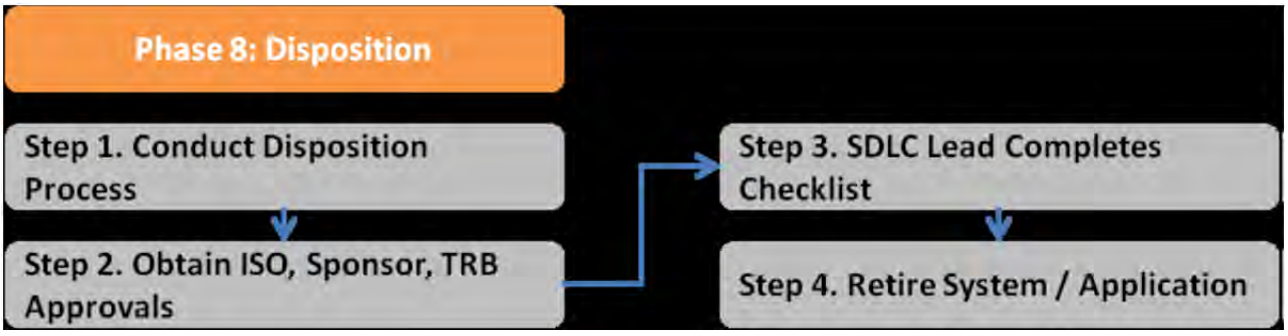

Figure 16 – SDLC Phase 8 Disposition Overview

Guidance on FNCS Capital Planning and Investment Control (CPIC)

1600 Overview

The Clinger-Cohen Act of 1996 requires that Federal agencies institute a disciplined approach to managing and controlling Information Technology (IT) investments. The Office of Management and Budget Circular A-130, "Management of Federal Information Resources" also mandates the disciplines of Capital Planning and Investment Control (CPIC) and information system security. These requirements, combined with the newly enacted Federal Information Security Management Act (FISMA), have now established a clear and convincing need for a systematic capital planning and investment process in FNCS.

CPIC is USDA's primary process for (1) making decisions about which initiatives and systems USDA should invest in and (2) creating and analyzing the associated rationale for these investments.

Through sound management of these investments, the USDA Executive Information Technology Investment Review Board (EITIRB) determines the IT direction for USDA, and ensures that FNCS manages IT investments with the objective of maximizing return and achieving business goals.

Currently, the IT Governance Branch coordinates all CPIC IT investments for the FNCS. The CPO reviews Agency IT investments based on their size, scope, or strategic impact on the Agency. The IT Governance Branch forwards the IT investments to OMB through the USDA Office of the Chief Information Officer for review and approval.

For further information and assistance on the FNCS CPIC process, please review section 1640 for the FNCS process flow of the CPIC process, by phase.

For the complete overview of the USDA CPIC Guidelines, please click on the following link: http://www.ocio.usda.gov/sites/default/files/docs/2012/DM3560-000.htm

1610 References

This Guidance is written in accordance with:

- NIST Special Publication 800-53 Rev.3
- NIST Special Publication 800-65
- USDA DM 3560-001, Security Requirements for CPIC
- FNCS Information Technology Investment Review Board Instructions
- IT Governance Branch Charter
- Appendix H – ITIRB/CPO Checklist
- Appendix I – ITIRB/CPO Recommendations

1620 Responsibilities

1621 The CISO will:

- Assist senior FNCS officials with IT issues.
- In coordination with the ISSPM, develop an overall Information Security Program for FNCS.

- Develop and maintain information system security procedures and control techniques.
- Designate an FNCS Information Systems Security Program Manager (ISSPM) who will perform the CIO directives as required by FISMA, including POA&M responsibilities.
- Design, implement and maintain processes for maximizing the value and managing the risks of IT acquisitions.
- Present proposed IT portfolios to the IT Investment Review Board (ITIRB).
- Provide final portfolio endorsements.
- Present and recommend control and evaluate decisions and recommendations.

1620 The ISSPM will:

- In conjunction with the System Owner create a preliminary security budget estimate, security analysis to determine estimated baseline costs e.g. resources.
- Provide training to all Information Security personnel.
- Assist senior agency officials with IT security-related responsibilities.

1621 The Technical Review Board (TRB) will:

- Conduct detailed IT investment reviews, security analyses and review business cases for the presence of security requirements.
- Balance IT investment portfolios based on the CIO/ITIRB security priorities and prioritization criteria.
- Recommend business case actions to the CIO; return to the originator for more information and forward to the ITIRB and/or refer to the OIT.
- Act as a focal point for agency coordination of the OCIO strategic planning, architectural standards and outreach to organizations and bureaus.

1622 The ITPM will:

- Develop a project management plan that integrates security throughout the SDLC.
- Develop a cost and schedule baseline; complete the project within schedule, under budget and to meet the needs of the customer.
- Coordinate the development, implementation, operation and maintenance of a system along with the System Owner, and others within FNCS.
- Report status of project to the System Owner, CPO and security personnel within FNCS.
- Provide baseline assessment performance measures to evaluate the security of the delivered IT initiative.
- Adhere to the established FNCS CPIC and project methodology.

- Provide feedback and lessons learned to the FNCS project management repository.
- Present, when applicable, the progress of critical systems to the CIO, ITIRB, CPO and security personnel within FNCS.

1623 The System Owner/ITPM will:

- In conjunction with the ISSPM create a preliminary budget estimate, security analysis to determine estimated baseline costs.
- In conjunction with the ISSPM and ITPM, create the SSP.
- Establish and maintain security costs.
- Review the security analyses for accuracy and update cost information based on actual acquisitions or additional items include since the select phase.
- Maintain a record of any security changes.
- Perform a Post Implementation Review (PIR) of the investment's security performance measures compared to the original performance goals.
- Identify initiative security risks and how they were managed or mitigated.
- Assess the continuing ability of the investment to meet the system's security performance goals.

1630 The Portfolio Manager will:

- Ensure that FNCS personnel adhere to CPIC procedures.
- Notify the OCIO CPIC staff of findings/documents.
- Update eCPIC and the Enterprise Architecture Repository (EAR) with CPIC related artifacts.
- Update the OMB Exhibit 300 and A-11 report with the appropriate security related information.
- Perform quarterly reviews.

1631 CPIC Phases

There are five (5) phases of the CPIC as defined by NIST SP 800-65, Integrating IT Security into the CPIC process and the USDA IT CPIC Guide.

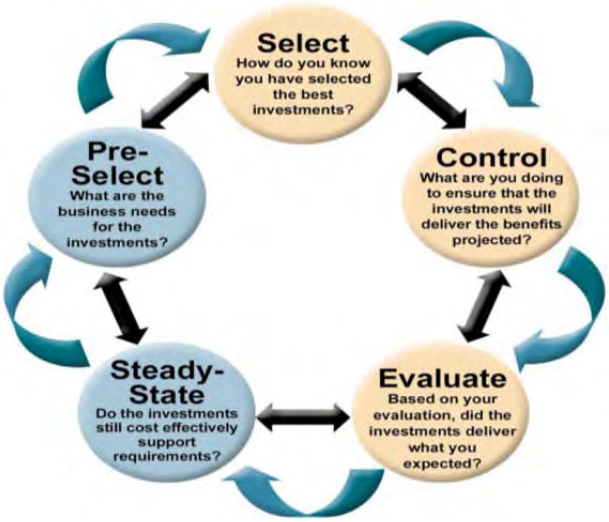

Figure 17 – USDA IT Capital Planning Phases

1632 Pre-Select Phase

The Pre-Select phase provides a process to assess a proposed investment's support of agency strategic and mission needs and to provide initial information to further support investments. It is during this phase that the business/mission need is identified and relationships to the Department and/or agency strategic planning efforts are established. There are significant information requirements and a potential expenditure of funds in the preliminary planning phase to prepare for review and selection of IT investments.

1633 Select Phase

In this phase, assess and prioritize proposed IT projects and then create a portfolio of IT projects. In doing so, this phase helps to ensure that the organization:

(1) Selects those IT projects that will best support mission needs and

(2) Identifies and analyzes a project's risks and returns before spending a significant amount of project funds.

A critical element of this phase is that a group of senior executives makes project selection and prioritization decisions based on a consistent set of decision criteria that compares costs, benefits, risks, and potential returns of the various IT projects.

1634 Control Phase

In this phase, we manage investments while monitoring the development process. Once the IT projects have been selected, senior executives periodically assess the progress of the projects against their projected cost, scheduled milestones, and expected mission benefits.

1635 Evaluate Phase

In this phase, there is a means for constantly improving the organization's IT investment process. The goal of this phase is to measure, analyze, and record results based on the data collected throughout each phase. Senior executives assess the degree to which each project has met its planned cost and schedule goals and has fulfilled its projected contribution to the organization's mission. The primary tool in this phase is the post-implementation review (PIR), which should be conducted once a project has been completed. PIRs help senior managers assess whether a project's proposed benefits were achieved and also help to refine the IT selection criteria to be used in the future.

1636 Steady State Phase

In this phase, there is a means to assess mature investments (fully implemented), ascertain their continued effectiveness in supporting mission requirement, evaluate the cost of continued maintenance support, assess technology opportunities and consider potential retirement or replacement of the investment. The primary review focus during this phase is on the mission support, cost and technological assessment. Process activities during the Steady-State phase provide the foundation to ensure mission alignment and support for system and technology succession management.

1637 CPIC Phases

CPIC PHASES AND PROCESSES	Pre-Select	Select	Control	Evaluation	Steady State
	• Identify project sponsor • Conduct mission analysis • Develop concept • Prepare preliminary business case • Prepare investment review submission package • Review / approve investment submission • Review initiative and recommend appropriate action • Make final	• Review the mission needs statement and update if needed • Approve integrated project team membership • Identify funding source(s) and obtain approvals. • Develop major investment supporting materials. • Prepare IT investment supporting materials • Review/Approve investment submission	• Establish and maintain initiative costs schedule and technical baselines • Maintain current initiative and security costs, schedule technical and general status information. • Assess initiative progress against performance measures using Earned Value Management Methodologies. • Prepare annual investment review submission package. • Review/approve investment submission.	• Conduct PIR and present results • Prepare annual investment review submission package • Review/approve investment submission • Review initiative's PIR results and recommend appropriate action • Make final investment decisions • Evaluate IT capital investment management	• Analyze mission • Assess user/customer satisfaction • Assess technology • Conduct O&M, e-Gov strategy and operational analysis (as necessary) • Prepare investment review submission package • Review/approve investment submission • Review initiative and recommend appropriate action • Make final investment

	investment decision	• Review initiative and recommend appropriate action. • Make final investment decisions.	• Review initiative and recommend appropriate action. • Make final investment decisions • Work with project sponsor to develop solutions.	process	decisions.

Table 13 – USDA IT Capital Planning Phases

1638 CPIC Phases and Security Requirements

1639 CPIC Required Documentation by Phase

This section outlines the needed documents required in each phase of the CPIC process.

- **Pre-Select Phase required documents list:**

  Preliminary Business Case

  Mission Analysis

  Other FNCS documentation requirements

  Mission Analysis Concept Document

  OMB Exhibit 300

- **Select Phase required documents list:**

  <u>Major Initiatives:</u>

  Business Case

  Performance Measures

  Functional Requirements

  Feasibility Study

  CPIC Risk Assessment/Mitigation Plan

  Update LC Cost Projections

  Alternatives Analysis

  Funding Source Identification

Technical Requirements

*System Security Plan

Telecommunications Plan

Enterprise Architecture Plan

e-Government Plan

System Dependencies

Project Plan

Telecommunication/Risk Mitigation Plan

Integrated Logistics Plan (if required)

Acquisition Plan and Strategy

IV&V Documentation (if required)

Section 508 Compliance Plan

Minor Initiatives:

*System Security Plan

Compliance with:

Telecommunications Standards

Enterprise Architecture

E-Government Requirements

Section 508 Requirements

*Please see Guidance on FNCS System Security Plans (SSP)

- **Control Phase required documents list:**
  - Costs
    - Overall Security Schedule
  - Baselines
    - Performance Measures
    - Risk Factors
  - Investment Summary
  - Assessments (Earned Value)
    - Cost vs. Baseline

        - Schedule vs. Baseline
    - Validation/Updates:
        - Cost-Benefits
        - Risk
        - Security
        - Telecommunications Architecture
        - Section 508
        - OMB Exhibit 300
    - System Documentation
    - System Test and Evaluation
    - Security Certification and Accreditation
    - Confirmed PIR Schedule

- **Evaluate Phase required documents list:**
    - Stakeholder Impact
    - Progress against Performance measures
    - Baseline goals evaluation
        - Cost
        - Return
        - Funding/Funding Sources
        - Schedule
        - Architecture
        - Accessibility
        - Telecommunications
        - Risk Management
        - Security Risk Mitigation
    - Lessons Learned

- **Steady State Phase required documents list:**
    - Annual Review/Update
    - Security Plan
    - Operational Analysis Report
        - Stakeholder Assessment
        - Cost/Schedule Performance
        - Risk Status Review
        - Alternatives Review
        - OMB Exhibit 300

1640 FNCS CPIC Process Flow Diagram (per Phase)

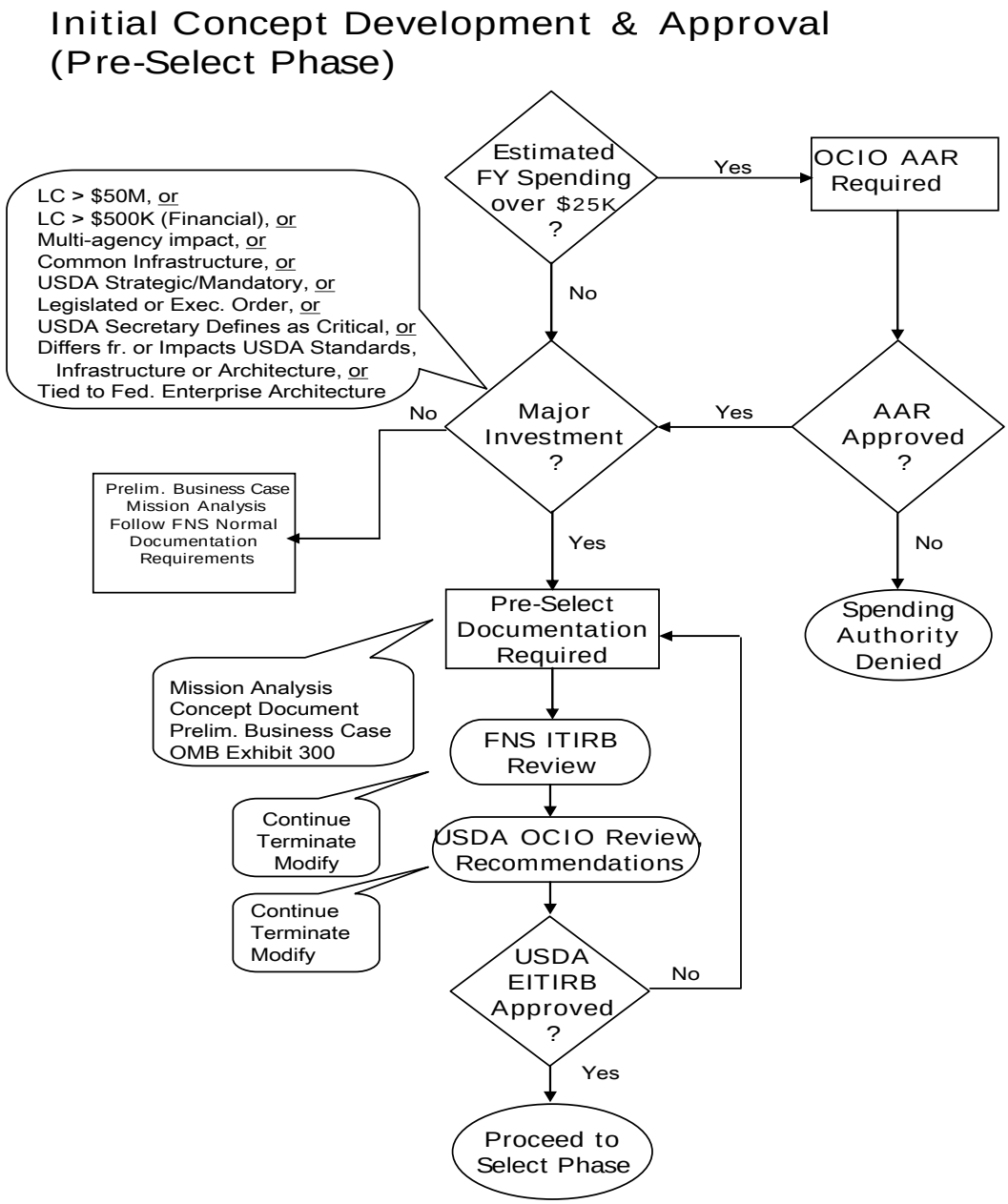

Figure 18 – FNCS CPIC Pre-Select Phase

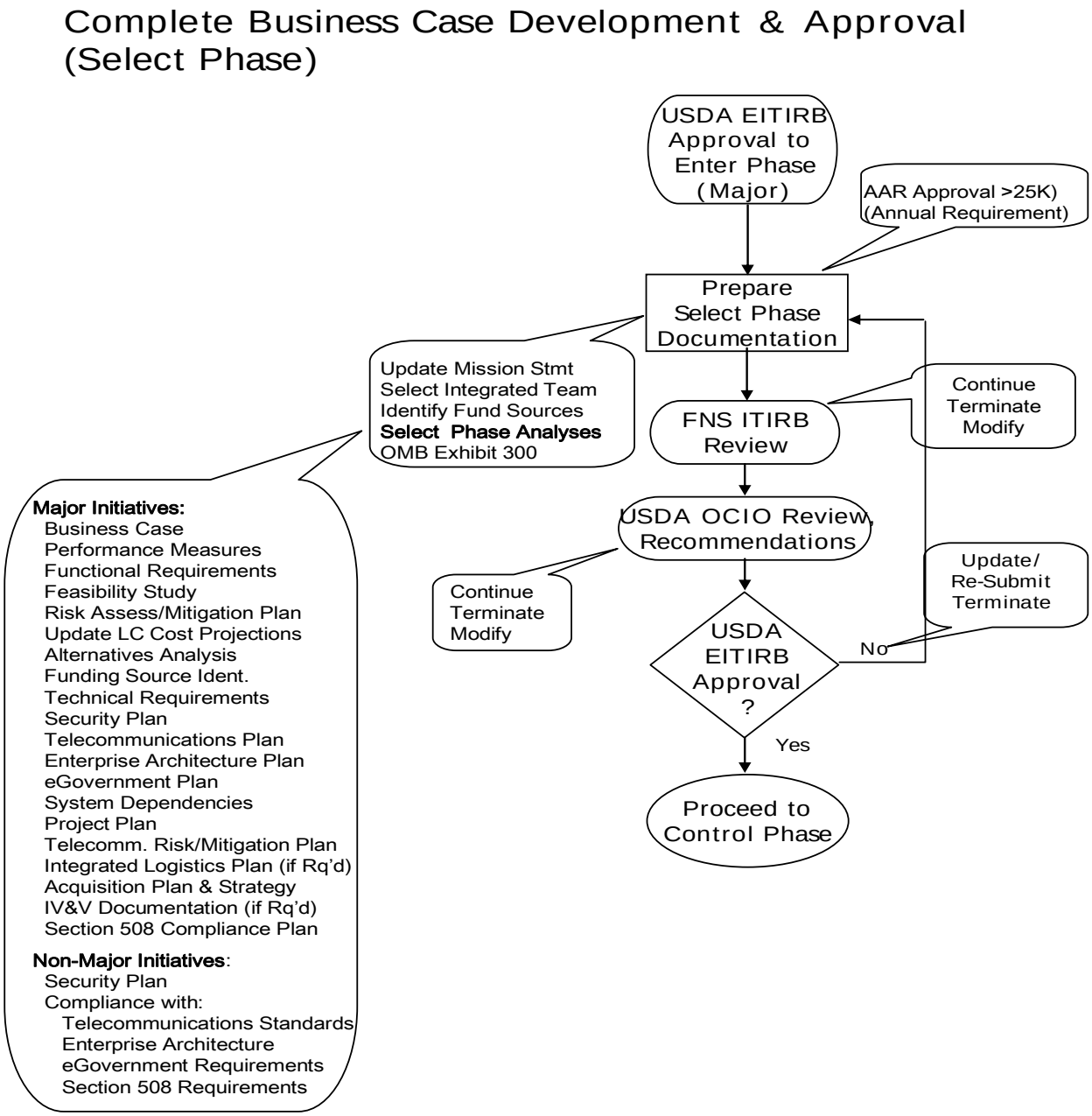

Figure 19 – FNCS CPIC Select Phase

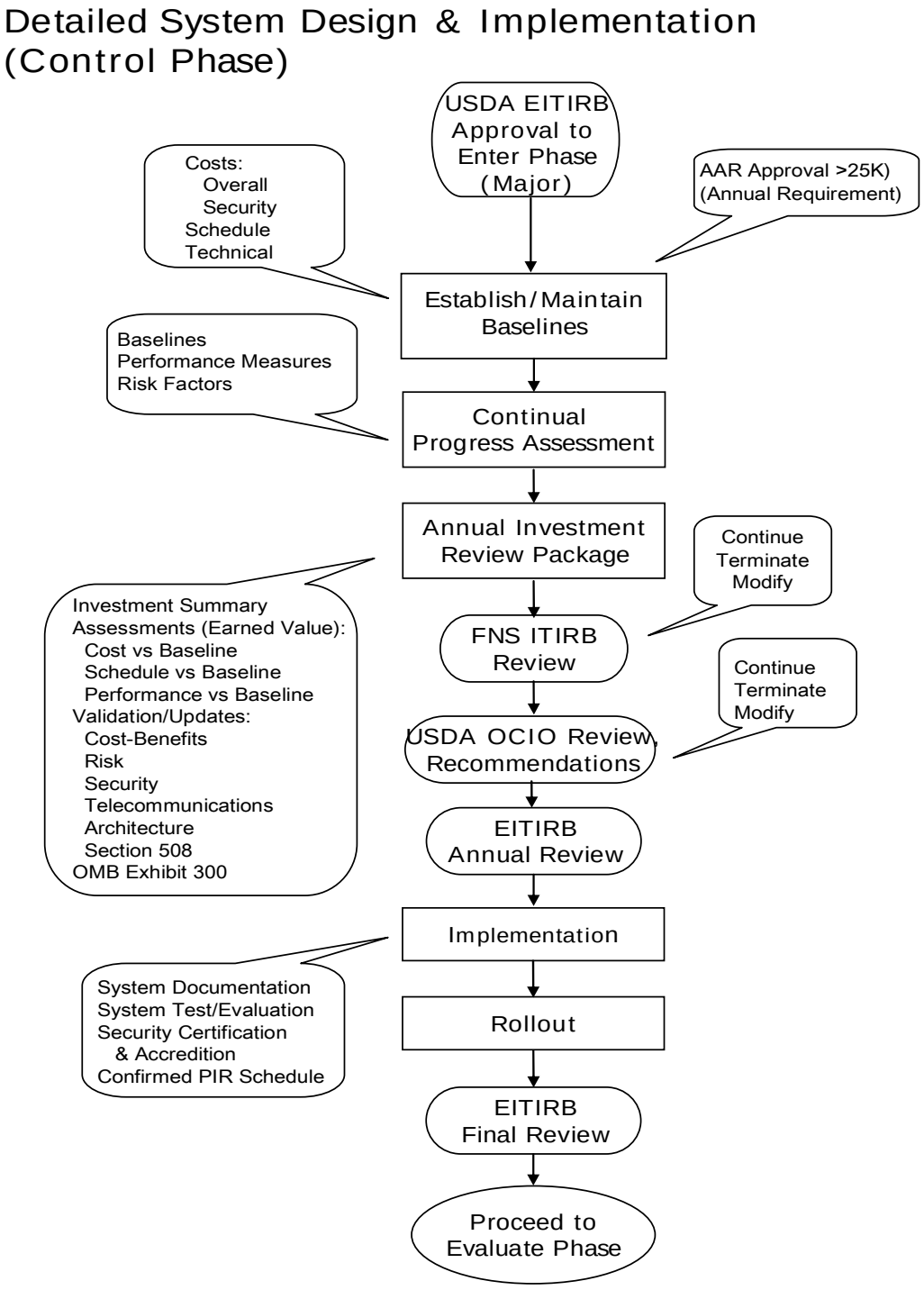

Figure 20 – FNCS CPIC Control Phase

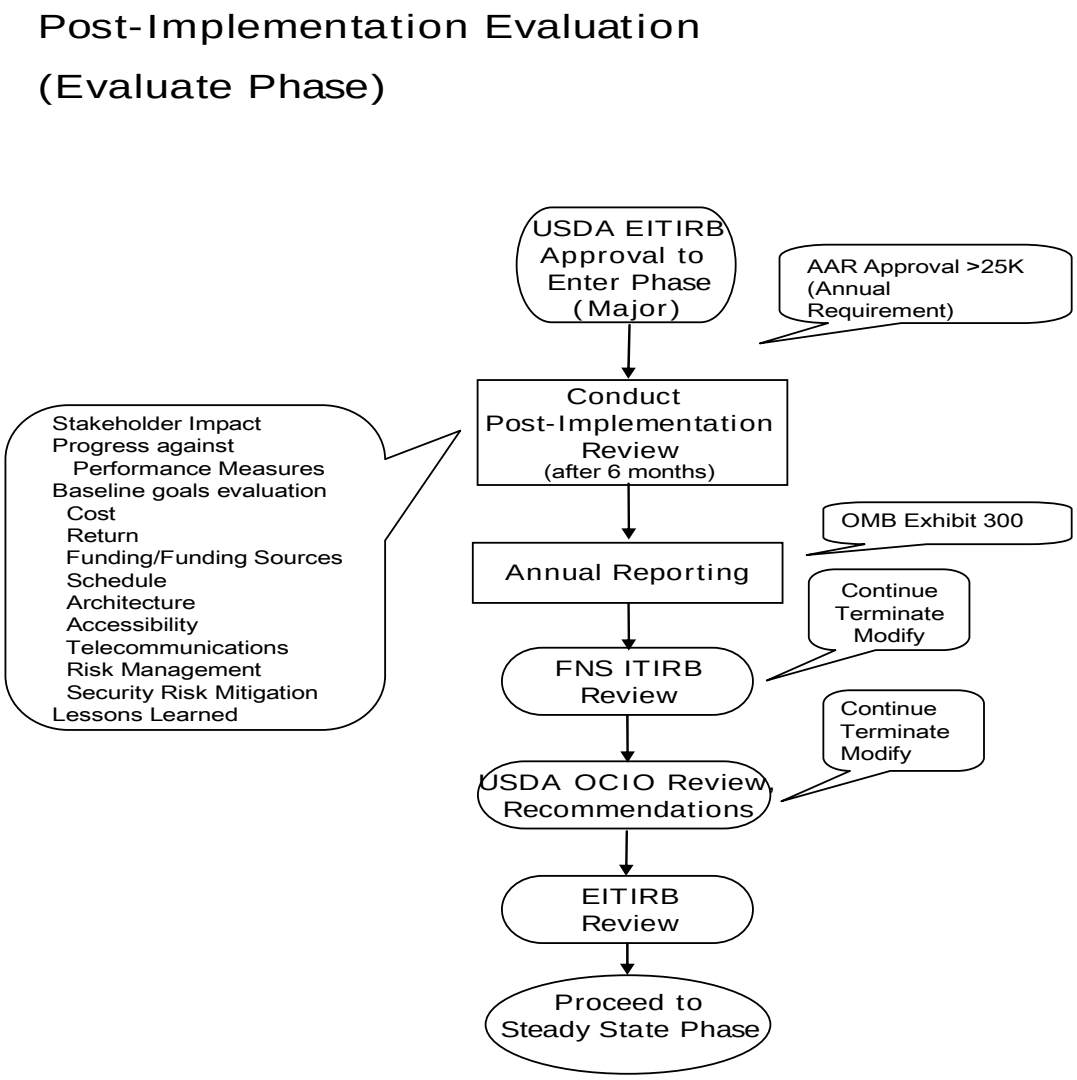

Figure 21 – FNCS CPIC Evaluate Phase

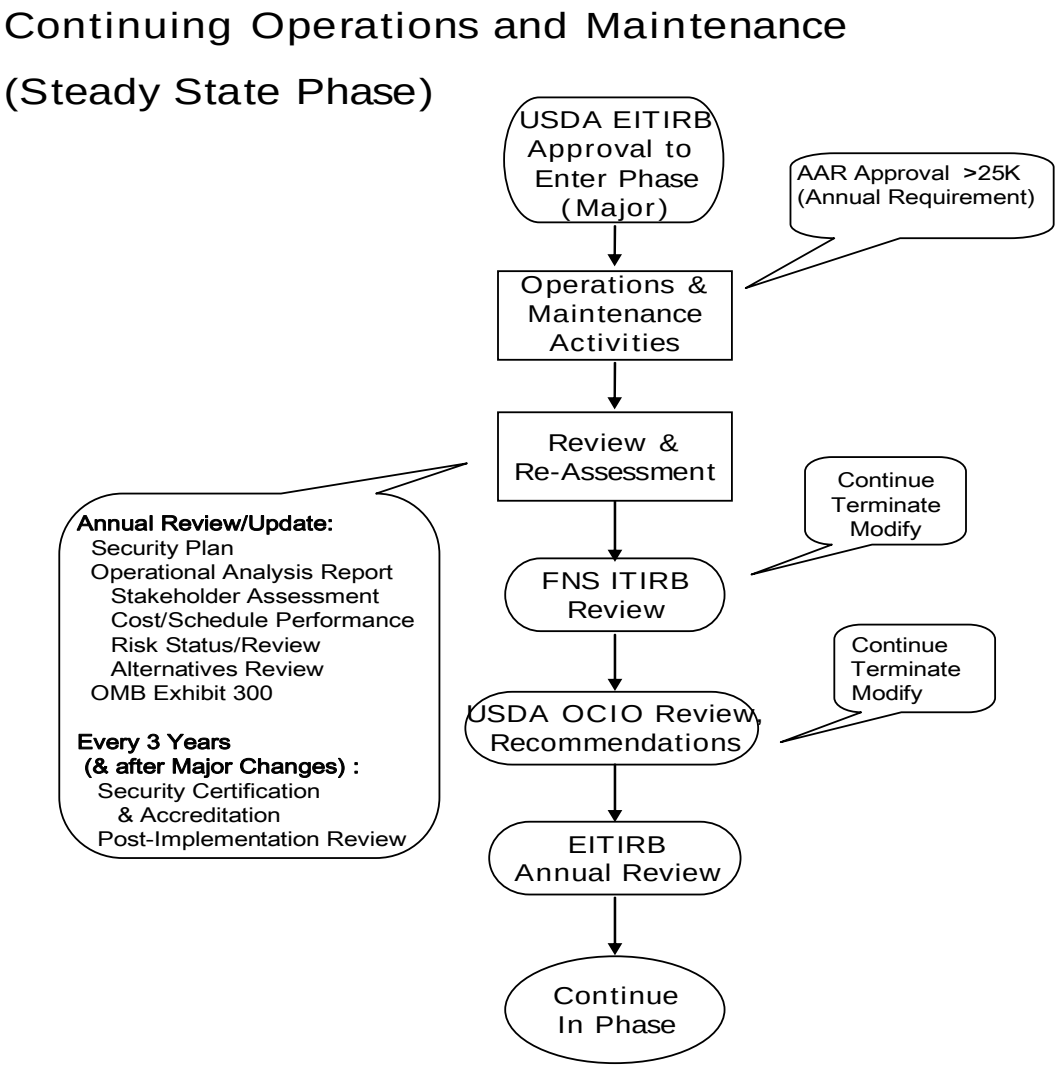

Figure 22 – FNCS CPIC Steady State Phase

Guidance on Maintenance of FNCS Information Systems

1641 Overview

NIST Special Publication 800-53 recommends that all Information Systems are maintained through a structured process. This process includes all steps necessary to perform scheduled maintenance, emergency repairs and routine maintenance onsite or remote to FNCS Information Systems.

This guidance includes processes that are involved in the maintenance of an information system, software and hardware. This guidance covers controlled maintenance, maintenance tools, remote maintenance, maintenance personnel and timely maintenance of information systems. The procedures are reviewed and updated at least annually.

1710 References

This Guidance is written in accordance with:

- NIST SP 800-53 Rev.3

1720 Responsibilities and Guidance

1721 The Network Operations and Engineering (NOEB) Branch will:

- Develop Standard Operating Procedures (SOPs) for performing maintenance on all Information Systems.

  Obtain and utilize appropriate automated tools to schedule and perform maintenance on Information Systems.

- Create logs of maintenance performed on all Information Systems and include:
  - Date and time of maintenance
  - Person (name) performing maintenance
  - FNCS personnel (name) escorting the repair person
  - Description of maintenance performed
  - List of equipment removed or replaced, if applicable. Including identification numbers.

- Assign authorized personnel (for local or remote maintenance) to perform the maintenance on Information Systems.
  - Assign authorized FNCS personnel to supervise maintenance personnel who do not have the appropriate authorizations.
  - Assign FNCS personnel to ensure all maintenance logs are kept current, complete and readily available for audits/assessments.

  - Ensure all use of maintenance tools are restricted to authorized personnel only.

- Approve all maintenance tools brought into the FNCS facility. Implement ongoing maintenance of the tools.

- Check all media containing diagnostic and test programs for malicious code prior to using on the Information System.

- Ensure all maintenance equipment that can retain information does not contain FNCS information on it. If information is retained on the equipment, properly sanitize it prior to leaving the FNCS facility.

- Monitor and control all remotely executed maintenance and diagnostic activities.

  - Ensure mechanisms are in place to audit remote maintenance sessions and provide all records to FNCS personnel for review.

  - Document the installation and use of remote maintenance and diagnostics links in the System Security Plan (SSP).

Guidance on Media Protection for FNCS Information System Resources

1800 Overview

NIST recommends that controls are in place to protect all FNCS media. Media includes both digital and non-digital, e.g. diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks (CD), digital video disks, paper and microfilm. Other examples of media include laptop computers, PDAs and cell phones. Media is also referred to as portable electronic devices (PED).

This document is written as a guide to ensure that media is protected through its life to include; access, labeling, storage, transport, sanitization, protection from theft and disposal.

This guidance applies to all FNCS Users, i.e. employees, contractors and official visitors who use government-furnished media for official FNCS business. This procedure is update and reviewed at least annually.

1810 References

This Guidance is written in accordance with:

- NIST SP 800-53 Rev.3
- Sensitive But Unclassified Guidance:

1820 Roles and Responsibilities

1821 The OIT Technology Division will:

- Provide and maintain Active Directory polices to restrict access to media storage areas.
- Provide a means to audit successful and unsuccessful logon attempts to FNCS media.
- Supply physical access controls as a means to protect information stored on media and ensure it is secured within a controlled area.
- Offer protection of media throughout its life until the media is destroyed or sanitized.
- Provide media that supports and enables encryption.
- Track any GFE that contains data and/or has the ability to store or transit data. This can included but not limited to laptops, printers, mobile devices, USB, tablets, and external drives.
- Sanitize media, through destruction, prior to disposal:
    - Track all sanitized media and include verification of sanitization and disposal methods used.
    - Test sanitization equipment to validate performance on an annual basis.
- Provide ability to audit selected removable FNCS information system media.

1822 Media Protection Guidelines

FNCS users who extract (print) output from SBU information systems are required to provide appropriate labels to clearly identify the output, its level of protection and to determine how it is used, handled and disseminated. When printing SBU information to a shared resource, retrieve all hard-copy printouts in a timely manner. If the originator of a printout cannot be determined, the printout must be shredded to protect against unwanted disclosure of SBU information.

FNCS users must exercise adequate precautions to ensure that FNCS Portable Electronic Devices (PEDs) are secure at all times. Precautions include, but are not limited to:

a. Encrypt the PED and any external media using a FNCS approved method.

b. Do not leave PEDs unattended in public places.

c. Always shut down, lock in a secured storage container and keep PEDs out of view.

d. Best practices are to never leave PEDs in vehicles. If you must, always conceal from view.

e. Report within one-hour if your PED is lost or stolen.

f. Connect PED (laptops) to the FNCS network every 30 days for a minimum of 60 minutes to ensure the device receives updates to virus definitions, operating systems and hot fixes.

Guidance on FNCS Personnel Information Security

1900 Overview

The greatest harm/disruption to a system may stem from the actions of individuals, both intentional and unintentional. Users, designers, implementers and managers are involved in many important issues in securing the information contained in FNCS Information Systems. Users of FNCS Information systems must adhere to the personnel requirements contained in this guidance.

1910 References

This guidance is written in accordance with:

- NIST SP 800-53 Rev. 3
- Background Investigation Request from FNCS

1920 Roles and Responsibilities

1921 The CIO will:

- Ensure all security access requirements are defined for each position.
- Ensure all personnel have undergone the appropriate background investigation.

1922 The ISO will:

- Develop, disseminate and periodically review/update personnel and information system security procedures and guidelines.
- Monitor the adherence to the personnel security guidance.
- Ensure all personnel are trained annually in computer security, privacy and specific security responsibilities that are applicable to their jobs.
- Promptly delete and/or request deletion of system access for application and/or systems when user terminates employment, suspects password has been compromised or no longer needs access.

1923 The Contracting Officer's Representative (COR) and ITPM will:

- Ensure all new contract personnel are aware of personnel security requirements prior to start of work at FNCS.
- Distribute the Background Investigation Request forms to all contract personnel.
- Approve the Background Investigation Request form and recommend the type of investigation that is needed.

1924 The Users will

- Understand their personnel security responsibilities and duties.

- Understand consequences as written in the Enforcement Statement if they do not comply with the Information Systems Security Procedures and Guidelines.
- Notify the ISO and Supervisor if misuse of data, security breach, violations of procedures or compromise of password occurs. Please refer to the Incident Reporting and Response guidance for additional instruction on reporting an incident.

1925 Personnel Security Guidelines

1926 Categorization of FNCS job positions

- FNCS assigns risk designations to all job positions.
- Risk designations are compliant with 5 CFR 731.106(a) and Office of Personnel Management (OPM) policy and guidance.
- FNCS establishes screening criteria for individuals filling all positions.
- FNCS reviews/updates job position risk designations any time description/duties/responsibilities of the position are significantly changed.

1927 Personnel Screening

FNCS screens personnel who require access to FNCS information and information systems by requiring a specified level of background investigation and the completion/approval of the User Access Request Form, FNS-674.

1928 Personnel Termination

- Upon voluntary termination of employment for FNCS personnel, the user must complete and have approved the Final Salary Report, form FNS-677.
- Contract personnel who voluntarily terminate employment will contact their COR and request the *Government Contractor's Employee Separation Checklist (GCESC)*.
    - The GCESC is also available for download from the E-forms, it can be found at: http://fncs/ondemand/elibrary/EForms/FNS-774.pdf
    - The GCESC must be completed with all applicable signatures on the last day of employment for the contract personnel.
- FNCS immediately terminates or submits requests to terminate system access following receipt of the FNS-677 or GCESC forms.
- FNS ensures that when employees and contractors are terminated the user access to the FNS information the information system is disabled not then 24 to 48 hours
- Supervisors are required to notify OIT of terminations. OIT can then begin the process of removing systems' accesses.
- Notification can consist of calling the Help Desk or E-mailing the Security Offices Mailbox.

1929 Personnel Transfer

- FNCS personnel who are transferred or reassigned to a new location within FNCS will complete the FNS-674 to request access to new systems and/or file shares.
- Supervisors must notify OIT of personnel transfers as soon as possible.
- FNCS personnel who are transferred or reassigned to a new position within FNCS will have all system accesses re-assessed based on the location and job type/categorization. The completion of the FNS-674 is needed to approve this request.

1930 Access Agreements

- FNCS requires the completion and approval of the FNCS User Access Request form, FNS-674 prior to providing access to FNCS Information Systems.
- FNCS ensures access agreements are reviewed and if necessary updated annually.
- FNCS requires through signature, an acknowledgement that the FNCS User understands and complies with network rules of behavior.
- The Rules of Behavior, distributed to each user prior to obtaining access to the FNCS Network, contains sanctions for personnel who fail to comply with information system security policies and procedures.

1931 Third-Party Personnel Security

All vendors and contractors that perform official FNCS business outside of FNCS facilities are given FNCS Information Systems Security policies/procedures within acquisition related documents and are required to adhere to them.

Appendix A – Glossary

Terms	Definitions
ACCESS	Interaction between a subject (person, process, or input device), and an object, (Information Technology resources e.g., a record file, program, or output device) that results in the flow of information from one to another. Also, the ability to obtain knowledge of information stored on the system.
ACCESS CONTROL	Measures imposed to limit to the exposure of Information Technology resources to only authorized users, programs, processes or other systems.
ACCESS POINT	An access point is the entry point from a wireless station to a Wireless Local Area Network (WLAN) or Wireless Wide Area Network (WWAN), from a WLAN or WWAN to a wired Local Area Network (LAN), between WLANs, WLANs and WWANs, or between WWANS. Access points generally consist of a radio, a wired network interface, and management and bridging software. Access point functionality can be implemented using a hardware device or an application installed in another network device (a router for example) and is configured based on architecture requirements. Some vendors have removed the management and bridging software from the access point and placed these features into a wireless switch. In a WLAN system with wireless switches, the access points are usually called access ports and are essentially transceivers (transmitter/receiver of data) with a network interface. Software applications are available that can be used to turn a laptop computer acting as a wireless station (wireless client) into an access point.
ACCREDITATION	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
ACL **ACCESS CONTROL LIST**	In computer security, an access control list (ACL) is a list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object. In a typical ACL, each entry in the list specifies a subject and an operation: for example, the entry (Alice, delete) on the ACL for file XYZ gives Alice permission to delete file XYZ.
AES - ADVANCED ENCRYPTION STANDARD	In cryptography, the Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It has been

Terms	Definitions
	analyzed extensively and is now used widely worldwide [2] as was the case with its predecessor, the Data Encryption Standard (DES). AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) in November 26, 2001 after a 5-year standardization process (see Advanced Encryption Standard process for more details). It became effective as a standard May 26, 2002. As of 2006, AES is one of the most popular algorithms used in symmetric key cryptography.
AIR CARD (aka) PC Card or Personal Computer Memory Card International Association (PMCIA)	PCMC Personal Computer Memory Card International Association card, also called a PC Card or Air Card®. A PCMCIA card may fit into an open slot in a mobile computing device, or may need to be installed. It can be equipped with a variety of features including modem and network interface capabilities, and may act as a radio transceiver. PCMCIA cards are often configured to work with specific wireless carriers, but may support more than one.
APPLICATION SYSTEM	An automated process or collection of processes, with the supporting hardware, operating systems and communication links that supports a business need.
AUDIT TRAIL	A chronological record of system activities sufficient to enable the reconstruction, review, and examination of the sequence of events and activities surrounding or leading to a given operation, procedure, or event in a transaction
AUTHENTICATION	The means of establishing the validity of a claim to authorized status. Three means of authenticating a user's identity can be used alone or in combination. Something the individual knows (secret password, Personal Identification Number (PIN), or cryptographic key); Something the individual possesses (token, an ATM card or a smart card); Something that belongs uniquely to or is part of the individual (a biometrics such as a voice pattern, handwriting dynamic, or fingerprint).
AVAILABILITY	The fractional amount of time that a system provides the services and meets the mission requirements for which it is designed and operated.
BACKGROUND INVESTIGATION	Review into a person's past in the determination of granting a security clearance.

Terms	Definitions
BIOMETRICS	Biometrics (ancient Greek: bios =”life”, metron =”measure”) is the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In information technology, biometric authentication refers to technologies that measure and analyzes human physical and behavioral characteristics for authentication purposes. Examples of physical (or physiological or biometric) characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while examples of mostly behavioral characteristics include signature, gait and typing patterns. All behavioral biometric characteristics have a physiological component, and, to a lesser degree, physical biometric characteristics have a behavioral element.
BLUETOOTH	Bluetooth® enabled electronic devices connect and communicate wirelessly via short-range (100m or less) in ad hoc networks called piconets. IEEE 802.15 Wireless Personal Area Networks (WPANs) formalized the specification. The Bluetooth® standard is a computing and telecommunications industry specification that describes how mobile phones, computers, and PDAs should interconnect with each other, with home and business phones, and with computers using short-range connections. Bluetooth® does not address audit and non-repudiation security services. Since Bluetooth® devices do not register when they join a network; they are invisible to network administrators. Consequently, it is difficult for administrators to apply traditional physical security measures.
CAPITAL PLANNING AND INVESTMENT CONTROL (CPIC)	A process resulting from the Clinger-Cohen Act (Information Technology Management Reform Act of (CPIC) 1996), which directs the head of each agency to design and implement a process to maximize the value and manage risks, associated with information technology (IT) investments. The primary objective of CPIC is for senior managers to systematically maximize the benefits of IT investments using a five phased management process established by the Office of Management and Budget and the General Accounting Office. • Pre-Select Phase: Initial concept and definition of business needs and the system’s scope and functionality • Select Phase: Concise quantification of the system’s design, project schedule, benefits, budget, and

Terms	Definitions
	performance standards • Control Phase: The design, development, and implementation of the system • Evaluate Phase: A review and analysis process that takes place after an IT investment is operational to determine whether the investment meets expectations. • Steady State Phase: The ongoing operation, maintenance, and monitoring of the investment against its planned schedules, budgets, and performance measures.
CERTIFICATION	The technical evaluation that establishes the compliance of a computer system, application, or network design and implementation with prescribed security requirements.
CERTIFICATION AUTHORITY	The official responsible for reporting the comprehensive evaluation of the technical and non-technical security features of the FNCS system and other safeguards made in support of the accreditation process to establish the extent to which the system design and implementation satisfies the FNCS Security Guidance and other cognizant security requirements.
CLASSIFICATION	Designation of the sensitivity level of an entity (i.e. sensitive, unclassified).
CLEARANCE VERIFICATION	The act of ensuring that a user has the proper security clearance authorizations prior to granting access to a facility or Information Technology system.
COLD SITE	A facility designated for emergency backup operations of another system but not in operation until staffed and uploaded for that task.
CONFIDENTIALITY	The physical and electronic condition that protects information and data from unauthorized disclosure.
CONFIGURATION MANAGEMENT (CM)	Oversight activities for changes and enhancements to the FNCS system's hardware, firmware, software, and documentation to ensure that unintentional modifications do not occur.
CONTINGENCY PLAN	A plan detailing emergency response, backup operations, and post-disaster recovery steps for an information technology system or program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. FNCS OIT refers to its CP as the ITCP IT Contingency Plan.
CONTINUITY OF OPERATIONS PLAN (COOP)	A plan developed to support the organization in case of a protracted infrastructure problem when relocation is

Terms	Definitions
	necessary. A COOP specifies the actions necessary to accomplish a smooth transition to an alternate site and resumption of business operation. A COOP consists of two components: • Disaster Recovery Plan – A plan that estimates how long a system can be down before adversely affecting the core business operation, the value of assets that will be affected, emergency support personnel required, and the availability of software, hardware and telecommunication facilities needed to support the system. • Business Resumption Plan – A plan developed for the re-establishment of business processes when the primary location for the business has been destroyed or rendered unavailable for an extended period of time. It typically covers relocating to a facility, business equipment requirements, local area network support, and all elements necessary to resume business functions for mission critical business processes.
CONTROLLED AREAS	The areas within the FNCS facility where access is monitored and restricted to authorized personnel.
COMMERCIAL OFF-THE-SHELF (COTS) SYSTEMS	Software acquired by government contract through a commercial vendor. The software is a standard product, not developed for a particular government project.
COMMERCIAL WIRELESS	Devices, Services and Technologies commercially procured and intended for use in commercial and unlicensed frequency bands, e.g., Starbucks, airports.
COMPROMISE	The disclosure of information to persons who are not authorized access thereto.
COMPUTER VIRUS	A program designed to infect system software or application programs in much the same way as a biological virus infects humans. The typical virus reproduces by making copies of itself when inserted into other programs.
DATA	A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by humans or by Information Technology resources.
DATA INTEGRITY	The attribute of data relating to the preservation of (1) its meaning and completeness, (2) the consistency of its representation(s) and (3) its correspondence to what it represents.

Terms	Definitions
DMZ – DEMILITARIZED ZONE	A part of the network that is neither part of the internal network nor directly part of the Internet. Basically a network sitting between two networks.
DECRYPT	To convert, by use of the appropriate key, encrypted (encoded or enciphered) text into its equivalent plain text.
DENIAL OF SERVICE (DoS)	Action or actions that deteriorate all or part of the ability of an Information Technology infrastructure to perform its designated mission.
DEPUTY REGIONAL INFORMATION SYSTEMS SECURITY OFFICER (DRISSO)	An individual appointed for each region within the organization. The DRISSO acts on behalf of the Information Systems Security Office to ensure compliance with the information systems security procedures developed for the local environment.
DIAL-BACK	A procedure used by some remote access software or hardware that receives a connection and authenticates the user, then hangs up the connection and dials a predetermined number in order to establish a communications session with the user.
DIGITAL SIGNATURES	A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.
DISASTER	An event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm.
EMERGENCY/INCIDENT RESPONSE	The prompt and effective reaction to disruptions in normal processing activities through preplanned, measured steps.
EMPLOYEE PERSONAL TIME	Non-Work Hours. Employees may use government furnished equipment during their own off-duty hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if their duty station is normally available at such times).
ENCRYPTION	The process of transforming data into a format that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process.

Terms	Definitions
ENCRYPTION ALGORITHM	A set of mathematically expressed rules through which transmitted information is rendered unintelligible. Cryptography affects a series of transformations through the application of variable elements, controlled by use of a cryptographic key, to the normal representation of the information.
EXTERNAL NETWORK	Any network outside of the control of the FNCS IT infrastructure staff. Examples are the Internet, the Public Telephone System (PTS), Value Added Networks (VANs), vendor networks, other Agency/Department networks, etc.
FIRMWARE	Logic circuits in read-only memory that can be altered by software under certain circumstances.
FIREWALL	A firewall is a device that guards the entrance to a private network and keeps out unauthorized or unwanted traffic.
GATEWAY	The interface between electronic mail environments to facilitate the exchange of messages and attachments despite the size and type of message content.
GENERAL SUPPORT SYSTEM (GSS)	An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).
GOVERNMENT OFF-THE-SHELF	Software developed by the government. This software is a standard product, not developed for a particular government project.
GFE – GOVERNMENT-FURNISHED EQUIPMENT	Any government issued equipment, issued by FNCS or USDA.
HOT FIX	A hot fix is code (sometimes called a patch) that fixes a bug in a product. Users of the products may be notified by e-mail or obtain information about current hot fixes at a software vendor's Web site and download the hot fixes they wish to apply. Hot fixes are sometimes packaged as a set of fixes called a combined hot fix or a service pack.
HOT SITE	A processing facility already equipped with processing capability and fully operational.
HUB	A common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub

Terms	Definitions
	contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
IDENTIFICATION	The means by which a user provides a claimed identity to the system.
INCIDENT	Event that has an actual or potential effect on an Information System.
INFORMATION SECURITY OFFICE (ISO)	The focal point for all organizational information systems security concerns and who ensures that the program requirements described in the FNCS security Guidance statements are implemented.
INFORMATION TECHNOLOGY INFRASTRUCTURE	The equipment used in the acquisition, processing, storage, and dissemination of information in all its forms (auditory, pictorial, textual, and numerical) through a combination of computers, telecommunications networks, networks (LAN's/WAN's consisting of switches, router, hubs, etc.), and electronic devices.
INTEGRITY	The quality of data that ensures the continuity of its format, content, and veracity.
INTERNET	The collection of worldwide "network of networks" that use the TCP/IP protocol suite for communications.
INTERCONNECTION SERVICE AGREEMENT (ISA)	An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.
INTRANET	A network internal to the organization that is based on TCP/IP protocols.
MEMORANDUM OF UNDERSTANDING/AGREEMENT (MOU/MOA)	A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.
MISSION CRITICAL SYSTEM	Systems that are essential to the execution of FNCS business functions. There would be major financial losses, as well as losses to the creditability of FNCS if these systems fail or become inoperable for any period of time.
NEED-TO-KNOW	A determination made by the owner or controller of certain information that a prospective recipient of the information has a valid requirement for access to, knowledge of, or possession of the information.

Terms	Definitions
NETWORK	A communication medium including all components connected to that medium (computers, routers, controllers, packet switches, etc.) used for the transference of information.
NETWORK ACCESS CONTROL MECHANISM	Hardware or software responsible for restricting access to network hosts. Examples are firewalls, secure application gateways, secure dial-up devices, Virtual Private Networking, etc.
NAT – NETWORK ADDRESS TRANSLATION	NAT (Network Address Translation or Network Address Translator) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and un maps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world. NAT is included as part of a router and is often part of a corporate firewall. Network administrators create a NAT table that does the global-to-local and local-to-global IP address mapping. NAT can also be used in conjunction with *Guidance routing*.
NETWORK MAPPING TOOL	An example of a Network Mapping Tool is Network Analyzer. It is a hardware or software device that monitors and analyses data traveling over a network. Network Analyzer offers various network troubleshooting features, including protocol-specific packet decodes, specific preprogrammed troubleshooting tests, packet filtering, and packet transmission.
NIC - NETWORK INTERFACE CONTROLLER(CARD)	A network card, network adapter or NIC (network interface controller) is a piece of computer hardware designed to allow computers to communicate over a computer network. It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.

Terms	Definitions
PACKET SNIFFERS	A packet sniffer (also known as a network analyzer or protocol analyzer or, for particular types of networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams travel back and forth over the network, the sniffer captures each packet and eventually decodes and analyzes its content according to the appropriate RFC or other specifications.
PASSWORD CRACKING	Password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password. The purpose of password cracking might be to help a user recover a forgotten password (though installing an entirely new password is less of a security risk, but involves system administration privileges), to gain unauthorized access to a system, or as a preventive measure by system administrators to check for easily crack-able passwords.
PATCH	A patch (sometimes called a “fix”) is a quick-repair job for a piece of programming. During a software product’s beta test distribution or try-out period and later after the product is formally released, problems (called bug) will almost invariably be found. A patch is the immediate solution that is provided to users; it can sometimes be downloaded from the software maker’s Web site. The patch is not necessarily the best solution for the problem and the product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a *binary file* or object module). In larger operating systems, a special program is provided to manage and keep track of the installation of patches.
PED – PORTABLE ELECTRONIC DEVICES	A PED is any electronic device that is capable of receiving, storing or transmitting information using any format (i.e., radio, infrared, network or similar connections) without a permanent link to Federal networks. Handheld devices such as PDAs and cell phones allow remote user to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing and Internet Access. Generally, PEDs include but are not limited to: cell phones, pagers, text messaging devices (Blackberries), hand scanners, PDAs, voice recorders and flash memory.

Terms	Definitions
PEER-TO-PEER	WLANs may be configured into a peer-to-peer (also known as ad hoc or independent) network that permits devices to communicate directly. Peer-to-peer WLAN communications can bypass required encryption and authentication mechanisms, making transmissions vulnerable to interception and unauthorized access from outsiders. Peer-to-peer voice communications are an exception to this Guidance.
PERFORMANCE MEASUREMENT	The use of measures for monitoring and assessing progress toward an effective Information Systems Security Program.
PDA – PERSONAL DIGITAL ASSISTANT/SMART PHONE	Personal digital assistants (PDAs) are handheld computers that were originally designed as personal organizers, but became much more versatile over the years. PDAs are also known as pocket computers or palmtop computers. PDAs have many uses: calculation, use as a clock and calendar, playing computer games, accessing the Internet, sending and receiving E-mails, video recording, typewriting and word processing, use as an address book, making and writing on spreadsheets, use as a radio or stereo, and Global Positioning System (GPS). Newer PDAs also have both color screens and audio capabilities, enabling them to be used as mobile phones (smart phones), web browsers, or portable media players. Many PDAs can access the Internet, intranets or extranets via Wi-Fi, or Wireless Wide-Area Networks (WWANs). One of the most significant PDA characteristic is the presence of a touch screen.
Personal Electronic Equipment	An electronic device that emits an audible or visual signal, displays a message, or otherwise summons the possessor, including, but not limited to, cellular telephones, tablets, paging devices, electronic e-mailing devices, radios, tape players, CD players, DVD players, video cameras, iPods or other MP3 players, portable video game players, laptop computers, personal digital assistants (PDA's), cameras, and any device that provides a wireless connection to the Internet.
PHYSICAL SECURITY	The physical application of barriers and control procedures as preventive measures or countermeasures against threats to IT resources, and sensitive information.
PERSONALLY IDENTIFIABLE INFORMATION (PII)	Any piece of information which can potentially be used to uniquely identify, contact, or locate a single person.
PICONET	A piconet is established when two or more portable devices make a wireless connection. When a piconet is

Terms	Definitions
	formed, one device controls one or more other devices for the duration of the communication session. A piconet is sometimes called a Personal Area Network (PAN).
POA&M – PLAN OF ACTION AND MILESTONES	A plan of action and milestones (POA&M) is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of this POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.
POE – PERSONALLY-OWNED EQUIPMENT	This is equipment that is not owned by FNCS or the Federal Government. Please see Network Access Guidance for restrictions on POEs.
PORT SCANNER	A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by crackers to compromise it.
PRIVACY	The concept that a user's data, such as stored files and e-mail, is not to be examined by anyone else without that user's permission.
PROXY SERVER	In computer networks, a proxy server is a server (a computer system or an application program) which services the requests of its clients by making requests to other servers. A client connects to the proxy server, requesting a file, connection, web page, or other resource available from a different server. A proxy server provides the resource by connecting to the specified server, with some exceptions: A proxy server may alter the client's request or the server's response. A proxy server may service the request without contacting the specified server.
QUALITATIVE RISK ASSESSMENT	A methodology used to assess risk based on descriptions and rankings.
QUANTITATIVE RISK ASSESSMENT	A methodology used to assess risk based on computational means.
REMOTE ACCESS	The interface by a user operating on a device at a location outside the internal environment of a specified internal IT network structure into that structure.

Terms	Definitions
Removable Media	Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer. This includes but is not limited to flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks.
REMOVABLE STORAGE MEDIA	USB/Flash drive, External hard drive, CD and DVD, Floppy Disks and Back-up Tapes
RISK	A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact.
RISK ASSESSMENT	The process of identifying, validating and analyzing the existing threats and vulnerabilities of an information system, and the potential impact that the realization of any of those risks would have on the delivery of agency service. The resulting analysis is then used as a basis for identifying appropriate and cost-effective measures to mitigate the risk. Risk analysis is the part of risk management that evaluates specific security measures and their commensurability with the value of the resources to be protected, the vulnerabilities of those resources, and the identified the identified threats against them.
RISK MANAGEMENT	Process concerned with the identification, measurement, safeguard, and control of security risks in the FNCS system.
RISK MITIGATION	The selection and implementation of security controls to reduce risk to a level acceptable to management.
ROUTER	A device or setup that finds the best route between any two networks, even if there are several networks to traverse. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create WANs.
SECURITY	Measures, safeguards and controls that ensure confidentiality, integrity, availability, and accountability of information transmitted, processed, and stored on FNCS IT systems.
SECURITY CLEARANCE	A level of assurance that an individual is trustworthy and reliable, so that he or she can have access to agency IT systems.
SECURITY CERTIFICATION	A formal testing of the security safeguards implemented in

Terms	Definitions
	and about the computer system to determine whether it meets applicable requirements and specifications.
SECURITY DOCUMENTATION	The technical records used and maintained throughout the information system's life cycle and the written guidance for users of the system's software applications and hardware. Technical documentation includes system and design specifications; management plans, architectural prototype, and detail design documents; test specifications and reports, and engineering change requests and results. User documentation includes customer reference and usage information.
SECURITY MANAGEMENT	Supporting services that oversee to the protection of Information and resources in accordance with applicable security Guidance.
SECURITY SAFEGUARDS	Measures and controls that are prescribed to meet specified system security requirements. Safeguards may include, but are not limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices.
SECURITY TEST AND EVALUATION	Examination and analysis of the measures, safeguards and controls required to protect the FNCS system, as they have been applied in an operational environment, to determine the security posture of the system.
SENSITIVE INFORMATION	"Any information the loss, misuse or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552 a of title 5 USC (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign Guidance."
SENSITIVITY ASSESSMENT	Looks at the sensitivity of both the information to be processed and the system itself. The assessment considers legal implications, organization Guidance, and the functional needs of the system.

Terms	Definitions
SERVER	Server (computing) a computer that provides services to other computers, or the software that runs on it also like the internet sites like Google and Yahoo. Application server, a server dedicated to running certain software applications Communications server, carrier-grade computing platform for communications networks Database server provides database services Proxy server Provides database IT server in services Fax server provides fax services for clients File server provides file services Game server a server that video game clients connect to in order to play online together Standalone server an emulator for client-server (web-based) programs Web server a server that HTTP, WWW, COM, ORG, NET, CC, Info, and TV clients connect to in order to send commands and receive responses along with data contents. Client-server a software architecture that separates "server" functions from "client" functions The X Server part of the X Window System Peer-to-peer a network of computers running as both clients and servers.
SERVICE PACK	A service pack is an orderable or downloadable update to a customer's software that fixes existing problems and, in some cases, delivers product enhancements. IBM and Microsoft are examples of companies that use this term to describe their periodic product updates.
SERVICE SET IDENTIFIER (SSID)	Short for ***s****ervice* ***s****et* ***id****entifier*, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the Basic Service Set (BSS). The SSID differentiates one WLAN from another, so all access points

Terms	Definitions
	and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network. An SSID is also referred to as a *network name* because essentially it is a name that identifies a wireless network.
SPAM OR Spam	Electronic, unsolicited or undesired bulk electronic messages. There are many types of electronic spam, including E-mail spam, unsolicited e-mail.
SPECIALIZED (CUSTOM) SYSTEMS	Software that is developed for a specific function/project by a vendor or internal source.
STRONG AUTHENTICATION	The use of at least two forms of authentication to identify and authenticate a subject. Forms of authentication include something the subject knows (e.g. passwords.), something the subject has (e.g. keys, authentication tokens, smart cards, etc.), or something the subject is (e.g. biometrics).
SWITCHES	A switch is a device for changing the course (or flow) of a circuit. The prototypical model is a mechanical device (for example a railroad switch) which can be disconnected from one course and connected to another. The term "switch" typically refers to electrical power or electronic telecommunication circuits. In applications where multiple switching options are required (e.g., a telephone service), mechanical switches have long been replaced by electronic variants which can be intelligently controlled and automated.
SYSTEM INTERCONNECTION	The state of systems being mutually connected to each other.
SYSTEM	A discrete set of information technology, data, and related resources, such as personnel, hardware, software, and associated technology services organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. A system must have logical boundaries around a set of processes, communications, storage and must: (1) be under the same direct management control; (2) have the same function or mission objective; (3) have essentially the same operating characteristics and security needs; and (4) reside in the same general operating environment.
SYSTEM SECURITY PLAN (SSP)	A formal document that fully describes the in place security features and procedures and the planned security tasks

Terms	Definitions
	required to meet security requirements and eventualities.
THREAT	Any circumstance or event with the potential to cause harm to FNCS IT systems in the form of destruction, disclosure, modification of data, or denial of service.
TCP/IP - TRANSMISSION CONTROL PROTOCOL (TCP) INTERNET PROTOCOL (IP)	A suite of rules (protocols) that define how data is transported among computers on the Internet.
TRUSTED FACILITY MANUAL	A document prepared to satisfy the requirement of any Trusted Computer Security (TCSEC) class. The Trusted Facility Manual provides detailed information on how to: 1) configure and install a secure system; 2) operate the system securely; 3) correctly and effectively use system privileges and protection mechanisms to control access to administrative functions; and 4) avoid improper use of those functions which could compromise the trusted computer base (TCB) and user security. A Trusted Facility Manual is a necessary tool for all system administrators to ensure that they are running in a “trusted manner”.
UNAUTHORIZED ACCESS	The use of IT resources by any person not authorized to have access to the facilities housing the FNCS system, the system itself or the information residing therein.
USB – UNIVERSAL SERIAL BUS	USB (Universal Serial Bus) is a plug-and-play interface between a computer and add-on devices (such as audio players, joysticks, keyboards, telephones, scanners, and printers). With USB, a new device can be added to your computer without having to add an adapter card or even having to turn the computer off. The USB peripheral bus standard was developed by Compaq, IBM, DEC, Intel, Microsoft, NEC, and Northern Telecom and the technology is available without charge for all computer and device vendors.
USERS	Personnel or processes accessing an Information Technology resource either by direct connections (i.e., via terminals) or indirect connections (i.e., prepare input data or receive output).
VALIDATION	Determination of the correct implementation in the completed FNCS system with the security requirements and approach agreed upon by FNCS, and the user community.
VPN - VIRTUAL PRIVATE NETWORK	A private data network that makes user of the telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Terms	Definitions
VULNERABILITY	A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to FNCS systems.
WAN	A wide area network (WAN) is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks. An intermediate form of network in terms of geography is a metropolitan area network (MAN).
Wi-Fi – Wireless Fidelity	Wi-Fi is a brand originally licensed by the Wi-Fi Alliance to describe the embedded technology of wireless local area networks (WLAN) based on the IEEE 802.11 specifications. Wi-Fi was developed to be used for mobile computing devices, such as laptops in LANs, but is now increasingly used for more services, including Internet and VOIP phone access, gaming, and basic connectivity of consumer electronics such as televisions, DVD players, and digital cameras. More standards are in development that will allow Wi-Fi to be used by cars on highways in support of an Intelligent Transportation System to increase safety, gather statistics, and enable mobile commerce (see IEEE 802.11p). Wi-Fi and the Wi-Fi CERTIFIED logo are registered trademarks of the Wi-Fi Alliance - the trade organization that tests and certifies equipment compliance with the 802.11x standards.
WIRELESS DEVICE	Hardware that provides wireless capabilities. This definition includes, but is not limited to wireless handheld devices like PDAs, cellular/PCS phones, two-way pagers, wireless audio/video recording devices, telemetry devices with wireless integrated technologies, electronic tablets and laptop computers.
WIRELESS HANDHELD DEVICE	Small computers often capable of synchronizing with a PC on specific software applications. Many handheld devices are capable of “beaming” data with the use of Infrared (IR) or Bluetooth technologies. Handheld wireless devices include a range of PDAs and Smart phones that may combine the capabilities of a traditional PDA, digital cellular telephone with voice services as well as E-mail, text messaging, Web access, voice recognition and any number of applications that serve a productivity tools.
WLAN – Wireless LAN	A wireless LAN (or WLAN, for wireless local area network,

Terms	Definitions
	sometimes referred to as LAWN, for local area wireless network) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. The IEEE 802.11 group of standards specify the technologies for wireless LANs. 802.11 standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing and include an encryption method, the Wired Equivalent Privacy algorithm.
WORM	A complete program that propagates itself from system to system, usually through a network or other communication facility. A worm is similar to a virus and can infect other systems and programs. A worm differs from a virus in that a virus replicates itself, and a worm does not. A worm copies itself to a person's workstation over a network or through a host computer and then spreads to other workstations, possibly taking over a network. Unlike a Trojan horse, a worm enters a system uninvited.
WPAN - WIRELESS PERSONAL AREA NETWORK	WPANs operate in the Personal Operating Space (POS) of a user, which extends 10 meters in any directions. Also known as Bluetooth®, WPAN communications are governed by the IEEE 802.15 family of standards.

Additional Terms are located in the DM3595-00, 1 USDA Cyber Security Manual Series 3500 Glossary. http://www.ocio.usda.gov/directives/doc/DM3595-001.pdf.

Appendix B – Form FNS-674 Completion Instructions

The FNS-674 form is to be used to obtain access to the network, escalation of privileges, access to privileged information systems, etc.

Please refer to the system Access FNS -674 User guide located online here for further details on how to complete the FNS-674 form.

Appendix C – Password Hints

Password Protection Standards

- Treat passwords as sensitive, confidential information.
- Memorize your password.
- Passwords should never be written down or stored online.
- Never share your password with anyone.
- Immediately contact your ISSO if you feel your password has been compromised.

Creation of Password Standards

- Passwords must contain a minimum of twelve (12) characters
- Include at least three of the following character sets: upper case; lower case; numeric characters; special non-alphanumeric characters such as # & % ! @ ( ).
- Do not include any simple pattern of letters or numbers such as “aaabbbccc” or “12345678910.”
- Do not make passwords easy to guess e.g., “my family name” or a birth date or a street address.
- Do not use words in any language, slang, jargon or words found in a dictionary. For example, you cannot use xylophone, but you can use “Xy!oph0ne12!”
- Try using a favorite quotation as an acronym by using the first letter of each word in the quotation including upper case, lower case and punctuation to make your password more secure and easier to remember. Don’t forget to make your password 12 characters or more. Some examples follow:
  a. “Once upon a midnight dreary, while I pondered, ...”Ouamd,wip...”
  b. “T’was the night before Christmas and all, ...”Ttnbcaa…”
  c. “I’d walk a mile for a camel…!,” “Iwamfacl,…!”

Remember, more secure passwords are those which are based on pass phrases and/or non-dictionary words (including “nonsense” words), combined with obscure character substitutions. These types of passwords can be extremely difficult to either guess or crack.

Appendix D – Required C&A System Security Documents

Security Categorization Document (SCD)	The SCD is used to determine the appropriate security categorization for the system or application, and the levels of involvement identified for confidentiality, integrity, and availability. Federal Information Processing Standards Publication (FIPS PUB) 199 provides guidance for assigning security categorization factors for information processed on federal systems. Each factor is assigned a level of low, moderate, or high. Business reference models (lines of business and data types) should be referenced from NIST SP800-60. The completed System Categorization aka "Syscat" from the ASSERT/CSAM tool is acceptable for meeting this requirement. Unique Project Identifier (UPI) codes must be included in the SCD of ASSERT/CSAM document for systems covered by the document. This document may be included as an appendix in the system security plan (SSP).	FIPS PUB 199 NIST SP 800-60
Risk Assessment (RA)	The baseline for the risk assessment is the agency self-evaluation from NIST SP 800-30. The agency RA should be completed in accordance with NIST guidance to ensure that system security controls are maintained to protect system assets and information. This document may be included as an appendix in the SSP.	NIST SP 800-30
Privacy Impact Assessment (PIA)	The PIA provides an analysis of how personal information is handled in an information system. Agencies must complete a PIA for all systems. This document may be included as an appendix in the SSP.	Privacy Act of 1974
System Security Plan (SSP)	The SSP should contain a description of the security controls required for the system and how these controls are implemented as part of the system's security posture.	NIST SP 800-18 DM 3565-001
Security Control Assessment Plan	The Security Control Assessment plan should contain detailed procedures and/or checklists for validating the implementation of each required security control.	NIST SP 800-53
Security Control Assessment Report	The Security Control Assessment report contains results of functional and security testing conducted on the system as required	NIST SP 800-53

	by the security categorization.	
Security Assessment Report (SAR)	The format and content of the security assessment are described, including major findings, recommended corrective actions, and a proposed accreditation statement. In particular, the major findings should include both proposed residual vulnerabilities and proposed vulnerabilities requiring correction.	USDA Certification and Accreditation Guide
Contingency and Disaster Recovery Plans (CDRP)	CDRPs should include all procedures that will be taken in the event of an incident that shuts down the system, or a large emergency that destroys the system entirely. These procedures should provide for system and data restoration within a prescribed time based on system criticality. Often, for USDA systems, this information can be found in LDRPS. Plans must be tested annually. The following systems must have a fully functional test performed annually: Systems categorized as "High" by NIST FIPS 199; Systems that retrieve records by personally identifiable information (PII) and/or requires a system of record (SOR) notice to be posted; and Systems storing, processing, or transmitting agency financial information. Tabletop tests may be conducted for all other systems twice a year. (Note for re-accreditation: If a system has undergone no major changes and has satisfied its annual contingency plan test requirement, this will satisfy the C&A requirement of a tested contingency plan.)	NIST SP 800-34 DM 3570-001 FPC-65
Trusted Facilities Manual (TFM) or Equivalent	The purpose of a TFM is to document the necessary information to operate the system in a secure and effective manner. The requirement includes the following: Documentation shall include guide(s) or manual(s) for the system's privileged users. The manual(s) shall at a minimum provide information on (1) configuring, installing, and operating	

	the system; (2) making optimum use of the system's security features; and (3) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation shall be updated as new vulnerabilities are identified. The TFM is not meant for general users of the system, but for use by those personnel designated as having specific security-related responsibilities. It provides information about the environment, roles, and responsibilities that guide security administrators and others with security responsibilities in the use of the security features provided by the IS. The TFM documents the configuration guidance used, the operational requirements, the security environment, the hardware and software configurations and interfaces, and all security procedures, measures, and contingency plans for an IS. It also identifies known security vulnerabilities and any risk mitigation approaches employed. This document may be included as an appendix in the SSP.	
Security Features Users Guide (SFUG) or Equivalent	The SFUG should be written for system and application users, and should clearly explain the security procedures and precautions that users are expected to follow (i.e., procedures for maintaining password secrecy, etc.). This document may be included as an appendix in the SSP.	
Configuration Management Plan (CMP)	The configuration management plan is used to manage the changes that occur during a system's life cycle to ensure the integrity of the system. The National Consensus Standard for Configuration Management Government Electronics and Information Technology Association describes Configuration Management functions and principles, and defines a neutral Configuration Management terminology for use with any product line. This document may be included as an appendix in the SSP.	ANSI/GEIA EIA-649-A
Security Control Compliance Matrix (SCCM)	The matrix should list each security control, the reference from which the security control was derived, and whether or not the control was implemented. The SCCM should start with the appropriate NIST SP800-53 control	NIST SP 800-25 NIST SP 800-53 Rev 1

	baseline. It should then be tailored with supplemental and compensating controls as determined by the risk assessment. Baseline tailoring should be described in the SSP. This document may be included as an appendix in the SSP.	FIPS PUB 199 FIPS PUB 200
System of Records (SOR) Notice	The Privacy Act of 1974 requires agencies to publish in the Federal Register a "notice of the existence and character of the system of records." A "system of records" is defined as a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. This document may be included as an appendix in the SSP.	Privacy Act of 1974
Plans of Action and Milestones (POA&Ms)	POA&Ms are descriptions of measures implemented or planned to correct deficiencies and reduce/eliminate vulnerabilities identified by the certification team. This document may be included as an appendix in the SSP.	OMB Memorandum 02-01
Interconnection Security Agreement (ISA/MOU/MOA)	NIST Special Publication 800-47 "Security Guide for Interconnecting Information Technology Systems" (August, 2002) provides a management approach for interconnecting IT systems, with an emphasis on security. The document recommends development of an Interconnection Security Agreement (ISA) and a Memorandum of Understanding (MOU). The ISA specifies the technical and security requirements of the interconnection, and the MOU defines the responsibilities of the participating organizations. The security guide recommends regular communications between the organizations throughout the life cycle of the interconnection. One or both organizations shall review the security controls for the interconnection at least annually or whenever a significant change occurs to ensure the controls are operating properly and are providing appropriate levels of protection." This document may be included as an appendix in the SSP as appropriate by system.	NIST SP800-47

Appendix E – FNCS Risk Management Acceptance Report

<table>
<tr><td colspan="2">Risk Number:</td><td colspan="2">Report Date:</td></tr>
<tr><td colspan="2">POA&M Number:</td><td colspan="2">Date Risk was Identified:</td></tr>
<tr><td colspan="2">Originator: (Who identified the risk?)</td><td colspan="2">Expiration Date for the Risk Acceptance:</td></tr>
<tr><td colspan="4">C&A Name of the System:</td></tr>
<tr><td colspan="4">Risk Statement: (Enter a simple statement of what the risk is.)</td></tr>
<tr><td>Risk Rating (Circle One if known)</td><td>High</td><td>Medium</td><td>Low</td></tr>
<tr><td colspan="4">List all Devices impacted by this vulnerability: (System(s), Server(s), Router(s), Printer(s), Workstation(s), etc.).</td></tr>
<tr><td colspan="4">If there is a deviation from applicable laws, regulations, standards and/or policies – explain:

If so, has a waiver been approved:</td></tr>
<tr><td colspan="4">Justification for Acceptance: (State the brief reasoning for the risk acceptance.)</td></tr>
<tr><td colspan="4">Risk Control: (State the current controls and/or corrective actions to mitigate the threat.)</td></tr>
<tr><td colspan="4">Are there any budgeting constraints? (Check if 'Yes') ☐

If 'Yes', explain:</td></tr>
</table>

Risk Number:	**Report Date:**
Future Mitigation: *(Describe any plans/system changes that would mitigate this risk in the future.)*	
Approximate Completion Date: None	**Actual Closing Date:**
Designated Approving Authority Name:	
Designated Approving Authority: _____ _____	**Date Approved:** _____ ___
System Owner Name:	
System Owner Signature: _____ _____	**Date Approved:** _____ ___
Certifying Agent Name:	
Certifying Agent Signature: _____	**Date Approved:** _____ ___

FNCS Risk Management Acceptance Report Instructions

Use the following instructions to complete the FNCS Risk Management Acceptance Report.

- **Report Date:** Fill in the date of the report.
- **Risk/POA&M Number:** Leave this field blank. The number will be assigned by FNCS.
- **Date Risk Was Identified:** Enter the exact date the risk was recognized. This date should be the date of a scan report or the date of an official or formal audit report (e.g., Security Evaluation Report (SER); internal audit; etc.).
- **Originator:** Enter the name of the person or business source that identified the risk. If an official audit, include the audit number and date and the source (e.g., OIG-11101-1-1, 04/15/05). If done via contract support in support of Certification and Accreditation, show the name of the company (e.g., Acme Solutions) and the C&A project name (e.g., Telecom GSS, 2004).

- **Risk Statement:** Enter a simple statement describing the risk. This information should reflect verbiage used in the audit or actual scan report. If originating from an audit, use the statement in full or summarize if the statement is in excess of one paragraph. Reference a number in the audit report, a category label, and/or security category if provided (e.g., #11, AU-3, Audit and Accountability).
- **Risk Rating:** Indicate the risk rating provided by the source. If the rating came from a scanner, provide the name of the scanner (e.g., nCircle) along with the scan vendor's classification (i.e., H, M, L). If the source is an audit, the risk rating will be available in the details associated with the vulnerability that is cited; ensure that references (i.e., a security control abbreviation or number, and the number assigned by the audit source) to the audit are included in the Risk Statement area.
- **Is there a deviation from applicable laws, regulations, standards and/or policies?** Answer 'Yes' or 'No' and then explain your response. If 'Yes', explain. If FNCS or USDA policy states that a specific standard is required, such as the initiation of the screen saver after 10 minutes of inactivity, and the risk to be accepted cannot meet that policy or requirement, such as the screen saver locking up an application, state the pertinent information here. If there is a deviation from policy, answer 'Yes'. Answering 'Yes' will require the eventual submission of a waiver, or providing waiver-oriented answers, if the condition is in opposition to an existing policy; refer to the FNCS policy regarding 'Waivers'. If there is no current policy regarding the vulnerability, answer 'No' and go to the next question.

  If so, has a waiver been approved? Answer 'Yes' or 'No'.

- **Justification for Acceptance:** Enter a brief reason for the risk acceptance. State why the 'acceptance' is necessary (e.g., the vulnerability mitigation will require funds that are not available; the vulnerability mitigation is not cost effective based on the available resources; etc.). If there has been a temporary workaround to lessen the risk associated with the vulnerability, state what that interim workaround is as well as any future plans for mitigating long term.
- **Risk Control:** Enter the current controls and/or corrective actions to mitigate the threat. Respond with what you will be doing in the immediate future to attempt to combat this vulnerability, which could be a workaround, temporary solution, or a decision to do nothing (as long as you have some justification to accept the full extent of risk). The project manager and the system owner are the individuals who will really assume any risks and responsibilities.
- **Are there any budgetary constraints?** Place a check in the checkbox if the answer is 'Yes.'

  If 'Yes', explain: Enter an explanation for any budgetary constraints in this space. Include cost of hardware and software, but also identify human resources and contract support that may justify the decision to 'accept' the risk (e.g., performing activities manually, to replace what monies may be needed to purchase an automated function may far exceed the cost of hardware and/or software).

- **Future Mitigation:** Enter any information that outlines any plans/system changes that would mitigate this risk in the future. State if a future mitigation has been evaluated or is planned. A future mitigation may not be considered. If a software upgrade may mitigate a current vulnerability, state when that upgrade is scheduled for deployment.

- **Approximate Completion Date:** Enter the estimated complete date. Using FY notation is acceptable (e.g., end FY-2006; mid FY2007.
- **Actual Closing Date:** Fill in the actual date the risk was closed. Leave blank as long as the risk is open. When the risk closes, such as when an upgrade is deployed, list the date of closure.
- **Primary Contact Name:** Enter the telephone number or email address for the Primary Point of Contact that the vulnerability is associated with, such as a project team leader or a Branch Chief, which is usually the person who is responsible for operation of a function.
- **Primary Contact Signature:** The primary POC should sign the form in this space; the POC will be at the Branch Chief or Project Leader level.
- **Date Approved:** The date the form is signed by the primary POC.
- **System Owner's Name:** Enter the system's owner's name. The system owner will be at the level of Division Director.
- **System Owner's Signature:** The system owner should sign the form in this space.
- **Date Approved:** The date the system owner signed the form.
- **ISSPM Concur by Name:** Enter the name of an ISSPM who will approve the form.
- **Approval (Concur) Signature:** The designated ISSPM should sign the form in this space.
- **Date Approved:** The date the form was approved by an ISSPM should be entered.

Appendix F – ITIRB Portfolio Management Office Checklist

This checklist is to be used when process consultants submit requests for assist in processing IT requests. It is intended to assist you in ensuring that the Program Management Branch steps are completed and that all of the documentation required to justify the IT services and IT polices being requested by different branches are present and is as complete as necessary to present to FNCS managers and, when appropriate, the FNCS ITIRB.

ITIRB PMB Steps

✓ Discuss the request with the processing consultant and /or the originator and understand the request and how they intend to justify the request. Provide assistance on the viability of the request.

✓ Verify with the process consultant and/or the originator that the following forms filled out correctly:

- FNS-754 ITIRB User Request Form Template – Policy
- FNS-755 ITIRB User Request Form Template – System
- FNS-758 ITIRB User Business Case Summary Template

✓ Verify with the process consultant the required content for Sections 1-8 of FNS-755 or the required content for Sections 1-4 of FNS-754.

✓ After the request has been submitted and once the Branch Chief provides approval, assist the originator with any additional information on sections 1-8 of form 755 or sections 1-4 of 754 (If necessary). Then assist the originator if necessary, with additional justification by completing sections 9 -10 of form 755.

✓ If asked, assist the originator with the proper completion of the business case summary (FNS Form 758). After form 758 is complete, ensure that all forms and all sections are complete.

✓ Make sure the user submits the request to the Division Director for approval and signature.

- ✓ The Process consultant facilitates the communication to Senior Management of all requests coming from their area.

- ✓ Receive the completed forms from the user/process consultant.

- ✓ Review all forms for content and ensure all signatures are in place.

- ✓ Review the content of all sections to ensure that sufficient justification exists.

- ✓ Review database and other sources for duplications or potential solutions.

- ✓ Certify alignment with enterprise architecture, if not discuss with CIO.

- ✓ Enter the request into the database.

- ✓ Prepare recommendation to CIO.

Appendix G – CPO-ITIRB RECOMMENDATION

<table>
<tr><th colspan="4">PMO ITIRB RECOMMENDATION</th></tr>
<tr><td colspan="2">Requirement Title:</td><td>Originating Office</td><td>Process Consultant</td></tr>
<tr><td colspan="4">Description</td></tr>
<tr><td colspan="4">Technical Feasibility – Can the requirement be technically capable?</td></tr>
<tr><td colspan="4">Technical Alternatives – Have feasible alternatives been considered?</td></tr>
<tr><td colspan="4">Technical Compatibility – Does the requirement technically fit within the structure of the agency? Does the requirement align with the current enterprise architecture?</td></tr>
<tr><td colspan="4">Resources – Does the requirement require funding and personnel resources beyond the capability of the agency</td></tr>
<tr><td colspan="4">Other – Does the requirement already exist, etc.?</td></tr>
<tr><td colspan="4">Recommendation</td></tr>
<tr><td colspan="2">Forward to ITIRB □</td><td>Refer to OIT □</td><td>Return to Originator □</td></tr>
<tr><td colspan="4">Comments Supporting Recommendation</td></tr>
<tr><td colspan="4">Reviewed by:</td></tr>
<tr><td>ITIRB PMO</td><td colspan="3"></td></tr>
<tr><td>Chief, SAB</td><td colspan="3"></td></tr>
<tr><td colspan="4">Approved by:</td></tr>
<tr><td>CIO</td><td colspan="3"></td></tr>
</table>

APPENDIX H – FNCS Initial Incident Report Template

Status of Incident: *(circle one)* **New In Progress Closed**	**Incident Severity**: Severe Impact ■ Serious Impact ■ Limited Impact ■ *(circle one)*

FNCS Initial Contact Information

FNCS Incident Number:	**Date & Time Reported to FNCS:**	**Name of person taking the report:**
US-CERT Number:(*if applicable*)	**Date & Time Reported to US-CERT:** (*if applicable*)	
Date & Time SNCC Hotline was notified: (*if applicable*)	**Date & Time the incident occurred:**	

Incident Contact Information

Reported By:		
Name:	**Type of employee: (Fed, Contractor….)**	**Agency/ Location: (Region/HQ…)**
Office & Cell:	**Email:**	
Other contact information:		
Name:	**Office & Cell:**	
Name:	**Office & Cell:**	

Impact and Scope *(Complete only those items applicable to this incident)*

Type Incident:
Personally Identifiable Information (PII) involved? (Yes or No)
Type of PII: (SSN, Patient Data, Research Data etc.), if yes, has USDA been contacted?
Information Security Categorization (FIPS 199 / Risk Level): (L,H,M)
Potential affected population size (1-99, 100-999, 1000-9999, 10000 or more):
Location of Incident:
Potential affected geographic area:
Was the data encrypted? (Yes or No)

Incident Description

Give a detailed description of the incident:
List the next steps to be taken in the investigation process

Incident Response Team Actions

List actions taken by all incident handlers (Incident Response Team) on this incident

Incident Evidence Gathered

List evidence gathered during this incident investigation by the Incident Response Team

Comments from Incident Response Team

List comments related to this incident

1. **List evidence gathered during this incident investigation by the Incident Response Team**

Next Steps

List the next steps to be taken in the investigation process

APPENDIX I – Information System Security Guidance and Security Control Mapping

FNCS Section Number	FNCS Section Name	NIST SP 800-53 Security Controls	Other NIST Publications	Related USDA Policy
050	INFORMATION SYSTEM SECURITY PLANNING	PL-1, PL-2, PL-3, PL-4, PL-5, PL-6		
100	ACCEPTABLE USE	AC-1, AC-11, AC-14, AC-20, MP-5, SA-7, RA-5, PE-1, IR-1, SC-9, PL-4	800-18, 800-37	USDA DN 3300-011; DM 3525-000; DR 3300-001;DR 3300-1A-1M
200	NETWORK ACCESS	AC-8, AC-9, AC-17,AC-20,AC-11, SI-4, SI-8		USDA DM 3535-001; DM 3530-000;001;004, DM 3525-003
300	WIRELESS	AC-18		USDA DM 3550-003; DN 3300-12 3300-19
400	INCIDENT REPORTING & RESPONSE	IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7	800-86, 800-61, Rev. 1	USDA Security Computer Incident Response Team Standard Operating Procedures; DM 3505-000 USDA Computer Incident Response Procedures Manual; USDA Memorandum on Reporting Lost or Stolen

				Information Technology Equipment
500	AUDIT & ACCOUNTABILITY	AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-11		USDA DM 3535-001
600	ACCESS CONTROL	AC-1,AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9,IA-2, IA-4, IA4, IA9,		USDA DM 3535-001, Password policy memorandum Dated: 6/2007; USAD DR 3180-001 Information Network Standards, Appendix O
700	IT RESTRICTED SPACE	PE-2, PE-3, PE-3, PE-4, PE-5, PE-6, PE-7, PE-8		USDA DM 3510-001
800	COMPUTER SECURITY AWARENESS	AT-1, AT-2, AT-3, AT-4	800-16, 800-50	USDA DM 3545-001
900	CERTIFICATION& ACCREDITATION	CA-1,CA-2, CA-3, CA-4, CA-5, CA-6, CA-7	800-37	USDA Condensed Guide Certification and Accreditation Methodology; USDA Certification and Accreditation Guide, Appendix A; USDA DM 3540-001 Risk Assessment Methodology;

				FIPS Publication 199
1000	INFORMATION SYSTEMS SECURITY PROGRAM	PL-1		USDA DM 3545-002
1100	PERSONALLY IDENTIFIABLE INFORMATION	PL-5, RA-3		USDA DM 3515-002, Memorandum on transporting PII info. Dated 2/22/07.
1200	RISK MANAGEMENT	RA-2, RA-3, RA-4, RA-5		USDA DM 800-30; DM 3540-000; DM 3540-001
1300	CONTINGENCY PLANNING AND DISASTER RECOVERY	CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, CP-8, CP-9, CP-10	800-34, 800-84	USDA DM 3570-000, DM 3570-001
1400	SYSTEM SECURITY PLANS	PL-2, PL-3, PL-4	800-18, FIPS 199, FIPS 200	USDA DM 3565-001, USDA SSP (GSS) and (MA) Checklists
1500	SDLC	RA-2, RA-3, RA-4, CM-3, MP-6, PL-5	800-64	USDA DM 3575-001
1600	CPIC	SA-2, SA-3, SA-4	800-65	USDA DM 3560-001
1700	MAINTENANCE	MA-1, MA-2, MA-3, MA-4, MA-5, MA-6		
1800	MEDIA PROTECTION	MP-1, MP-2, MP-3, MP-4, MP-5, MP-6		
1900	PERSONNEL SECURITY	PS-2, P2-3, PS-4, PS-5, PS-6, PS-7, PS-8		