United States Department of Agriculture
Food, Nutrition and Consumer Services

Food, Nutrition and Consumer Services

Information Systems Security Guidelines & Procedures

702 Handbook

- VERSION 1-

RELEASE DATE: JANUARY 31, 2008

PREPARED FOR: ENRIQUE GOMEZ, CIO

OFFICE OF INFORMATION TECHNOLOGY (OIT)

PREPARED BY: OIT - INFORMATION SECURITY OFFICE (ISO)

THIS PAGE INTENTIONALLY LEFT BLANK

This is a complete revision of previous versions of the *FNCS 702 Handbook*. In this handbook you will find Guidance on the protection and use of FNCS Information Resources in accordance with USDA's Department Manuals, CS 3500-3599 Series, Memorandums, National Institute of Standards and Technology (NIST) publications, Office of Management and Budget (OMB) Circulars and Federal Information Processing Standards (FIPS) requirements. Please update any existing links you may have to the 702 Handbook with this new version
Dated: January 2008

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 V.1
Document Title	FNCS Information System Security Guidelines and Procedures 702 Handbook

Owner Details	
Name	Shawn Jones, ISSPM
Contact Number	703-305-2528
E-mail Address	Shawn.Jones@fns.usda.gov

Revision History			
Revision	Date	Author	Comments
1.0	January 31, 2008	Carol Ware	Created original version of the 702 Handbook.

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

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

IT SECURITY OVERVIEW ---- 9

GUIDANCE ON ACCEPTABLE USE OF FNCS INFORMATION RESOURCES ---- 11

100 OVERVIEW ---- 11
110 REFERENCES ---- 11
120 GUIDELINES ---- 11
130 PERSONAL USE ---- 12
140 E-MAIL USE ---- 13
150 INTERNET USE ---- 14
160 TELEPHONE EQUIPMENT AND SERVICES ---- 15

GUIDANCE ON ACCESSING THE FNCS NETWORK ---- 18

200 OVERVIEW ---- 18
210 REFERENCES ---- 18
230 FNCS NETWORK ACCESS FOR GOVERNMENT-OWNED EQUIPMENT (GOE) ---- 18
231 FNCS NETWORK ACCESS FOR POE ---- 19
232 FNCS NETWORK SECURITY CONTROLS ---- 20
233 FNCS NETWORK RESTRICTIONS ---- 20
234 HOW TO REQUEST ACCESS TO THE FNCS NETWORK ---- 21
235 HOW TO REQUEST REMOTE ACCESS TO THE FNCS NETWORK ---- 21
236 HOW TO LOG ONTO THE FNCS NETWORK (INTERNAL AND REMOTE) ---- 22
237 HOW TO LOG OFF OF THE FNCS NETWORK (INTERNAL AND REMOTE) ---- 22
238 HOW TO LOG ONTO WEB BASED APPLICATIONS, E.G. OUTLOOK WEB ACCESS (OWA) ---- 22
239 SEPARATION FROM FNCS ---- 23

GUIDANCE ON THE PROTECTION AND USE OF WIRELESS AND PED ---- 25

300 OVERVIEW ---- 25
310 REFERENCES ---- 25
320 WIRELESS TECHNOLOGY GUIDELINES ---- 25

GUIDANCE ON INCIDENT REPORTING AND RESPONSE ---- 26

400 OVERVIEW ---- 26
410 REFERENCES ---- 26
420 FNCS INCIDENT RESPONSE REPORTING GUIDANCE ---- 26
430 FNCS INCIDENT RESPONSE TRAINING AND TESTING GUIDANCE ---- 28

GUIDANCE ON AUDIT & ACCOUNTABILITY OF THE FNCS NETWORK ---- 29

500 OVERVIEW ---- 29
510 REFERENCES ---- 29
520 AUDIT AND ACCOUNTABILITY GUIDANCE ---- 29

GUIDANCE ON ACCESS CONTROL FOR FNCS INFORMATION SYSTEMS ---- 31

600 OVERVIEW ---- 31
610 REFERENCES ---- 31
620 FNCS ACCESS CONTROL GUIDANCE ---- 31
630 FNCS RECERTIFICATION OF ACCESS CONTROLS ---- 32
640 FNCS PASSWORD GUIDANCE ---- 32
641 NON-PRIVILEGED USER - PASSWORD GUIDELINES ---- 32
642 PRIVILEGED USER - PASSWORD GUIDELINES ---- 33
643 PASSWORD GUIDELINES FOR GOVERNMENT-OWNED WIRELESS PEDS ---- 33

GUIDANCE ON IT RESTRICTED SPACE AND PHYSICAL ACCESS CONTROL ---- 34
700 OVERVIEW ---- 34
710 REFERENCES ---- 34
720 RESPONSIBILITIES ---- 34
730 IT RESTRICTED SPACE AND USER ACCESS RECERTIFICATION PROCESS (PROPERTY MANAGEMENT BRANCH) 36
GUIDANCE ON FNCS COMPUTER SECURITY AWARENESS AND TRAINING ---- 37
800 OVERVIEW ---- 37
810 REFERENCES ---- 37
820 COMPUTER SECURITY AWARENESS ---- 37
830 COMPUTER SECURITY TRAINING ---- 38
GUIDANCE ON CERTIFICATION AND ACCREDITATION (C&A) OF SYSTEMS AT FNCS ---- 40
900 OVERVIEW ---- 40
910 REFERENCES ---- 40
920 RESPONSIBILITIES ---- 40
930 C&A GUIDANCE ---- 42
GUIDANCE ON THE INFORMATION SYSTEMS SECURITY PROGRAM (ISSP) FOR FNCS ---- 49
1000 OVERVIEW ---- 49
1010 REFERENCES ---- 49
1020 PURPOSE ---- 49
1030 FNCS ISSP STRUCTURE ---- 50
1050 ISSP ROLES AND RESPONSIBILITIES ---- 52
1060 DESIGNATION OF ISSPM AND DEPUTY ISSPM ---- 56
GUIDANCE ON THE PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION AT FNCS ---- 57
1100 OVERVIEW ---- 57
1110 REFERENCES ---- 57
1120 PERSONALLY IDENTIFIABLE INFORMATION (PII) ---- 57
1130 GUIDELINES ---- 58
GUIDANCE ON RISK MANAGEMENT AT FNCS ---- 60
1200 OVERVIEW ---- 60
1210 REFERENCES ---- 60
1220 FNCS RISK MANAGEMENT PROGRAM ---- 60
1230 RISK ASSESSMENT GUIDELINES ---- 61
1240 RISK ACCEPTANCE PROCEDURES ---- 62
GUIDANCE ON IT CONTINGENCY PLANNING AND DISASTER RECOVERY ---- 63
1300 OVERVIEW ---- 63
1310 REFERENCES ---- 63
1320 RESPONSIBILITIES ---- 63
1330 CONTINGENCY PLAN AND DISASTER RECOVERY GUIDELINES ---- 65
GUIDANCE ON FNCS SYSTEM SECURITY PLANS (SSP) ---- 66
1400 OVERVIEW ---- 66
1410 REFERENCES ---- 66
1420 RESPONSIBILITIES ---- 66
1430 USDA DEFINITIONS OF SYSTEM AND MAJOR APPLICATIONS ---- 67
1440 SSP GUIDELINES ---- 68
1450 SSP CHECKLIST(S) ---- 68

GUIDANCE ON THE FNCS SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC) ---- 69
1500 OVERVIEW ---- 69
1510 REFERENCES ---- 69
1520 RESPONSIBILITIES ---- 69
1540 SDLC PHASES ---- 71
1541 SDLC PHASES AND SECURITY REQUIREMENTS ---- 72
1542 SDLC PHASES AND DETAILED SECURITY REQUIREMENTS FOR EACH PHASE ---- 73
GUIDANCE ON FNCS CAPITAL PLANNING AND INVESTMENT CONTROL (CPIC) ---- 79
1600 OVERVIEW ---- 79
1610 REFERENCES ---- 79
1620 RESPONSIBILITIES ---- 80
1630 CPIC PHASES ---- 81
1631 PRE-SELECT PHASE ---- 82
1632 SELECT PHASE ---- 82
1633 CONTROL PHASE ---- 82
1634 EVALUATE PHASE ---- 82
1635 STEADY STATE PHASE ---- 82
1636 CPIC PHASES ---- 83
1637 CPIC REQUIRED DOCUMENTATION BY PHASE ---- 83
1640 FNCS CPIC PROCESS FLOW DIAGRAM (PER PHASE) ---- 86

FIGURES & TABLES

FIGURE 1-1 FNCS INCIDENT RESPONSE/REPORTING PROCESS FLOW ---- 27
TABLE 1-1 LEVEL OF CONCERNS FOR CONFIDENTIALITY, INTEGRITY AND AVAILABILITY - FIPS 199 ---- 43
TABLE 2-1 SECURITY CONTROLS AND REFERENCES ---- 44
FIGURE 2-1 GENERAL USDA RISK ASSESSMENT METHODOLOGY ---- 61
FIGURE 3-1 USDA IT CAPITAL PLANNING PHASES ---- 81

APPENDICES

APPENDIX A FNS 674 INSTRUCTIONS ---- 91
APPENDIX B INFORMATION SECURITY STAFF CONTACT LIST ---- 93
APPENDIX C PASSWORD HINTS ---- 96
APPENDIX D – REQUIRED C&A SYSTEM SECURITY DOCUMENTS ---- 97
APPENDIX E FNS RISK MANAGEMENT ACCEPTANCE REPORT ---- 100
APPENDIX F MAJOR APPLICATION SYSTEM SECURITY PLAN CHECKLIST ---- 103
APPENDIX G GSS SYSTEM SECURITY PLAN CHECKLIST ---- 108
APPENDIX H - ITIRB PORTFOLIO MANAGEMENT OFFICE CHECKLIST ---- 111
APPENDIX I CPO-ITIRB RECOMMENDATION ---- 112

GLOSSARY

GLOSSARY OF TERMS ---- 113

THIS PAGE INTENTIONALLY LEFT BLANK

IT 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.

- 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, computer security (e.g., hardware and software) and a mix of these areas.
- All guidelines within the 702 Handbook are written in accordance to USDA policies within the Department Manual Cyber Security 3500-3599 series.
- The sensitivity level of data processed on FNCS IT systems has been determined as Sensitive but Unclassified (SBU). Control measures are in place to protect FNCS data and the supporting IT systems commensurate with the sensitivity of the data.
- Mechanisms shall be integrated into the FNCS architecture to detect and minimize inadvertent and/or malicious modification or destruction of FNCS data.
- All guidelines within the 702 Handbook shall be adhered to by all FNCS Employees, Contractors and Official Visitors to 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 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 .

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 for both internal and remote access connections to the FNCS Network.

The purpose of 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 Owned Equipment (GOE) and the FNCS network is a privilege which imposes certain responsibilities and obligations to each FNCS user.

110 References

This Guidance is written in accordance with:

- NIST Special Publication 800-53 Rev. 1
- FNS Rules of Behavior
- 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 policies 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.
- Know who their Information System Security Officers (ISSOs) 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.

- 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 government office equipment for personal needs if the use does not interfere with official business and involves minimal additional expense to the Government. This limited personal use of government office equipment should take place during the employee's personal time, not during official duty time. This privilege to use Government office equipment 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

- 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 government office equipment 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 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, trade marked 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, Citrix or HTTPS.

- Securing SBU information prior to transmission. Please see Guidance for the Protection of SBU for further guidance on E-mailing SBU information.

- NewsStand is to be used as the official posting site for approved non-work related postings.

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 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 contact your ISSO before opening this attachment*.

- Sending to "Everyone", "Reply All" or similar groups in FNCS when the message is inappropriate or not authorized for distribution on the FNCS network.

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 GOE 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.

- 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 Instate 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 Telephones 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.

161Acceptable Telephone Use

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

- Does not adversely affect the performance of official duties by the employee or the employee's organization.

- Authorization was granted to use such resources for official Government business before they were made available for personal use.

- Use could not have been reasonably accomplished at another time.

- 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.
    - Call to notify family of a schedule change while traveling on Government business and delays that occur due to official business or transportation.
    - Make a brief call to their residence, while traveling. Not more than one call per day.
    - Call to advise their family of the change in schedule to make alternate transportation or child care arrangements.
    - Make daily brief calls to locations within the local commuting area to speak with spouse, minor children, schools and day care centers, etc.
    - Make brief calls to locations within the local commuting area that can only be reached during working hours, such as local government agencies, or physicians.
    - Make calls to arrange for emergency repairs for their residence or automobile, local calls only.
    - Make long distance calls during working hours for personal reasons that are:
        - Charged on the FNCS User's home phone number, calling card or other non-government number.
        - Made to a toll-free number.

162 Unacceptable Telephone Use

Inappropriate telephone use includes, but is not limited to:

- Use of the FTS2000/2001, government long distance service, commercial network, placing unauthorized long distance calls, calling "900" numbers including dialing an "800" number that connects to a "900" number.
- 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.

Guidance on Accessing the FNCS Network

200 Overview

This guidance applies to all devices/technologies (computers, laptops, printers, personal digital assistants (PDAs), routers, firewalls, servers, switches, access points, Universal Service 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 permitted to access the FNCS network remotely only via secured connections such as; Virtual Private Network (VPN), Hypertext Transfer Protocol over Secure Socket Layer, (HTTPS) and Citrix.

The purpose of this guidance is to define standards 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. 1
- 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 Guidelines

230 FNCS Network Access for Government-Owned Equipment (GOE)

FNCS Internal Access

- All requests for user level network access shall be made by completing the FNS 674 form. Please see Section 234 for details on requesting access. Access granted is applicable to only those applications that are necessary for the FNCS user's job.

- New hires to FNCS must complete Computer Security Awareness Training (CSAT) and Privacy Training prior to requesting access to the FNCS. Please contact your ISSO to receive instructions for taking this CD or Paper-based training.

- Any equipment connecting to the FNCS Network within FNCS facilities shall conform to FNCS 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 POE 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.

Remote Access

- All requests for remote network access shall be made by completing the Computer Access Request form, FNS 674. This request is not needed for access via Outlook Web Access (OWA).

- FNCS users requiring modifications to their current network access must complete the access request form, FNS 674.

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

- 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 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.

- Connections to the FNCS Network through VPN shall automatically disconnect a user from the network when inactivity is detected for 30 minutes.

- Remote FNCS network access connections are permitted only through FNCS approved secured methods, such as: VPN, Citrix or HTTPS.

231 FNCS Network Access for POE

Remote Access

- All requests for remote network access shall be made by completing the Computer Access Request form, FNS 674 and the Network Device Checklist (NDC), contact the IT Help Desk for the checklist.

- FNCS users requiring modifications to their current network access must complete the access request form, FNS 674. .

- 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.

- POE access to the FNCS network is permitted only via secured connections such as: VPN, HTTPS or Citrix.

232 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.

- All network traffic between FNCS locations shall be transported on dedicated FNCS/USDA owned circuits or through a VPN connection meeting encryption levels set by FNCS encryption standards.

- At anytime, 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. FNCS Users shall not use one of these or other devices to extend or re-transmit network services.

233 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 Users shall use only those Network Internet Protocol (IP) addresses issued by FNCS. Selecting an IP address at random 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.

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

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

234 How to Request Access to the FNCS Network

Complete the FNS Computer System Access Request Form FNS-674. This form can be accessed through the Intranet (E-forms) or by contacting the IT Help Desk. See Appendix A for instructions on how to complete the FNS-674 form.

- If you already have access to the FNCS Network and need to request access to the STARS, eDRS or FPRS Systems, request a level 2 e-Authentication User ID. To learn more about e-Authentication, click here.
- After all signatures are obtained, return the FNS-674 to the IT Help Desk.
- Upon approval:
  - Users will be notified when access has been granted.
  - Users must report to their corresponding OIT Security Office to obtain ID and temporary password.
  - Users must contact the IT Help Desk and request to have user profiles and Outlook set-up.
  - Users are provided with and required to read the Rules of Behavior. Users are required to sign the FNS Security Acknowledgement/Certification of Computer ID Acceptance Form, FNS-646 that will be attached to the Rules of Behavior. Pending the type of access provided, FNS Security Agreement for Local Administrator Rights, form FNS-761, will need to be signed.
  - Users are required to return the signed FNS-646 form to their appropriate security office within 15 days, failure to return will cause the user's FNCS Network access to be disabled.
  - Users may refer to Appendix B of this document to locate the security office for their area.

235 How to Request remote access to the FNCS Network

Complete the FNS Computer System Access Request Form FNS-674. This form can be accessed through the Intranet or by contacting the IT Help Desk. See Appendix A for instructions on how to complete the FNS-674 form. Submit this form to the IT Help Desk, they will ask you a series of questions about your request.

- The FNS-674 can be accessed through the Intranet (E-Forms) or by contacting the IT Help Desk.
- Upon approval:
  - Users will be notified that access has been granted.

- Users must report to the OIT Security Office to obtain ID and password. User must contact the IT Help Desk and request to set-up for remote access tools, i.e. VPN, Citrix. During this time, the IT Help Desk will determine which instructions are needed for logging onto the FNCS network remotely.

- Users are provided with and required to read the Rules of Behavior. Users are required to sign the FNS Security Acknowledgement/Certification of Computer ID Acceptance Form, FNS-646 that will be attached to the Rules of Behavior. Pending the type of access provided, FNS Security Agreement for Local Administrator Rights form FNS-761 will need to be signed.

- Users are required to return the signed FNS-646 form to their appropriate security office within 15 days, failure to return will cause the user's FNCS Network access to be disabled.

- Users may refer to Appendix B of this document to locate the security office for their area.

236 How to Log onto 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.

- Users must connect Government-owned equipment (GOE) 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.

- Users will contact the IT Help Desk for assistance in Outlook set-up.

237 How to Log off of the FNCS Network (Internal and Remote)

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". At the end of the day, do a log off of the network. At the end of the week, do a shut down of your computer.

238 How to Log onto web based applications, e.g. Outlook Web Access (OWA)

When logged onto the FNCS network (internal or remote), please adhere to the following procedures when accessing web-based applications:

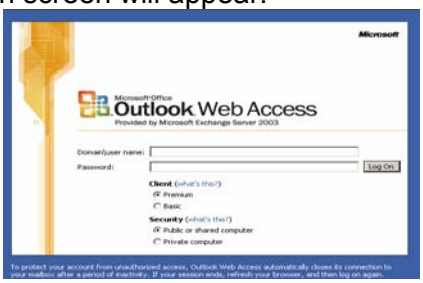
- POE is permitted to connect to the FNCS network to access web-based applications.

- Users may download/save FNCS information, E-mails, attachments and SBU information to GOE.

- How to access OWA:
  - Step 1: Navigate to the FNS OWA site located at: https://www.fns.usda.gov/fns/owa.htm
  - This FNS OWA screen will appear.

  - Step 2: Read the Official Warning and Click the "I Accept" button to continue.

  - Step 3: The OWA login screen will appear.



  - Step 4: **Enter** your FNS Network User ID in the Domain/User Name text box then **Enter** your FNS Network password into the password box.

  - Step 5: For Client, make sure Premium is selected.

  - Step 6: For Security, select Public/Shared computer or Private computer.

  - Step 7: **Click** Log On.

  - Step 8: You are now in your FNS Outlook Mailbox where you can send/read e-mail, view your calendar and schedule meetings.

239 Separation from FNCS

All users are required to send an E-mail to their Information Security Office (ISO) when access to a particular computing resource is no longer required for reasons such as; a project is complete, transfer to another position, retiring or resigning.

- ISSPM, ISSM and ISSO contact E-mail addresses:
  HQ: SecurityOfficers.Mailbox@fns.usda.gov
  MARO:SecurityOfficers.MailboxMARO@fns.usda.gov
  BRSB: ISSO.BRSB@fns.usda.gov
  MWRO:SecurityOfficers.MailboxMWRO@fns.usda.gov

NERO: SecurityOfficers.MailboxNERO@fns.usda.gov
SERO: SecurityOfficers.MailboxSERO@fns.usda.gov
SWRO: SECMailSWRO@fns.usda.gov
WRO: SecurityOfficers.MailboxWRO@fns.usda.gov
MPRO: MPSecurityOfficersMailboxMPRO@fns.usda.gov

- All FNCS employees must 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 will contact their COTR and request the Government Contractor's Employee Separation Checklist. This checklist is also available for download on the Electronic Library under COR Documents. The checklist must be completed with all applicable signatures on the last day of employment.

Guidance on the Protection and Use of Wireless and Portable Electronic Devices (PED)

300 Overview

Wireless is a technology that permits the active transfer of information involving emanation of energy between separated points without physical connection. Currently, wireless technologies use Infrared (IR), radio frequency (RF) and optical technology but as wireless evolves, it could include other methods of transmission.

310 References

This guidance is written in accordance with:

- NIST Special Publication 800-53 Rev. 1
- DM 3550-003USDA Portable Electronic Devices and Wireless Technology
- DN 3300-012 through 3300-019 USDA Commercial Wireless Technologies in USDA, Unclassified Security

320 Wireless Technology Guidelines

321 Present State of Wireless Technologies at FNCS

- Currently, FNCS does support a wireless networking infrastructure. GOE with Wi-Fi capabilities may be used to access OWA, Citrix and VPN.

- FNCS has approved the use of the following wireless devices/technologies:
  - Smart phone/Personal Digital Assistant (PDA) – *Only approved users*
  - Air Card – *Only approved users*
  - Bluetooth® - Voice
  - NIC – Network Interface Card
  - Commercial Wireless

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

322 Home/Commercial Wireless 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 only via secured connections such as; VPN, HTTPS or Citrix.

Guidance on Incident Reporting and Response

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, availability and 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.

410 References

This guidance is written in accordance with:

- NIST Special Publication 800-53 Rev. 1
- 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

420 FNCS Incident Response Reporting Guidance

- As soon as an FNCS user suspects or confirms an incident that involves FNCS Information Resources, i.e. workstations, documents, laptops that contains Personally Identifiable Information (PII) or Sensitive but Unclassified (SBU) information, the Information Security Office (ISO) must be contacted immediately by dialing 703-305-2528 or sending an E-mail to SecurityOfficers.Mailbox@fns.usda.gov .

- The ISO will request additional information from the user to gauge the severity of the incident.

- The person reporting the incident should be able to provide as much of the following information as possible:

1. Incident type: e.g. Lost laptop with PII
2. Time of incident:
3. Date of incident:
4. Time incident report to ISO:
5. Time and Date incident report filed with ISO:
6. Time incident resolved:
7. How was the incident resolved?
8. How was the incident reported/discovered?
9. Impact and scope (Client outage, loss of functionality, regions affected, etc.):
10. Description of incident:
11. Description of Data contained in Computer/Laptop:
12. Description of Sensitive Data contained in Computer/Laptop:
13. Cause of incident:
14. Police Report filed? (Attach copy of police report)
15. Equipment Information: (Serial Number, Type; Mfg; Model, etc.)

- The ISSPM will meet with the CIO and discuss the details of the incident. The CIO to determine how and to whom the incident should be reported.

- After the CIO has reviewed the specifics of the incident and determined the severity of the incident, he will approve the ISSPM to report it to USDA in accordance with the reporting procedures stated in the Cyber Security CIRT SOP, Security Computer Incident Response Team Standard Operating Procedures. The Incident Reporting/Response process provides an overview of steps taken to report and respond to an incident. The FNCS user should be familiar with this process.

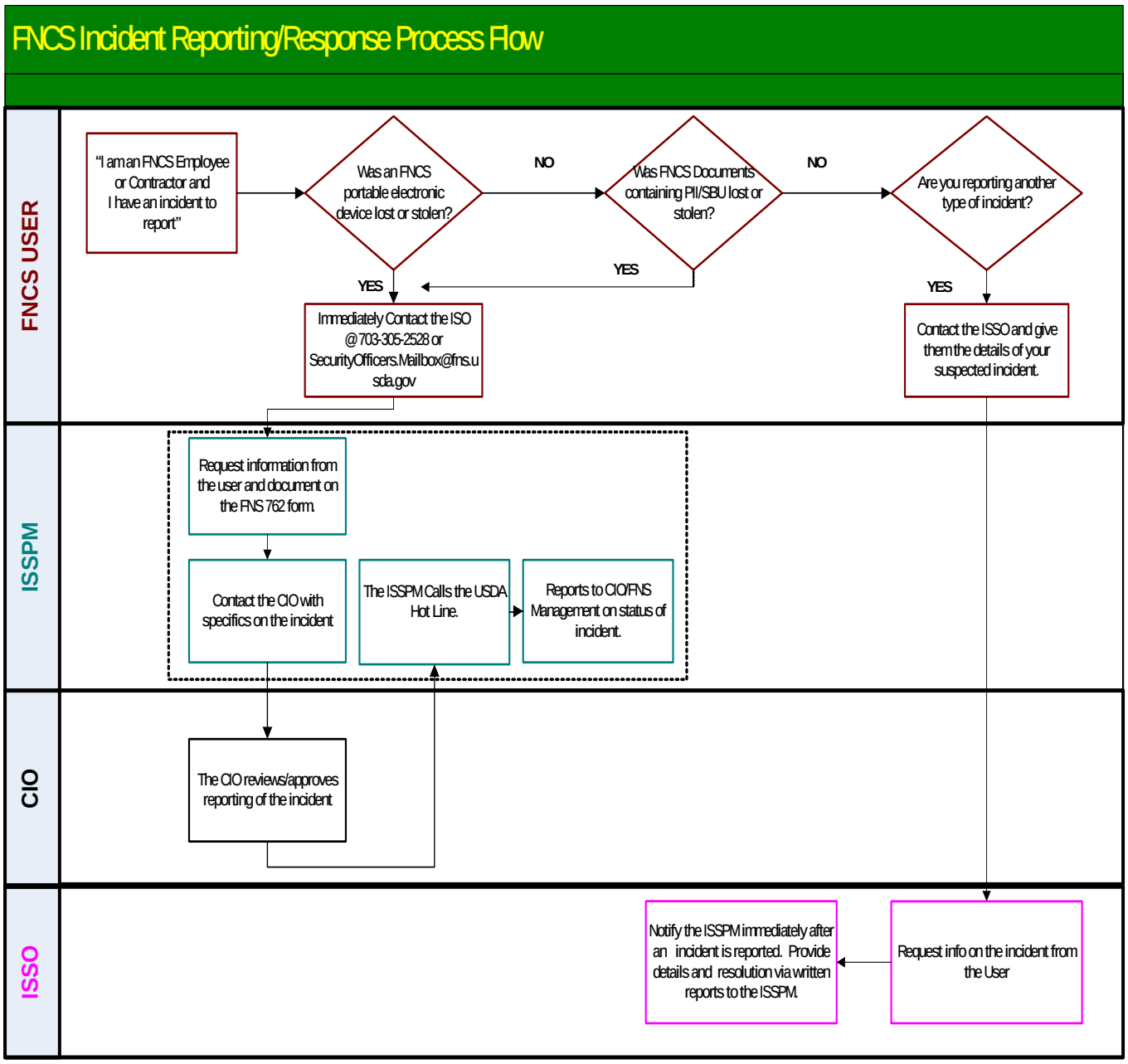


Figure 1-1 FNCS Incident Response/Reporting Process Flow

430 FNCS Incident Response Training and Testing Guidance

- FNCS shall assign roles and responsibilities to designated personnel who are a part of the FNCS Incident Response Team (IRT).
    - IRT is the official FNCS incident response resource team.
    - IRT shall offer advice and assistance to users for handling and reporting security incidents.
    - Based on the type of incident discovered, the IRT shall report security incidents to the ISSPM and/or the USDA ACIO CS. The ACIO CS is responsible for reporting designated incidents to United States Computer Emergency Readiness Team (US-Cert).
- FNCS shall provide annual security incident and response training for the IRT.
    - Training shall include "real" security incident scenarios to provide the response team with actual incidents and responses.
    - FNCS shall provide automated mechanisms to create a realistic training environment.
- FNCS shall test its security incident response capability annually through the execution of planned tests and/or exercises. The IRT and other designated personnel shall participate in:
    - creating test plans for security incidents;
    - scheduling the security incident tests/exercise;
    - assist in the creation of the simulated security-incident.
- The IRT and other designated FNCS personnel shall participate in all testing of simulated security incidents.
- The IRT shall document all results from the security incident tests/exercise.
- FNCS shall implement security incident handling capabilities to properly prepare, detect, analyze, contain, eradicate and recover from FNCS security incidents. This guidance is detailed in the Security Computer Incident Response Team Standard Operating Procedures

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 security audits on FNCS Information Systems. FNCS uses NetPro Auditor for its FNCS IT Systems. Audits are performed to protect entire systems from the most 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.

510 References

This policy is written in accordance with:

- NIST Special Publication 800-53 Rev. 1
- DM 3535-001 USDA C2 Level of Trust Policy

520 Audit and Accountability Guidance

521 It is the responsibility of FNCS LAN Administrator 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.

- Protect audit records and audit mechanisms from unauthorized access, modification or deletion. All audit records produced from an information system shall contain:

  - Date and time of the event, e.g. Time stamps are synchronized with internal information system clocks;
  - Whether the event occurred from software or 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 its capacity.

- 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 every 30 days or more based on the transaction volume.

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

522 It is the responsibility of FNCS User to understand that audit tools are used to monitor and control the FNCS Network.

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.

Access controls also include biometric scans, hidden paths, metal locks, digital signatures, encryption, social barriers and monitoring by human and automated mechanisms.

The purpose of this guidance is to maintain information security by preventing unauthorized access to FNCS Information systems and data. 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 the guidelines for Identification and Authentication.

610 References

- NIST Special Publication 800-53 Rev. 1
- DM 3535-001 USDA C2 Level of Trust Policy
- Password Policy Memorandum dated: 12 June 2007

620 FNCS Access Control Guidance

- FNCS uses Microsoft Active Directory to manage all information systems that establish, activate, modify, review, disable, and remove user accounts.

- Accounts that are created, modified, disabled and terminated are to be audited. Alerts shall be sent to the appropriate FNCS IT staff members when such actions occur.

- Temporary and emergency accounts are terminated weekly.

- Inactive accounts are automatically disabled after one month of inactivity.

- 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, this is considered Discretionary Access Controls which consists of Access Control lists (ACL).

- 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. This will be determined by the executive or manager deemed to be the system owner of the asset.

- FNCS shall implement least privilege that grants users only those accesses required to perform their duties.

- FNCS shall establish object reuse capabilities to ensure storage objects/devices that store SBU information is 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.

630 FNCS Recertification of Access Controls

- All system database access user lists must be reviewed and recertified every 90 days by the System Owner. This review includes all user privilege levels to any or all portions of a database.

- Recertification forms (FNS-763) can be found on the Intranet (E-Forms). Once a recertification is completed, the signed form must be submitted to the Information Security Office (ISO) and signed by the System Owner and ISSPM.

640 FNCS Password Guidance

641 Non-privileged User - Password Guidelines

Non-privileged users do not have administrative rights on a system or application.

- Non-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 alpha, numeric 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 IT Help Desk or submit a work order via the IT Customer Support Web portal at http://home.fnsnet/management_intranet/OIT/fnsnet/trackit.htm to report that your account is locked. Follow instructions given by the IT Help 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.

- 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.

- 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 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 alpha, numeric and special characters.
- Dictionary words used for passwords are prohibited.
- User accounts are locked after five (5) failed attempts. If this occurs, call the IT Help Desk or submit a work order via the IT Customer Support Web portal at http://home.fnsnet/management_intranet/OIT/fnsnet/trackit.htm to report that your account is locked. Follow instructions given by the IT Help 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.
- Do not automate passwords through use of function keys, scripts or other methods that store passwords on systems.
- Please refer to Appendix C for Password Hints.

643 Password guidelines for Government-owned Wireless PEDs

- 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 IT Help Desk.
- Lock the device after 15 minutes of inactivity.

Guidance on IT Restricted Space and Physical Access Control

700 Overview

The United States Department of Agriculture, Food, Nutrition and Consumer Services houses and 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 (SCIFs) and isolation zones.

710 References

This policy is written in accordance with:

- NIST Special Publication 800-53 Rev. 1
- DM 3510-001 USDA Physical Security Standards for IT Restricted Space

720 Responsibilities

721 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.

722 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.

723 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:
  - Branch Chief, Technical Services Branch (TSB), OIT Headquarters
  - Branch Chief, Benefit Redemption Systems Branch (BRSB)
  - Branch Chief, Regional Offices (RO)

724 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.
- Document non-compliance found in IT restricted space and provide a written report to the ACIO for Cyber Security within 150 days from issuance of this document.

725 The Property Management Branch will:

- Maintain all user access requests to IT restricted space by generating weekly reports of user access and performing audits for unauthorized access.
- Remove access to users who have been inactive for 90 days.
- Remove all access for users who have been terminated: FNS employees, contractors and others who are no longer at FNCS.
- Ensure that all user access requests to IT restricted spaces meets 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 730 for details on recertification.

726 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:
  - Fire detection personnel
  - Alarm system personnel
  - Air Conditioning maintenance personnel
  - UPS maintenance personnel
  - Hardware maintenance personnel
  - Software maintenance personnel
  - Other Vendors

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

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

Step 2: The Property Management Branch will review and determine which users need access to IT restricted space.

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

Step 4: The Property Management Branch 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 Property Management Branch has the appropriate corrective action plans in place.

Step 6: The Property Management Branch will retain all recertification documents for 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.

810 References

This policy is written in accordance with:

- NIST Special Publication 800-53 Rev. 1
- NIST Special Publication 800-16
- NIST Special Publication 800-50
- DM 3545-001 Computer Security Training and Awareness Policy

820 Computer Security Awareness

Awareness – "relies on the creation of an eye-catching package that gets the attention and reaches broad audiences".

- The FNCS Information Security Office (ISO) will conduct computer security awareness campaigns through several vehicles:
  - hosting seminars on computer security
  - distributing interactive electronic-based training
  - giving demonstrations on computer security and
  - conducting computer security "trivia games" throughout the year

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

- The ISO will promote computer security in the Office of Information Technology's efforts on the improvement of outreach and communication within OIT.

830 Computer Security Training

831 Computer Security and Awareness (CSAT) and Privacy Basic Training

- CSAT and Privacy training is currently implemented by USDA on an annual basis.
- The CSAT and Privacy training consists of an interactive, electronic-based training module that provides computer security information and assessments of that information.

- All FNCS employees, contractors and official visitors, regardless of their job duties are required to complete this training with a passing score.

- Currently, the USDA CSAT and Privacy Basic training is given via 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/ .

832 Computer Security Training Requirements

- Computer security 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.

- Computer Security Awareness and Training requirements are to be included in new employee orientation at FNCS. All FNS new-hires are required to complete this training prior to receiving access to the FNCS Network.

- The ISO will implement an annual security training compliance and evaluation process.

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

- The ISO will develop a security training program and ensure all information security professionals are appropriately trained to fulfill their security responsibilities. The training program will include but is not limited to:
    - Legal use of software
    - Software license agreements
    - FISMA information security controls
    - Information security controls and application development
    - USDA and FNCS information security policies and procedures
    - Privacy, Personal Identifiable Information (PII)
    - Risk Management
    - Contingency Planning
    - Disaster Recovery

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

- Information systems security professionals are required to take refresher training at least annually or when there are major system modifications, changes/upgrades in software or change of duties.

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

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:

- National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 1
- National Institute of Standards and Technology (NIST) Special Publication 800-26
- National Institute of Standards and Technology (NIST) Special Publication 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

920 Responsibilities

This sections details the responsibilities of all teams and individuals who are impacted by or involved in system C&As. Please identify your individual or team role in the C&A process.

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 at the Certifying Official for FNCS.

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 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.
- Issue an Interim Authority to Operate (IATO) when presented with a system with approved plans for remediation of uncorrected risks.

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 ST&E 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.

930 C&A Guidance

1. C&As are performed every three (3) years or when a significant system change occurs.
2. C&As are performed for both General Support Systems (GSS) and Major Applications.
3. 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.
4. The C&A process consists of three phases:

   - Phase 1 Pre-certification
   - Phase 2 Certification and Accreditation
   - Phase 3 Post Accreditation

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

The following steps will provide guidance on 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 5-1 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 ST&E and inform the CO. The CO approves the ST&E team and ensures they are independent of FNCS OIT.

932 Level of Concern for Confidentiality, Integrity and Availability

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.
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 severe 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 1-1 Level of Concerns for Confidentiality, Integrity and Availability - 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.

Example

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 Appendix G CA-1*				

Table 2-1 Security Controls and References

Step 3: **Conduct a PIA and if required complete a 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 competed 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:

√	C&A Scope	
√	Security Categorization Document	SCD
√	Security Controls Compliance Matrix	SCCM
√	Privacy Impact Assessment	PIA
√	System of Record and Notice	SORN
√	Initial Risk Assessment	RA

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

934 Phase 2 Certification and Accreditation

The following steps will provide guidance on the steps taken to perform a certification and accreditation:

Step 1: **Conduct a Security Test and Evaluation (ST&E) (Acquisition/Development Phase of the SDLC)**

a. The ST&E Team evaluates the effectiveness of security controls through hands-on testing. FNCS has uses a third-party to perform ST&Es.
b. The ST&E consists of three steps:
    1. Create an ST&E Test 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 ST&E 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 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 each system vulnerability and evaluate the likelihood that the identified threat may exploit a 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, ISA and PIA**

a. The SSP should be updated to reflect the results of the ST&E 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 complete.

a. The Certification Team documents all findings in the Security Evaluation Report (SER).
b. The findings include:
   - ST&E
   - Risk Assessment
   - The Certification Team creates and submits the Certification Package. The certification package is forwarded to the CO for review. The package includes:
     √ SCCM
     √ ST&E
     √ ISA
     √ PIA
     √ SORN
     √ Risk Assessment
     √ System Security Plan
     √ 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 their review, a Certification Statement is created that 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 CO's recommendation and the ACIO-CS concurrence, the DAA will grant system accreditation or deny it.
b. 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
   - ST&E
   - ISA
   - PIA, if applicable
   - SORN, if applicable - *A SORN is a System of Record Notice. The Privacy Act of 1974 requires any agency that maintains information about an individual in a "system of records" (a group or records … where information is retrieved by the name of an individual, or by some*

identifying number, symbol, or other identifying particular) to publish a notice in the Federal Register of the existence and character of that system of records. A SORN is only required if the information in a system of records is actually retrieved by a personal identifier.

- 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.

935 Phase 3 Post-Accreditation

The following steps will provide guidance on what occurs during the Post-Accreditation phase of the C&A process.

Step 1: During this phase, the system configuration is managed to ensure that changes to the system do not affect the security posture of the system and to facilitate follow-on C&A activities. Any system changes will be discussed and approved by the CCB.

Step 2: The System Owner keeps the SSP, Risk Assessment, as well as other documents up-to-date, ensuring to include new security controls as they are implemented.

Step 3: The system is re-accredited every three years or when major changes occur to the system configuration.

Step 4: The system owner will begin the certification and accreditation process (for re-accreditation) in time to meet the three year anniversary of the system.

Step 5: The system owner will test the Contingency Plan on an annual basis during the post accreditation phase of the C&A.

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.

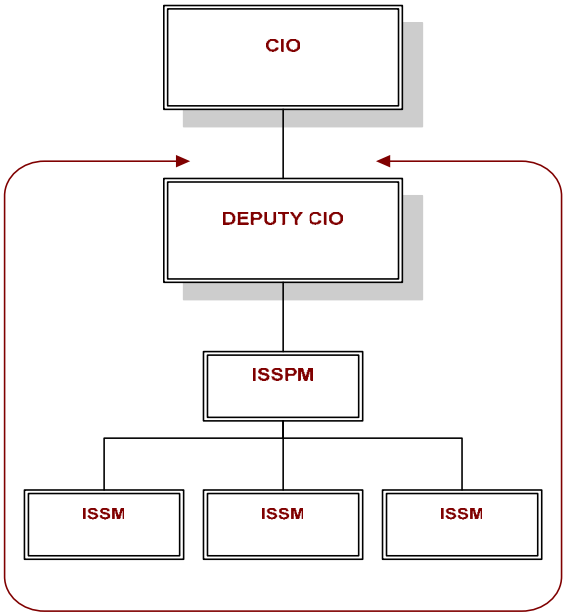
1030 FNCS ISSP Structure

FNCS has elected an alternative structure for the ISSP. An alternative structure is useful in agencies that have more than 1000 IT users. Currently, FNCS has approximately 1500 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.

The ISSP Management hierarchy is represented in the Organizational Chart below:



Information Security Office Management 3-Tier Structure

1040 Management Structure of the ISSP

1041 Information Systems Security Program Manager (ISSPM):

The duties and responsibilities of an ISSPM are diverse, comprehensive and complex. This position is one of high sensitivity and level of trust and therefore will be filled only by full time government personnel. In addition, this position has a requirement for high confidentiality due to the critical nature of the investigatory and compliance work. Therefore space should be assigned to the ISSPM that affords locking files and the ability to conduct meetings of a highly sensitive nature in private. In no case, are ISSPMs to be assigned to a work/office area with individuals not associated with information security. To successfully establish, manage and improve an FNCS ISSP, the ISSPM shall receive comprehensive annual security training. The ISSPM, ISSM, PM and ISSO positions are considered to be High Risk Public Trust positions as defined by 5 CFR 731. 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 FNCS CIO office.

The FNCS ISSPM shall be recognized as the organization's Cyber Security (CS) expert, leader and point of contact. This person is responsible for managing the ISSP efforts for the Agency. This person is a program manager responsible for the strategic security requirements of the program to include planning, budget review, consolidation of agency security reports, and coordination of the ISSP into the culture of the entire organization. ISSPMs will act as consultants for ISSM, PM and ISSOs and work with them to resolve highly technical matters, when necessary. Ultimately, the ISSPM is still responsible for efficient operation of the overall ISSP.

1042 Information Systems Security Manager (ISSM):

This person 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.

1043 Information Systems Security Officer (ISSO):

FNCS 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 work closely with and report directly to the ISSM assigned to their system.

1050 ISSP Roles and Responsibilities

1051 The CIO/Deputy CIO will:

1. Act as the agency Chief Information Security Officer (CISO) who is responsible for supporting the strategic requirements of the ISSP.
2. Ensure adequate funding, training and resources are provided to the ISSP to support the agency mission.
3. Facilitate the resolution of high-level security matters within the agency by acting as a proponent for ISSPM.
4. Ensure that ISSM/ISSOs are designated to provide adequate security to business, functional or operational entities.
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. Ensure that the designated ISSPM is a permanent member of all system development, telecommunications planning and the System Development Life Cycle (SDLC) planning teams.
9. Designate a Contingency Planning Coordinator.
10. Ensure that the ISSPM receives role-based and specialized security-based training.
11. *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 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 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 ACIO CS.
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 form 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 encryption standards.
14. Participate in the C&A process.
15. Oversee Contingency and Disaster Recovery Plans for each site, in coordination with COOP.
16. Approve updates to the SSPs.
17. Enter all POA&Ms into the USDA approved tool.
18. Create and disseminate updated security document templates to the ITPM, System Owners and Contractor/Development Teams.
19. Lead special projects, e.g. CSAMS development, 702 handbook updates, etc.

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 an agency 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; (See also Table 1: Phases of the Basic C&A Process).
15. Update system SORN annually in coordination with ISSM and Privacy Officer. Update SSP, Risk Management Plan (RMP), and CMP annually (See also Table 1: Phases of the Basic C&A Process).
16. 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.
17. Grant access and password requests after receiving authorization from system owners or from authorization officers designated by system owners.
18. Update the CCB Charter annually and as needed, and CCB minutes as needed.
19. Support and facilitate the security awareness, training and education program; follow up with users for annual CSAT and Privacy training;
20. Participate in monthly Security Office/Privacy meetings.
21. Assist the ISSM in any other security related duties, as required; participate in special projects as directed by the ISSPM.

1060 Designation of ISSPM and Deputy ISSPM

Name:_____
Agency: _____

GS Series/Title:_____

Level of Background
Investigation:_____

Location: _____

_____

Phone Number: _____ Cell Number: _____

Fax Number: _____ E-mail:_____

Agency CIO Name :_____

Agency CIO Signature: _____

Date: _____

Guidance on the Protection of Personally Identifiable Information (PII) at FNCS

1100 Overview

PII refers to information that can be used to distinguish or trace an individual's identity such as name, social security number, or medical records, etc., that when combined or used with other identifying information is linked or linkable to a specific individual.

FNCS is responsible for ensuring the privacy, confidentiality, integrity, and availability of customer and employee information. FNCS recognizes that its customers and employees have some reasonable expectation of privacy about themselves. This includes an expectation that FNCS will protect personal, financial and employment information from unauthorized disclosure. Customers and employees also have the right to expect that FNCS will collect, maintain, use, and disseminate personally identifiable information only as authorized by law and as necessary to carry out agency responsibilities.

1110 References

This Guidance is written in accordance with:

- NIST Special Publication 800-53 Rev. 1
- DM 3515-002 Privacy Impact Assessment
- Protecting Personally Identifiable Information: Social Security Number Policy Guidance Memorandum, dated September 17, 2007
- The Privacy Act of 1974
- Computer Security Act of 1987
- OMB Circular A -130
- OMB Instructions for Complying with the President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"
- Freedom of Information Act, as Amended
- Memorandum on Physical Transport of Personally Identifiable Information, dated February 22, 2007
- http://www.usdapii.gov/

1120 Personally Identifiable Information (PII)

Social Security number
Place of Birth
Date of Birth
Mother's maiden name
Biometric record (e.g. fingerprint, iris scan, DNA)
Medical history information (includes medical conditions, and metric information, e.g. weight, height, blood pressure)
Criminal history
Employment information to include ratings disciplinary actions, performance elements and standards
Financial information
Credit card numbers
Bank account numbers
Security clearance history (not including actual clearances held)

If you have questions on identifying PII, please contact the Information System Security Officer in your area, immediately. See Appendix B

Table 3-1 List of PII

1130 Guidelines

1131 Protecting PII

- In the event electronic media which contains PII is lost or stolen, immediately report this incident to the ISSPM, by calling 703-305-2528 or emailing SecuritOfficers.Mailbox@fns.usda.gov . For additional details on reporting incidents, please refer to the Guidance on Incident Reporting and Response.

- All FNCS employees and contractors are responsible for identifying customer and employee PII. All documents with PII shall be marked and transported accordingly. Please refer to the Guidance on the Protection, Maintenance and Use of Sensitive but Unclassified Information (SBU).

1132 Transporting PII

- FNCS personnel are allowed to transport PII as long as it is in electronic format and encrypted using FNCS approved encryption methods.

- PII may be physically transported, only when deemed necessary. In this case, the electronic media containing PII:

    - Must be encrypted using FNCS approved encryption methods.
    - Must be transported by the United States Postal Service, Federal Express, DHL or private courier.
    - Must be double wrapped in an opaque package that is sealed to prevent inadvertent opening and shows signs of tampering.
    - Must have an accompanying decryption key forwarded via a separate package or other alternate channel.
    - Must be sent via a certified carrier that provides the ability to track, pickup, transfer and deliver the package with PII.
    - If necessary, electronic media with PII may be transmitted via interoffice mail provided it is double-wrapped to afford sufficient protection against inadvertent or unauthorized access.

1133 Performing a Privacy Impact Assessment (PIA)

- New systems in the early stages of development (initiation phase of the SDLC) and systems undergoing major enhancements are required to perform a PIA.

- System Owners and developers must work together to complete the PIA. The system owner is responsible for stating how the data will be used, who will use the data and for what reasons.

- All existing systems will undergo a PIA every three (3) years.

- The system developer must address whether the implementation of the system owner's requirements present any threats to individual privacy.

- Please refer to this link for the latest PIA template; http://www.ocionet.usda.gov/ocio/security/docs/PIA_Template-2007June6.doc

- After the PIA is performed it should be given to the Program Management Office (PMO) for review and submission to the ISSPM.

1134 Guidance on the collection, use, maintenance and dissemination of Social security number (SSN) or Tax ID number (TIN)

- SSNs and tax identification numbers may be used, collected, disseminated and maintained in FNCS systems only when a system of record notice (SORN) has been published in the Federal Register. This has to be completed prior to collecting SSNs or TINs.

- SSNs and TINs are not to be used as unique identifiers or embedded in a number used for identification. Only government-wide established unique identifiers will be used in lieu of individual or business SSNs or tax identification numbers.

- FNCS systems that do not have authority and approval to collect and/or use SSNs or TINs as system unique identifiers are required to remove them as unique identifiers by September 2008.

- For the legal use of SSNs and TINs:

    - They are not to be used as unique identifiers.
    - SSNs and TINs are encrypted or masked from view on the computer screen, reports and print documents

- For the development of new systems which collect, maintain and use SSNs or TINs

    - Perform a PIA. See section 1133 for details.
    - Create/publish a SORN with the Federal Register, contact the FNCS Privacy Officer.
    - Submit the completed PIA and SORN to the Program Management Office for review and submission to the Privacy Officer and ISSPM.

Guidance on Risk Management at FNCS

1200 Overview

Protection of information assets and maintaining the confidentiality, integrity and availability of FNCS information technology 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.

This guidance provides the strategies used to implement an FNCS Risk Management (RM) Program. RM includes a structured approach to assessing risks, identifying vulnerabilities, reporting, accepting risk and implementing appropriate mitigation strategies through the creation of Plan of Actions and Milestones (POA&Ms).

1210 References

This Guidance is written in accordance with:

- NIST Special Publication 800-53 Rev. 1
- NIST Special Publication 800-30
- USDA DM 3540-000 Risk Management Program
- USDA DM 3540-001 Risk Assessment Methodology

1220 FNCS Risk Management Program

- FNCS has established a risk management program through the creation of a risk management team comprised of IT representatives from FNSHQ and each Region.

- 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 the FNSHQ ISSM allows 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.

- A Share Point site has been established as the Risk Management Team's formal collaboration tool, all documents related to Risk will be stored here.

1230 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

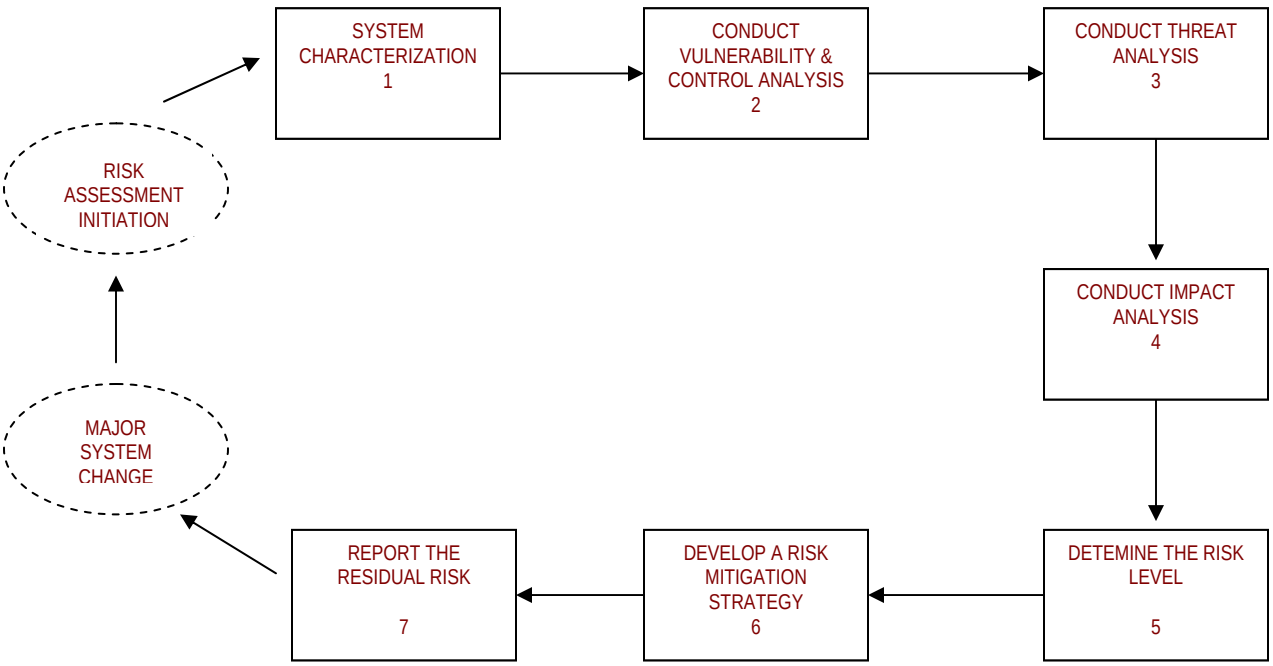


Figure 2-1 General USDA Risk Assessment Methodology

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 ST&Es.
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.

1240 Risk Acceptance Procedures

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:

1. Recognition by a user or system administrator
2. An equipment or network scan
3. An annual self assessment
4. The Certification and Accreditation (C&A) Security Testing and Evaluation (ST&E) process

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

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. 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 weekly to discuss current issues with agency-wide IT Contingency and Disaster Recovery Plans and to provide recommendations to standardize IT Contingency and Disaster Recovery Plans.

This procedure will be updated in version 2 to include the outcome of the CPWG recommendations to USDA Cyber Security. The anticipated outcome of this working group includes the following:

- Recommendations for a Standardized Table of Contents (TOC) for IT Contingency Plans
- Recommendations for a Standardized Table of Contents (TOC) for Disaster Recovery Plans
- Standardized Business Impact Analysis (BIA)
- Disaster Recovery Test Plan template
- After Action Report template

1310 References

This Guidance is written in accordance with:

- NIST Special Publication 800-53 Rev. 1
- 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 Responsibilities

1321 The CIO 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 Occupant Emergency Plan (OEP), Interconnected Systems and business process as part of the SDLC.
- Ensure DRPs are tested at least bi-annually or when a major change occurs to a system.
- Ensure all system recovery procedures are developed and implemented.
- 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 Planning Coordinator (CPC) will:

- Be a member of the ISO.
- Coordinate with the System Owners and Project Managers for each system to define the way they depend on or support the IT System.
- Ensure daily back-up procedures are in place for each system.
- Confirm that off-site storage is available for all system data.
- Identify disruption impacts through the results of the system(s) BIA.
- In coordination with the System Owner and Project Manager, prioritize the recovery strategies that personnel will implement during contingency plan activation.
- Coordinate with System Owners and Project Managers to establish contingency teams and team leads for disaster recovery and damage assessment.
- Ensure all plans are reviewed and updated bi-annually.
- Work closely with FNCS COOP Coordinator.

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 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 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 assessable in the event of a disaster.

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

- 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.

- The ISO will develop a Contingency training program to be used as a guide for training all recovery teams on an annual basis. Refresher training will be offered for new employees or after a major change to a system occurs.

- 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' telecommunication services are provided by AT&T's Universal Telecommunications Network (UTN). Currently, FNS has a Service Level Agreement (SLA) with AT&T that permits the resumption of system operations within 4 hours in the event that primary capabilities are unavailable.

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. 1
- NIST Special Publication 800-18
- USDA DM 3565-001 Annual Security Plans for Information Technology (IT) Systems
- Cyber Security IT System Security Plan Review Report, November 2007
- Federal Information Processing Standards (FIPS) 199
- Federal Information Processing Standards (FIPS) 200

1420 Responsibilities

1421 The CIO 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 CIO, 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.
- Ensure all SSPs are submitted to the CIO with a cover letter for signature attesting the accuracy and completeness of the plans.
- Participate in the development of exception requests.

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 USDA Definitions of a System .

1440 SSP Guidelines

- An Information System Inventory is required for 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 SSPs are reviewed and updated annually.

- The security plan will reference:
    i. Risk Assessment
    ii. Plan of Action and Milestones (POA&M)
    iii. Accreditation decision letter
    iv. Privacy impact assessment
    v. Contingency plan
    vi. Configuration management plan
    vii. Security configuration checklist
    viii. Results of penetration testing
    ix. All system interconnection agreements (MOUs)

- The cover page of the SSP will contain the system name and investment number.

- Contact the ISSM for the SSP templates.

1450 SSP Checklist(s)

- Based on the type of system; major application or GSS, an SSP checklist is provided to validate the information in the SSP. The checklist must be completed. See Appendix F and Appendix G for the GSS and Major Application Checklists.

- After the check list is complete, if there are any items that are marked as “N”, review this area of the SSP and update, if applicable.

- Submit both the SSP and SSP checklist(s) to the ITPM. the ITPM will submit the completed documents to the ISSPM for review and approval.

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. 1
- DM3575-001 Security Controls on the Systems Development Life Cycle
- NIST Special Publication 800-64

Please see the USDA definition of a "System".

1520 Responsibilities

1521 The CIO will:

- Be responsible for the organization's information system planning, budgeting, investment, performance and acquisition.
- Provides 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.
- Plays a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize information security risks to the organization.
- Coordinates and performs system risk analyses, analyzes risk mitigation alternatives, and builds the business case for the acquisition of appropriate security solutions that help ensure mission accomplishment in the face of real-world threats.
- Supports senior management in ensuring that security management activities are conducted as required to meet the organization's needs.

1523 The ISSM will: ensure there 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 is 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 Parties

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 ST&E	ST&E 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	TSB
Hardware and Software Disposal	TSB

1540 SDLC Phases

There are five (5) basic phases of the SDLC as defined by NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems, they are:

1. Initiation
2. Acquisition/Development
3. Implementation
4. Operation/Maintenance
5. Disposition

Within each phase of the SDLC security requirements are put in place and tested, please see Table 4-1 SDLC

1541 SDLC Phases and Security Requirements

	Initiation	Acquisition/ Development	Implementation	Operations/ Maintenance	Disposition
SDLC Phases and Processes	**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
Security Requirements	• System Categorization • Preliminary Risk Assessment • Privacy Impact Assessment (PIA) • System Security Plan (SSP) • Interconnection Service Agreement (ISA) • Configuration Management Plan	• Risk Assessment • Security Functional Requirements Analysis • Security Assurance Requirements Analysis • Cost Considerations and Reporting • Security Planning • Security Control Development • Development Security Test and Evaluation (ST&E) • 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 4-1 SDLC Phases and Security Requirements

1542 SDLC Phases and Detailed Security Requirements for each Phase

1. Initiation Phase

This is the first phase of the SDLC which includes security requirements such as valuation of system assets, functional requirements and the development of the ISA. The initiation phase is where the formal process change control begins.

It is the responsibility of the System Owner, ISSM, Project Manager and Developers to work in coordination throughout this phase.

1a. Valuation of System Assets:

- Each System Owner needs to determine the value and sensitivity of data to meet program delivery requirements.
- A business case is the start of the valuation of system assets.
- The primary source of business case information is the System Owner.
- The valuation of system assets is completed in the initiation phase.

1b. Determine the System's Categorization (High, Moderate, Low)

- By defining the level of the system, the system owner will determine the potential impact on FNS in the event there is a breach of security (a loss of confidentiality, integrity and availability).
- *Please refer to FIPS 199 Standards for Security Categorization of Federal Information and Information Systems and the FNCS Guidance on Certification and Accreditation for further information on determining the System Category.*
- Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.
- The system categorization is completed in the initiation phase of the SDLC. Please contact the ISO for a template to complete the system categorization document (SCD).

1c. Privacy Implications:

- Privacy implications need to be determined during the initial phase of the SDLC.
- Please refer to the *Guidance on the Protection of PII and the C&A Procedures* for further information on performing a Privacy Impact Assessment (PIA).
- In the event privacy information is identified a System of Record (SOR) Notice is also required for this system.
- The PIA is completed in the initiation phase of the SDLC. Please see the PIA template at http://www.ocionet.usda.gov/ocio/security/docs/PIA_Template-2007June6.doc

1d. Interconnectivity Security Agreement (ISA):

- In cases where the system is connected to other systems, the system owner must discuss the requirements for connectivity with the other system owner's and work to identify the security requirements for this connection.
- *Please contact the ISO for an ISA template.*
- ISAs are required for each system that is connected to the new system.
- The ISA is refined in the next phase (Acquisition/Development); however it may not be finalized until the Implementation phase of the SDLC.

1e. Preliminary Risk Assessment (RA):

- The preliminary risk assessment defines the possible threat(s) to the environment that the system will operate.
- The risk assessment also includes a set of initial basic security controls and potential countermeasures.
- The RA is refined in the next phase (Acquisition/Development) of the SDLC.

1f. System Change Control:

At the completion of the Initiation Phase, the Configuration Management process and formal CM plan is developed.

2. Acquisition and Development Phase

During the second phase of the SDLC, the system is developed and acquired. This section identifies security requirements that need to be performed during this phase.

Pre-Requisites: To enter into this phase, an ISA must be started (if applicable), a valuation of system assets must have been completed and a preliminary risk assessment must be performed.

It is the responsibility of the System Owner, ISSM, Project Manager and Developers to work in coordination throughout this phase.

2a. Risk Assessment:

- The initial risk assessment will be used to analyze the system and identify the protection requirements. This analysis will be documented in the formal risk assessment process.
- The risk assessment will take into consideration other USDA systems that may be affected directly or indirectly connected to the new system.
- The risk assessment will address the following key enterprise-wide security objectives:
    - Prevent the creation of vulnerabilities or unintended interdependencies.
    - Prevent decreasing the availability of other enterprise systems.
    - Prevent decreasing the security posture of other enterprise systems
    - Analyze any attempts made to counter hostile actions created through external domains.
    - Possess the appropriate security specifications for the system environment
    - Security specifications are clearly stated.
    - Security specifications that are implemented will reduce the risk to the system and USDA mission that supports the system.
- The risk assessment is performed prior to approval of the design specifications.

2b. Security Functional Requirements Analysis:

An analysis of the functional requirements includes the system security environment and compliance with applicable laws and regulations, such as Privacy, FISMA, NIST, OMB, FIPS and other federal regulations that define baseline security requirements.

2c. Security Assurance Requirements Analysis:

- An analysis of requirements is conducted to address the developmental activities required and evidence needed to produce the desired level of assurance that the security requirements are appropriate for the system.
- The results of this analysis will be used to determine how much and what kinds of assurance are required.
- Cost effective assurance that meets the requirements for protection of FNCS' information assets and legal mandates is the goal.

2d. Cost Considerations and Reporting:

- Through the results of the risk assessment, the development costs attributed to information security over the life cycle of the system can be determined.
    - A cost benefit analysis on the recommended controls is performed to see if the recommendation is cost-effective, in the event of an incident or potential impact to FNCS.
    - Once a control is selected, the cost of each can be totaled for an overall security cost.
    - The benefits of incorporating the cost early into the SDLC is it usually more difficult to add functionality into a system after it has been built and it is less expensive to include the preventive measures to deal with a cost of a security incident.

2e. Security Planning:

- Ensure that all system security controls, planned or in place are documented in a system security plan (SSP). Refer to the Guidance on System Security Plans for further details on the SSP.
- Evaluate and update the ISA as needed with other system owners.

2f. Other Security Planning Components:

During the acquisition/development phase of the SDLC, other considerations include:

- Type of Contract;
- Review by other functional groups;
- Review by Certifying Official (CO) and Designated Accrediting Authority (DAA);
- Continuance of System Change Control.

2g. Security Control Development:

- Ensure the security controls described in the respective security plans are designed, developed and implemented as documented in the SSP.
- Include additional and/or modify existing security controls for existing systems as needed.

2h. Security Test and Evaluation (ST&E) development:

- The technical security controls that can be tested prior to deployment of the system are tested within this phase of the SDLC.
- The ST&E plan is developed and performed by an independent team, the results of this test provides valuable feedback to the developers, system owners, project manager and integrators.
- This test is included as a part of the C&A package.

3. Implementation Phase

The third phase of the SDLC consists of the installation and evaluation of the system in the operational environment.

Pre-Requisites: The Risk Assessment, ST&E and the ISA are completed and approved by the DAA. All other tasks of the Acquisition and Development Phase have to be accomplished.

It is the responsibility of the System Owner, ISSM, Project Manager and Developers, Certifying Team and DAA to work in coordination throughout this phase.

3a. Inspection and Acceptance:

- QA/CM verifies and validates the functionality of the system through an Independent Validation and Verification (IV&V). The IV&V will include testing of security in the system as well.
- QA/CM officially accepts the system (deliverables) through a formal sign-off.

3b. Security Control Integration:

- Ensure that security controls are integrated at the operational site where the system is to be deployed for operation.
- Ensure all security control settings and switches are enabled in accordance with manufactures instructions and the availability of security implementation guidance, such as a Trusted Facilities Manual (TFM).

3c. Security Certification:

- The Certification Team creates needed documents to prove that the appropriate safe guards and countermeasures are in place to protect the system.
- The system is certified.
- See the Guidance on C&A Process for further information.

3d. Security Accreditation:

- The DAA gives authorization for the system to process, store or transmit information.
- The system is accredited or an IATO is approved.
- See the Guidance on C&A Process for further information.

3e. System Change Control:

Continue change control as directed by the Configuration Management Plan to ensure that the system has been designed in accordance with the baseline system requirements.

4. Operations/Maintenance Phase

The fourth phase of the SDLC occurs when the systems are in place and operating, enhancements and modifications to the system are developed and tested.

Pre-Requisites: The system is certified and accredited by an authorized DAA who has granted authority to the system to operate or approve an Interim Authority to Operate (IATO) and mitigation strategy for the system.

It is the responsibility of the System Owner, ISSM, Project Manager and Developers, QA/CM to work in coordination throughout this phase.

4a. Configuration Management and Control:

- Manage the potential security impacts to systems when specific changes are suggested to systems or its surrounding environment.
- Maintain an on-going effort to document all system changes and assess the potential impact on the security of the system, currently all Change or Enhancement Requests (CERs) are documented in an FNCS approved CM tool.

4b. Continuous Monitoring:

- Monitor security controls for effectiveness through periodic assessments and evaluations.
- FNCS ISO, PM and System Owners will coordinate and implement self-assessments of each system security controls based on FISMA security requirements, SP 800-53, Revision 2.

4c. Continuous Certification and Accreditation:

All systems will be re-certified and re-accredited every 3 years at a minimum.

5. Disposition Phase

The fifth phase of the SDLC is the final phase of the SDLC. This phase states the security requirements involved in the disposition of systems, hardware and software.

Pre-Requisites: The DAA grants authority to retire the system after the Agency CIO approves the proposed system retirement and determines that this other systems are not impacted.

It is the responsibility of the System Owner, ISSM, Project Manager, QA/CM and FNCS Records Officer to work in coordination throughout this phase.

5a. Information Preservation:

- All electronic records created by FNCS will be managed as federal records.
- All federal records will be managed throughout the records life-cycle and ensure the reliability and authenticity of records as legal evidence of their actions and decisions.
- Electronic records are only destroyed in accordance with the disposition schedule approved by the Archivist of the United States.

5b. Configuration Management and Control:

After the determination and approval to retire a system, the system baseline is frozen and all CM documents are included in the information preservation process.

5c. Media Sanitization:

A degaussing process is used to delete and/or erase data from all media that is no longer in use. Contact TSB for further details on degaussing.

5d. Hardware and Software Disposal:

- Prior to the sell or surplus of hardware, it will be sanitized through degaussing.

- Prior to the destruction of software, it will be destroyed in accordance with the license agreement.

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 Capital Planning and Strategic Management Office (CPO) 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 CPO 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 see click on the following link: OCIO.usda.gov/cpic/doc/2007_CPIC_Guide-complete_AppendixN.pdf

1610 References

This Guidance is written in accordance with:

- National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 1
- National Institute of Standards and Technology (NIST) Special Publication 800-65
- USDA DM 3560-001, Security Requirements for CPIC
- OCIO.usda.gov/cpic/doc/2007_CPIC_Guide-complete.pdf
- FNCS Information Technology Investment Review Board Instructions
- IT Capital Planning and Strategic Management Office (CPO) Charter
- Appendix H – ITIRB/CPO Checklist
- Appendix I – ITIRB/CPO Recommendations

1620 Responsibilities

1621 The CIO 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.

1622 The ISSPM will:

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

1623 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.

1624 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.

1625 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.

1626 The Portfolio Manager will:

- Ensure that FNCS personnel adhere to CPIC procedures.
- Notify the OCIO CPIC staff of findings/documents.
- Update Worklenz 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.

1630 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.

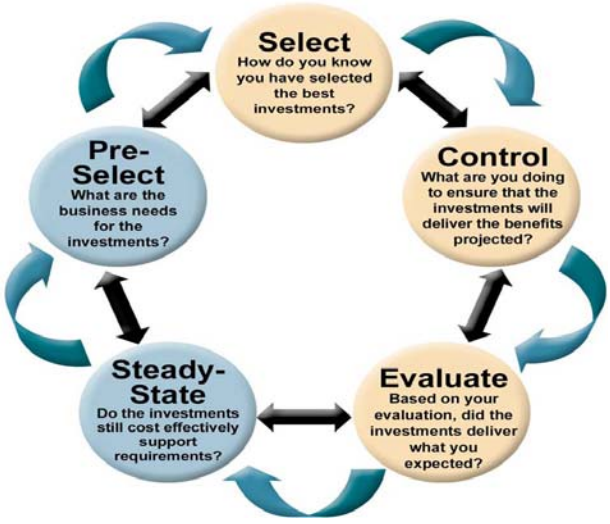


Figure 3-1 USDA IT Capital Planning Phases

1631 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.

1632 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.

1633 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.

1634 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.

1635 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.

1636 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 investment decision	• 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 • Review initiative and recommend appropriate action. • Make final investment decisions.	• 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. • Review initiative and recommend appropriate action. • Make final investment decisions • Work with project sponsor to develop solutions.	• 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 process.	• 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 decisions.

1637 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:**
  Major Initiatives:

  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

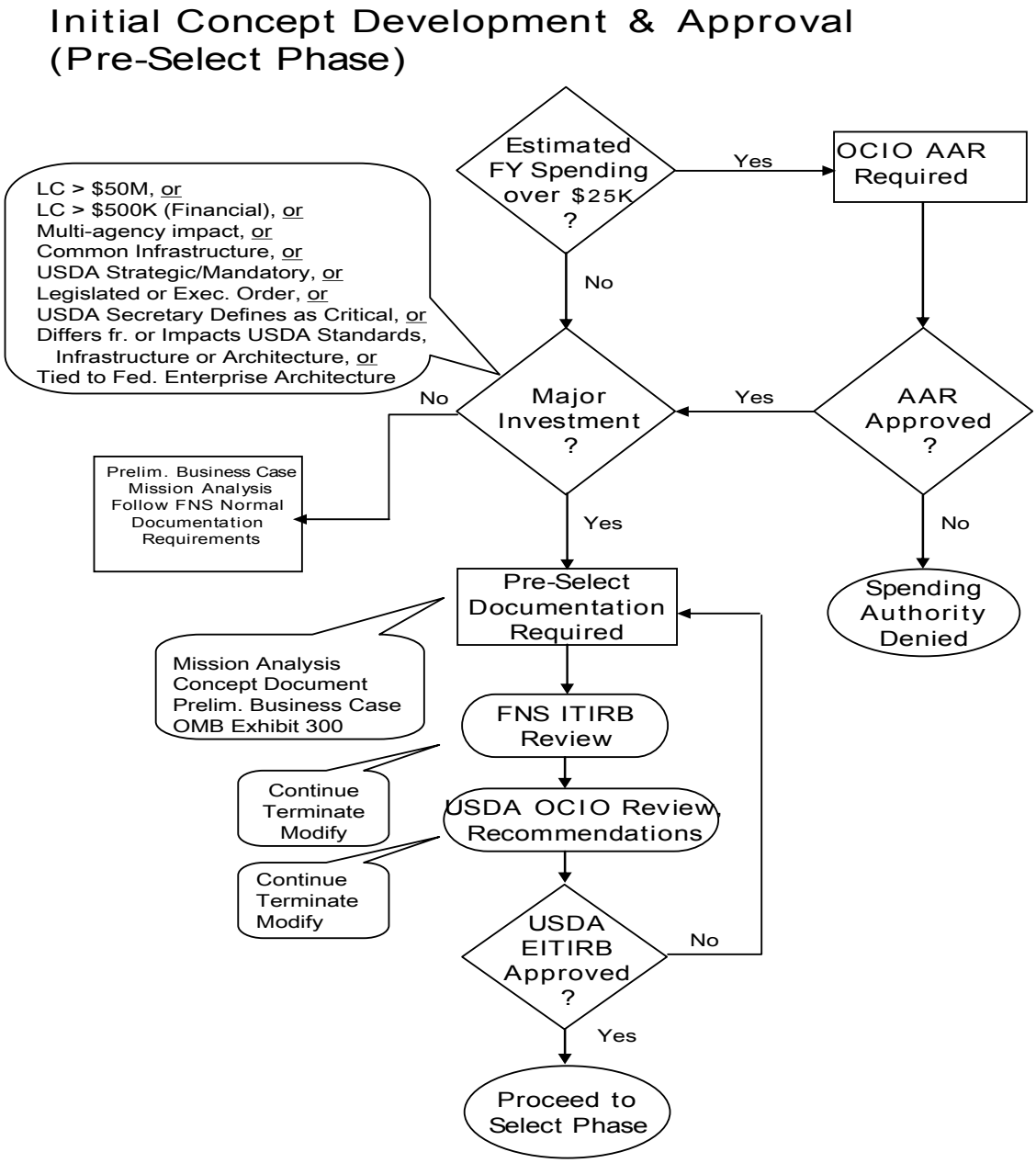
*Please see Guidance on FNCS System Security Plans (SSP)

- **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

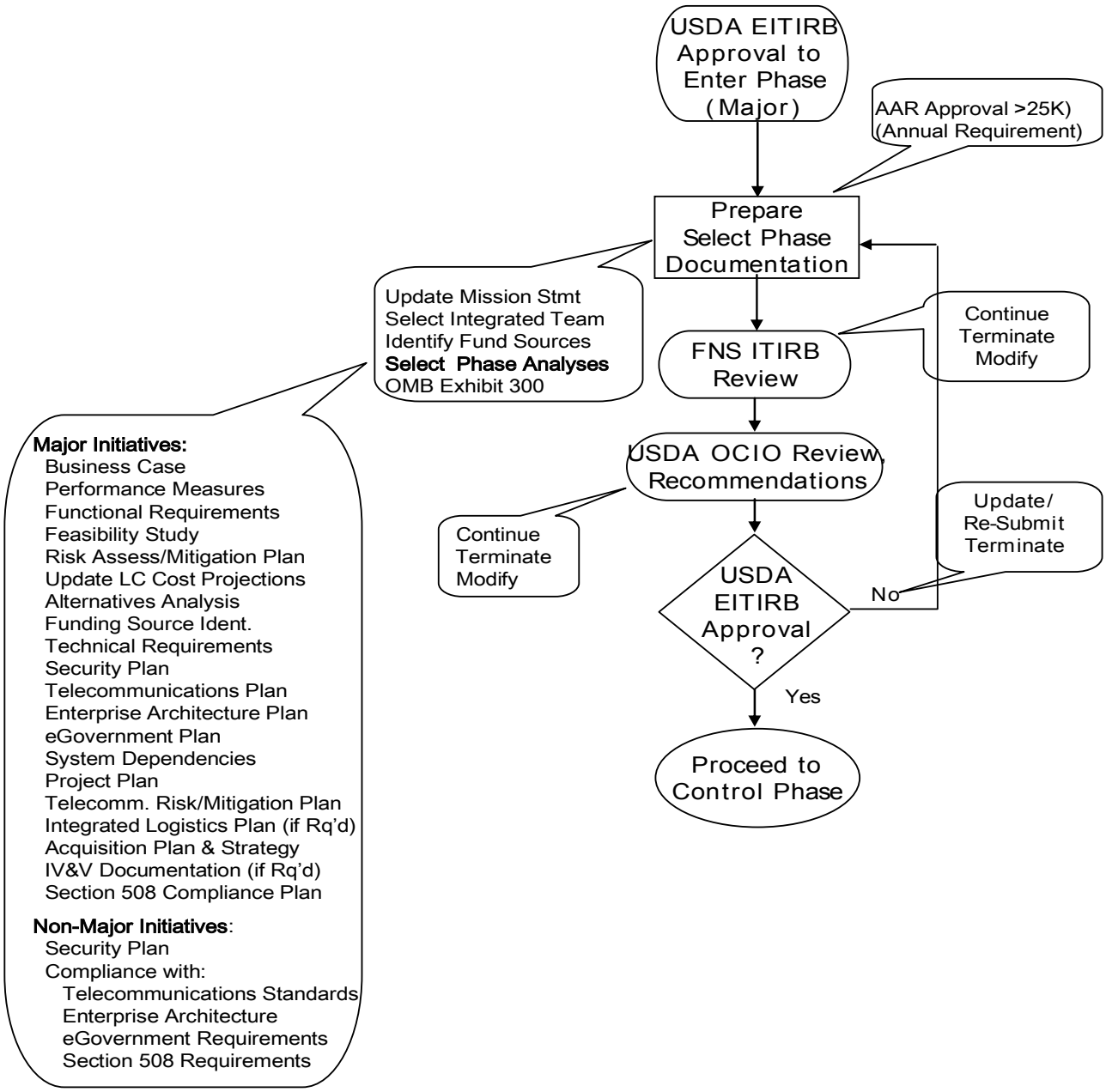
- **Evaluate Phase required documents list:**
  - Stakeholder Impact
  - Progress against Performance measures
  - Baseline goals evaluation
    - Cost
    - Return
    - Funding/Funding Sources
    - Schedule
    - Architecture
    - Accessibility
    - Telecommunications
    - Risk Management
    -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

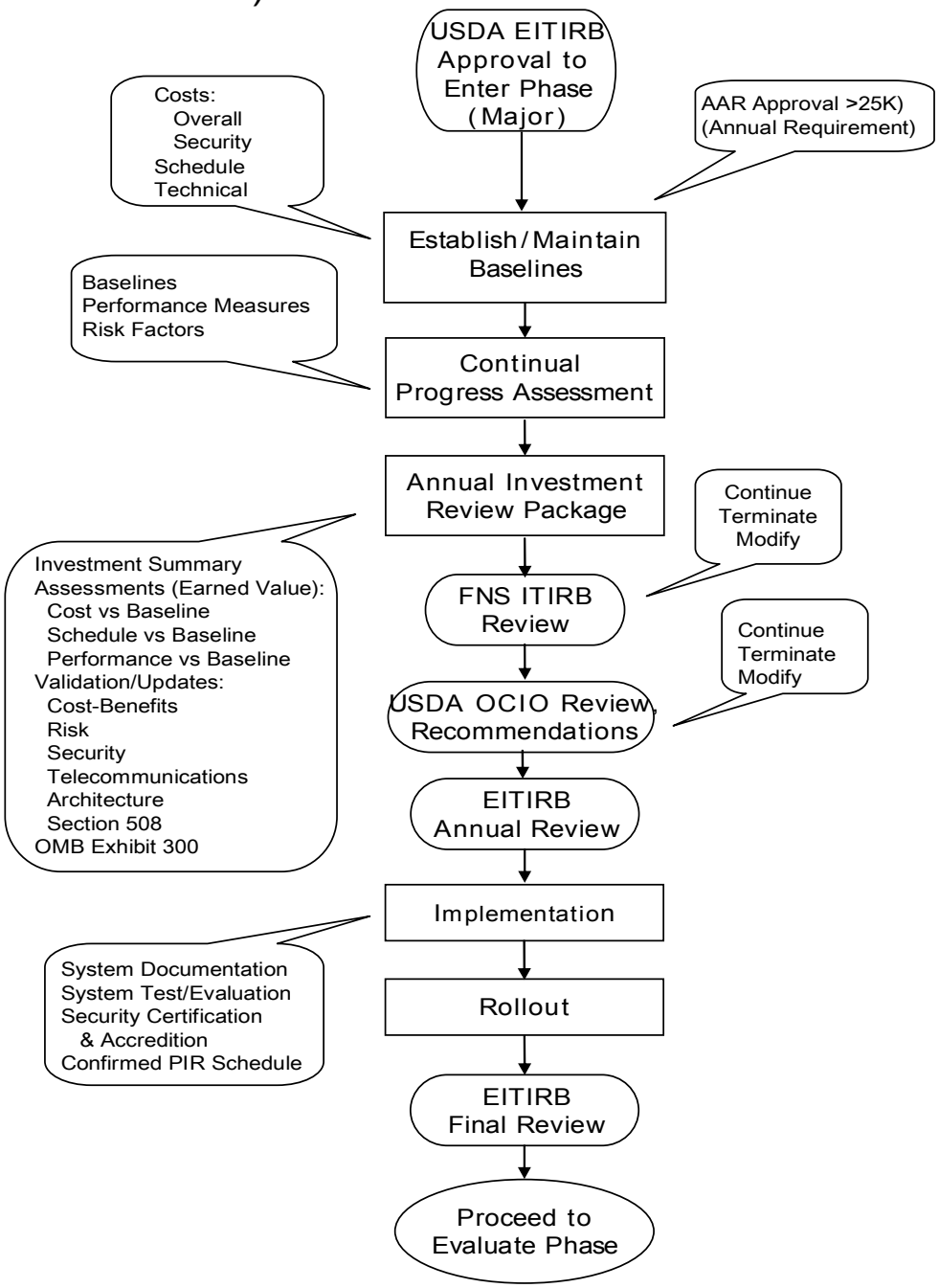
1640 FNCS CPIC Process Flow Diagram (per Phase)



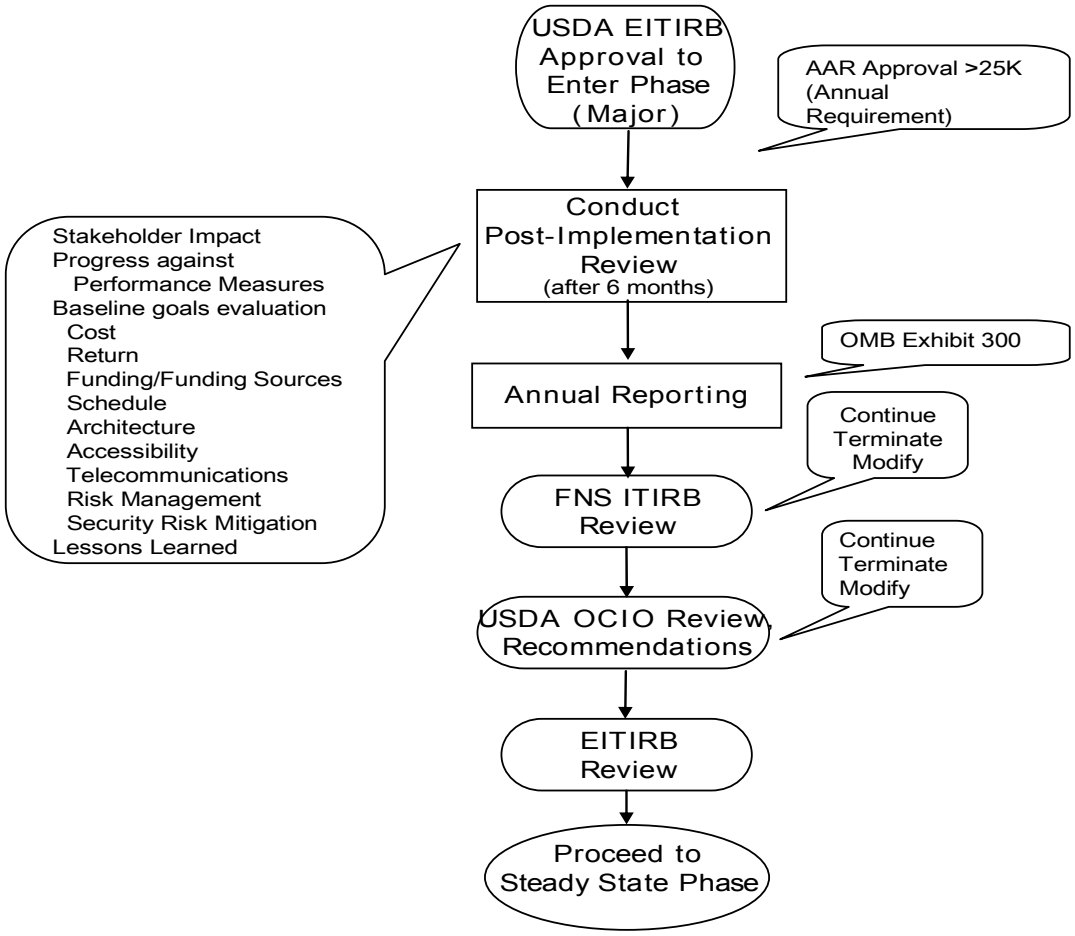
Complete Business Case Development & Approval (Select Phase)



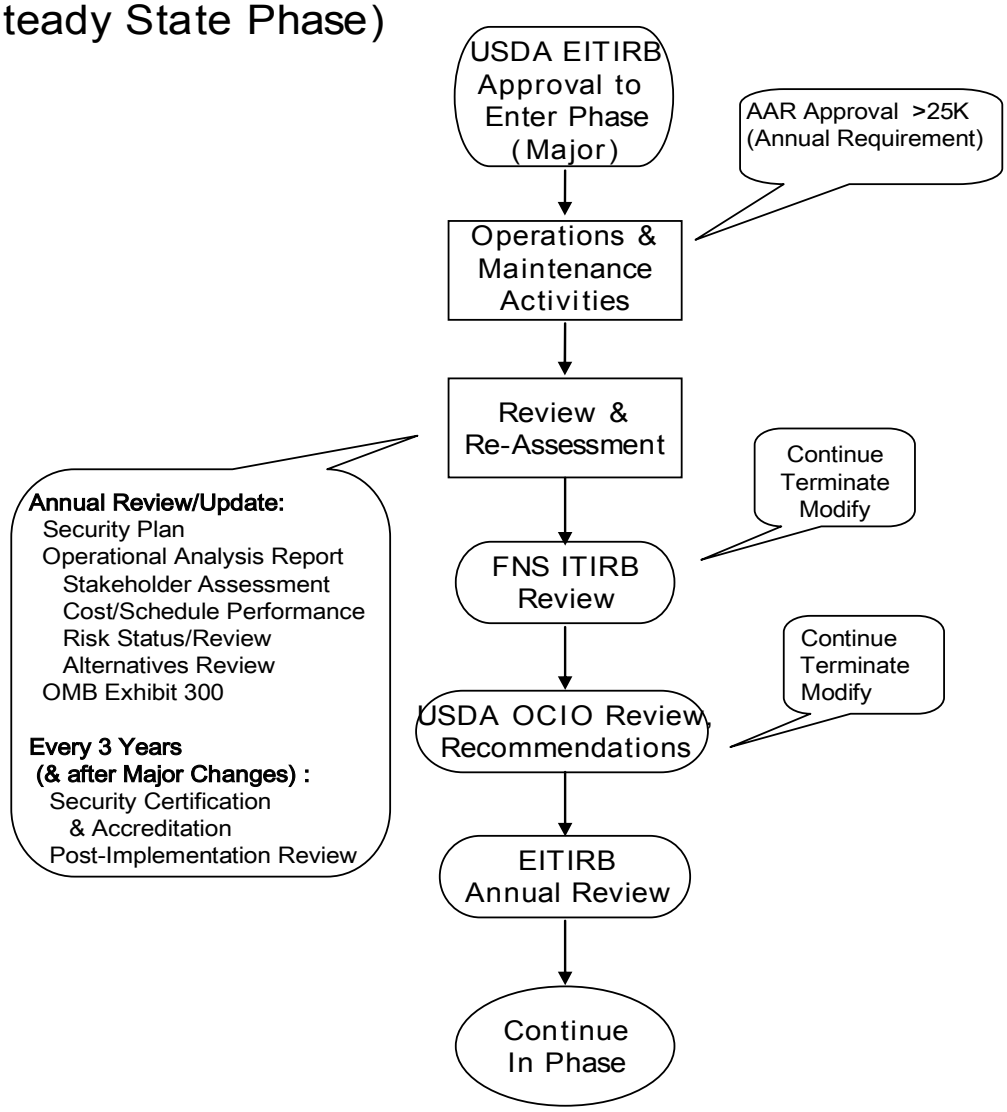
Detailed System Design & Implementation (Control Phase)



Post-Implementation Evaluation (Evaluate Phase)



Continuing Operations and Maintenance (Steady State Phase)



Appendix A FNS 674 Instructions

Please complete as much of the requested information as possible prior to requesting signatures. Birth date and Social Security number are only required for specific users, please read instructions prior to providing this information.
USER NAME (First, Mi, Last) – The first, middle initial, and last name of the person requesting FNS computer system access. Check appropriate box.

USDA E-AUTH ID – Enter your official e-Authentication ID. To obtain an e-Auth ID go to http://www.eauth.egov.usda.gov/index.html and click on “Create an Account”.

DATE OF REQUEST – The date the Computer System Access Request form is submitted.

ORGANIZATION – The name of the organization where the requesting person is employed.

ADDRESS – The street name and number, suite number, city, state and zip code of the FNS organization where the requesting person is employed.

TELEPHONE NUMBER – Enter the area code and seven-digit telephone number.

DATE OF BIRTH – Enter the date of your birth in mm/dd/yyyy format. This information is required for new JP Morgan Boss system users.

SOCIAL SECURITY NUMBER – This must be a valid nine-digit U.S. Social Security Number. This information is required for new NFC system users.

HOME ZIP – Enter zip code from your home address. This information is required for new JP Morgan Boss system users.

E-MAIL – Enter your E-mail address.

SYSTEM ACCESS SECTION – In this section, provide the following information to request access to one or more FNS computer systems. Use additional pages if more space is needed.

SYSTEM NAME – This is the name of the FNS computer system that you need to access.

FORM – Within the above named system there may be specific forms that you need to access. Enter the name of the forms in the space provided.

TYPE OF ACCESS – This determines the type of access for the FORM once it’s displayed on your computer. Access types are FORM specific. Access types are usually Inquiry, Store, Update, and Delete. Please check with your system documentation for all valid Access Types.

ACTION REQUESTED – Enter either Add (to grant access), Delete (to revoke access), or Modify (to change access).

LOGIN ID – Enter your current Login ID for the system you are requesting to access. If this is a new access request and you do not have a Login ID, then leave this area blank.

STATE/LOCALITY CODE(S) – These are FNS organization codes that a particular FNS computer system might require. If required, these codes will determine the information that you can access within the FNS computer system. Check with the system administrator for the FNS computer system in question to determine if these access codes are required.

SYSTEM NAME – This is the name of the FNS computer system that requires Organization Access Codes. In the space provided next to the System Name, enter the Organization Access Codes.

COMMENTS, SPECIAL INSTRUCTIONS – This section of the form can be used to submit comments or instructions to the FNS Security Staff.

APPROVALS – Before any person submits a Computer System Access Request, it must be approved by the requesting person's HQ or Regional Deputy Computer Security Officer. For each system listing in Section 6A, that system's Authorizing Officer must also approve access.

DECISION – The appropriate Official will use this space to mark whether they have approved or denied your Computer System Access Request.

DATE – This is the date of the decision to either approve or deny your Computer System Access Request.

OFFICIALS – This space is used for the appropriate Official to sign their name.

PHONE NUMBER – This is the area code and seven-digit telephone number of the corresponding Official.

DATE RECEIVED/PERSON – This section is for FNS Staff use only.

DATE COMPLETED – This section is for FNS Staff use only.

Appendix B Information Security Staff Contact List

Information Systems Security Program Manager (ISSPM)
Shawn Jones
Office of Information Technology - HQ
Food and Nutrition Service
Phone: (703) 305-2528
e-mail: Shawn.Jones@fns.usda.gov

Information Systems Security Manager (ISSM)
Cord Chase
Office of Information Technology - HQ
Food and Nutrition Service
Phone: (703) 305-2796
e-mail: Cord.Chase@fns.usda.gov

Information Systems Security Officer (ISSO)
Gene Beasley
Benefit Redemption Branch
P.O. Box 135
Minneapolis, MN 55440
Phone: (612) 370-3350
e-mail: Gene.Beasley@fns.usda.gov

Robert Speary
Mid-Atlantic Regional Office
Mercer Corporate Park
300 Corporate Boulevard
Robbinsville, NJ 08691
Phone: (609) 259-5067
e-mail: Robert.Speary@fns.usda.gov
(States: Delaware, District of Columbia, Maryland, New Jersey, Pennsylvania, Puerto Rico, Virginia, Virgin Islands, West Virginia)

John Ferraina
Mid-Atlantic Regional Office
Mercer Corporate Park
300 Corporate Boulevard
Robbinsville, NJ 08691
Phone: (609) 259-5036
e-mail: John.Ferraina@fns.usda.gov
(States: Delaware, District of Columbia, Maryland, New Jersey, Pennsylvania, Puerto Rico, Virginia, Virgin Islands, West Virginia)

Scott Veling
Northeast Regional Office
10 Causeway Street, Room 501
Boston, MA 02222
Phone: (617) 565-4677

e-mail: Scott.Veling@fns.usda.gov
(States: Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, Vermont)

Lori Lodato
Northeast Regional Office
10 Causeway Street, Room 501
Boston, MA 02222
Phone: (617) 565-6483
e-mail: Lori.Lodato@fns.usda.gov
(States: Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, Vermont)

Owen Daniels
Midwest Regional Office
77 West Jackson Boulevard, 20th Floor
Chicago, IL 60604
Phone: (312) 353-2796
e-mail: Owen.Daniels@fns.usda.gov
(States: Illinois, Indiana, Michigan, Minnesota, Ohio, Wisconsin)

Stephanie Means
Midwest Regional Office
77 West Jackson Boulevard, 20th Floor
Chicago, IL 60604
Phone: (312) 353-7270
e-mail: Stephanie.Means@fns.usda.gov
(States: Illinois, Indiana, Michigan, Minnesota, Ohio, Wisconsin)

David Lee
Southeast Regional Office
61 Forsyth Street, SW Room 8T36
Atlanta, GA 30303
Phone: (404) 562-1825
e-mail: David.Lee@fns.usda.gov
(States: Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee)

Reginald Rice
Southeast Regional Office
61 Forsyth Street, SW Room 8T36
Atlanta, GA 30303
Phone: (404) 562-1819
e-mail: Reginald.Rice@fns.usda.gov
(States: Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee)

Brenda Komloske
Mountain Plains Regional Office
1244 Speer Boulevard, Suite 903
Denver, CO 80204

Phone: (303) 844-0321
e-mail: Brenda.Komloske@fns.usda.gov
(States: Colorado, Iowa, Kansas, Missouri, Montana, Nebraska, North Dakota, South Dakota, Utah, Wyoming)

Bonnie Mullins
Mountain Plains Regional Office
1244 Speer Boulevard, Suite 903
Denver, CO 80204
Phone: (303) 844-0325
e-mail: Bonnie.Mullins@fns.usda.gov
(States: Colorado, Iowa, Kansas, Missouri, Montana, Nebraska, North Dakota, South Dakota, Utah, Wyoming)

Paul Ruppi
Southwest Regional Office
1100 Commerce Street, Room 555
Dallas, TX 75242
Phone: (214) 290-9810
e-mail: Paul.Ruppi@fns.usda.gov
(States: Arkansas, Louisiana, New Mexico, Oklahoma, Texas)

Charlene Grundhoffer
Southwest Regional Office
1100 Commerce Street, Room 555
Dallas, TX 75242
Phone: (214) 290-9810
e-mail: Charlene.Grundhoffer@fns.usda.gov
(States: Arkansas, Louisiana, New Mexico, Oklahoma, Texas)

Chuck Hendricks
Western Regional Office
550 Kearny Street, Room 400
San Francisco, CA 94108
Phone: (415) 705-1328
e-mail: Chuck.Hendricks@fns.usda.gov
(States: Alaska, Arizona, California, Hawaii, Idaho, Nevada, Oregon, Washington, Guam Trust Territories, Commonwealth of the Northern Mariana Islands, America Samoa)

Annie Chow
Western Regional Office
550 Kearny Street, Room 400
San Francisco, CA 94108
Phone: (415) 705-1328
e-mail: Annie.Chow@fns.usda.gov
(States: Alaska, Arizona, California, Hawaii, Idaho, Nevada, Oregon, Washington, Guam Trust Territories, Commonwealth of the Northern Mariana Islands, America Samoa)

Appendix C Password Hints

1. Password Protection Standards

All passwords are to be treated as sensitive, confidential information. Your password should not be easy to guess.

2. Be sure to memorize your passwords.

Passwords should never be written down or stored online. You should never share your password with anyone.

3. Choosing Your Password:

Passwords are more secure if they are hard to guess by hackers and strangers.

Passwords must meet the following requirements:

- Contain a minimum of twelve (12) characters
- Contain at least three of the following character sets: upper case; lower case; numeric characters; special non-alphanumeric characters such as # & % ! @ ( ).
- Not contain any simple pattern of letters of numbers such as “aaabbbccc” or “qwertyui.”
- Not easy to guess e.g., “my family name” or a birth date or a street address.
- No words in any language, slang, jargon or found in a dictionary.
- Using a favorite quotation using upper case, lower case, and punctuation will make your password more secure and also easier to remember. Some examples follow:
    - "Once upon a midnight dreary, while I pondered, ..."Ouamdwip,.”
    - "T'was the night before Christmas and all, ..."Ttnbcaa…”
    - "I'd walk a mile for a camel," “Iwamfac,!!”

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 can be extremely difficult to either guess or crack.

Appendix D – Required C&A System Security Documents

Document	Description	References
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 "Syscat" from the ASSERT tool is acceptable for meeting this requirement. Unique Project Identifier (UPI) codes must be included in the SCD of ASSERT 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 Test and Evaluation (ST&E) Plan	The ST&E plan should contain detailed procedures and/or checklists for validating the implementation of each required security control.	NIST SP 800-53
ST&E Report	The ST&E report contains results of functional and security testing conducted on the system as required by the security categorization.	NIST SP 800-53
Security Assessment Report (SAR)	The format and content of the security assessment (ST&E) 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	NIST SP 800-34 DM 3570-001

Document	Description	References
	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 records notice (SORN) 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.)	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.	

Document	Description	References
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 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.	NIST SP 800-25 NIST SP 800-53 Rev 1 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 FNS Risk Management Acceptance Report

<table>
<tr><td colspan="3">RISK MANAGEMENT ACCEPTANCE REPORT</td><td>Report Date:
_____</td></tr>
<tr><td colspan="3">Risk Number: _____</td><td>Date Risk Was Identified:
_____</td></tr>
<tr><td colspan="3">Originator: (Who identified the risk?)</td><td></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">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>
<tr><td colspan="4">Future Mitigation: (Describe any plans/system changes that would mitigate this risk in the future.)</td></tr>
<tr><td colspan="2">Approximate Completion Date:</td><td colspan="2">Actual Closing Date:</td></tr>
<tr><td colspan="4">Primary Contact Name:</td></tr>
<tr><td colspan="3">Primary Contact Signature:
_____</td><td>Date Approved:
_____</td></tr>
<tr><td colspan="4">System Owner's Name:</td></tr>
<tr><td colspan="3">System Owner's Signature:
_____</td><td>Date Approved:
_____</td></tr>
<tr><td colspan="4">ISSPM Concur by Name:</td></tr>
<tr><td colspan="3">Approval (Concur) Signature:
_____</td><td>Date Approved:
_____</td></tr>
</table>

FNS Risk Management Acceptance Report Instructions

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

- **Report Date:** Fill in the date of the report.
- **Risk Number:** Leave this field blank. The number will be assigned by FNS.
- **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 FNS 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 can not 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 FNS 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 Major Application System Security Plan Checklist

Requirement[1]	Yes	No	Comments
Is there a System Security Plan (SSP), and does the plan describe the function or purpose of the application and the information processed?			
Does the plan describe the processing flow of the application from system input to system output?			
Does the plan provide a general description of the technical system?			
Does it include any environmental or technical factors that raise special security concerns (e.g., dial-up lines, open network, etc.)?			
Does the plan describe the primary computing platform(s) used and the principal system components, including hardware, software, and communications resources?			
Does the plan list interconnected systems and system identifiers?			
Does the plan require that written authorization such as Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) be obtained prior to connection with other systems and/or sharing sensitive data/information?			
Does the plan describe, in general terms, the information handled by the system and the need for protective measures?			
Does the plan describe the risk assessment methodology used to identify the threats and vulnerabilities of the system?			
If there is no system risk assessment, does it include a milestone date (month and year) for completion of the assessment?			
Does the plan discuss performance measures that should be established around criteria such as Level of System			

[1] These criteria were derived from NIST 800-18, *Guide for Developing Security Plans for Information Technology Systems*.

Requirement[1]	Yes	No	Comments
Compromises, Timeliness of User Administration and Overall System Availability or other measures that reflect security?			
Does the plan include a set of rules of behavior, and does it contain a signature page to acknowledge receipt?			
Do the rules of behavior clearly delineate responsibilities and expected behavior of all individuals with access to the system, state the consequences of inconsistent behavior or non-compliance, and include appropriate limits on interconnections to other systems?			
Does the plan state which phase of the life cycle the system or parts of the system are in?			
Does the plan provide the date of authorization, name, and title of management official authorizing processing in the system?			
If not authorized, is the name and title of manager requesting approval to operate and date of request, provided?			
Does the plan state if all positions have been reviewed for sensitivity level?			
Does the plan state if individuals have received background screenings appropriate for the position to which they are assigned?			
Does the plan address the physical security measures provided for the system and the facility in which it is housed in accordance with the Cyber Security Manual, Chapter 2?			
Does the plan address physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, and interception of data, mobile and portable systems?			
Does the plan describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling			

Requirement[1]	Yes	No	Comments
and distribution procedures for the information and media (discuss user support, audit trails, restricting access to output products, external labeling, and controlling storage)?			
Does the plan discuss if the application software is developed in-house or under contract?			
Does the plan discuss whether the government owns the software? Was it received from another agency?			
Does the plan discuss whether the application software is a copyrighted commercial off-the-shelf product or shareware?			
Does it describe whether it has been properly licensed with enough copies purchased for all systems?			
Does the plan discuss virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?			
Does the plan discuss whether intrusion detection tools are installed on the system?			
Does the plan discuss whether penetration testing is performed on the system?			
Does the plan's discussion of documentation for the system include descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security in the application and support systems(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures?			
Does it list the documentation maintained for the application (e.g., vendor documentation of hardware/software, functional requirements, security plan, general system security plan, application program manuals, test results documents,			

Requirement[1]	Yes	No	Comments
standard operating procedures, emergency procedures, contingency plans, user rules/procedures, risk assessment, certification/accreditation statements/documents, and verification reviews/site inspections)?			
Does the plan describe the awareness program for the system (e.g., posters, booklets, and trinkets)?			
Does the plan describe the major application's authentication control mechanisms and the method of user authentication?			
Does the plan describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user ID that is assigned to a single person)?			
Does the plan discuss the controls in place to authorize or restrict the activities of users and system personnel within the application?			
Does the plan describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users?			
Does the plan discuss if the public accesses the major application?			
Does the plan discuss the audit trail support accountability by providing a trace of user actions?			
Does the plan discuss audit trails designed and implemented to record appropriate information that can assist in intrusion detection?			

Evaluator Comments
(Information Security Office)

Evaluator Recommendations
(Information Security Office)

Evaluator Signature Date

Appendix G GSS System Security Plan Checklist

Requirements	Yes	No	Comments
Does the plan list any independent security reviews conducted on the system in the last three years?			
Does the plan include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings and the actions taken as a result?			
Does the plan describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable (agreements for backup, documented backup procedures, location of stored backups, tested contingency/disaster recovery plans)?			
Does the plan discuss restriction/controls on those who perform maintenance and repair activities and special procedures for performance of emergency repair and maintenance?			
Does the plan discuss version control that allows association of system components to the appropriate system version?			
Does the plan discuss procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production?			

Requirements	Yes	No	Comments
Does the plan discuss change identification, approval, and documentation procedures?			
Does the plan describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends?			
Does the plan describe the type and frequency of application-specific and general support system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the job training)?			
Does the plan describe the level of enforcement of the access control mechanism (network, operating system, and application)?			
Does the plan discuss if there are procedures for reporting incidents handled either by system personnel or externally?			
Does the plan describe the method of user authentication (e.g., password, token, and biometrics)?			

Evaluator Comments
(Information Security Office)

Evaluator Recommendations
(Information Security Office)

Evaluator Signature Date

Appendix H - 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 Office 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 FNS managers and, when appropriate, the FNCS ITIRB.

PMO 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 I CPO-ITIRB Recommendation

PMO ITIRB RECOMMENDATION		
Requirement Title:	**Originating Office**	**Process Consultant**
Description		
Technical Feasibility – Can the requirement be technically capable?		
Technical Alternatives – Have feasible alternatives been considered?		
Technical Compatibility – Does the requirement technically fit within the structure of the agency? Does the requirement align with the current enterprise architecture?		
Resources – Does the requirement require funding and personnel resources beyond the capability of the agency		
Other – Does the requirement already exist, etc.?		
Recommendation		
Forward to ITIRB □	Refer to ITD □	Return to Originator □
Comments Supporting Recommendation		
Reviewed by:		
PMO		
Chief, IAB		
Approved by:		
CIO		

Glossary of Terms

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. BACK
ACCESS CONTROL	Measures imposed to limit to the exposure of Information Technology resources to only authorized users, programs, processes or other systems. BACK
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. BACK
ACCREDITATION	A written statement of certification by designated technical personnel that the system meets established technical requirements that provide an approved level of system security. BACK
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. BACK

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 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. BACK
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. BACK
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 BACK
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). BACK
AVAILABILITY	The fractional amount of time that a system provides the services and meets the mission requirements for which it is designed and operated. BACK
BACKGROUND INVESTIGATION	Review into a person's past in the determination of granting a security clearance. BACK

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 analyze 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. BACK
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. BACK
CAPITAL PLANNING AND INVESTMENT CONTROL	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 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. BACK

CERTIFICATION	The technical evaluation that establishes the compliance of a computer system, application, or network design and implementation with prescribed security requirements. BACK
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. BACK
CLASSIFICATION	Designation of the sensitivity level of an entity (i.e. sensitive, unclassified). BACK
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. BACK
COLD SITE	A facility designated for emergency backup operations of another system but not in operation until staffed and uploaded for that task. BACK
CONFIDENTIALITY	The physical and electronic condition that protects information and data from unauthorized disclosure. BACK
CONFIGURATION MANAGEMENT	Oversight activities for changes and enhancements to the FNCS system's hardware, firmware, software, and documentation to ensure that unintentional modifications do not occur. BACK
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. BACK
CONTINUITY OF OPERATIONS PLAN (COOP)	A plan developed to support the organization in case of a protracted infrastructure problem when relocation is 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. BACK
CONTROLLED AREAS	The areas within the FNCS facility where access is monitored and restricted to authorized personnel. BACK
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. BACK

COMMERCIAL WIRELESS	Devices, Services and Technologies commercially procured and intended for use in commercial and unlicensed frequency bands, e.g., Starbucks, airports. BACK
COMPROMISE	The disclosure of information to persons who are not authorized access thereto. BACK
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. BACK
DATA	A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by humans or by Information Technology resources. BACK
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. BACK
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. BACK
DECRYPT	To convert, by use of the appropriate key, encrypted (encoded or enciphered) text into its equivalent plain text. BACK
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. BACK
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. BACK
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. BACK
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. BACK
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. BACK
EMERGENCY/INCIDENT RESPONSE	The prompt and effective reaction to disruptions in normal processing activities through preplanned, measured steps. BACK

EMPLOYEE PERSONAL TIME	Non-Work Hours. Employees may use government office 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). BACK
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. BACK
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. BACK
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. BACK
FIRMWARE	Logic circuits in read-only memory that can be altered by software under certain circumstances.
FIREWALL	A firewall is a device or devices that guards the entrance to a private network and keeps out unauthorized or unwanted traffic. BACK
GATEWAY	The interface between electronic mail environments to facilitate the exchange of messages and attachments despite the size and type of message content. BACK
GENERAL SUPPORT SYSTEM	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). BACK
GOVERNMENT OFF-THE-SHELF	Software developed by the government. This software is a standard product, not developed for a particular government project.
GOE – Government-Owned Equipment	Any government issued equipment, issued by FNCS or USDA. BACK
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. BACK
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 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. BACK
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. BACK
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. BACK
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. BACK
INTEGRITY	The quality of data that ensures the continuity of its format, content, and veracity. BACK
INTERNET	The collection of worldwide "network of networks" that use the TCP/IP protocol suite for communications. BACK
INTRANET	A network internal to the organization that is based on TCP/IP protocols. BACK
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. BACK
NETWORK	A communication medium including all components connected to that medium (computers, routers, controllers, packet switches, etc.) used for the transference of information. BACK
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. BACK

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*. BACK
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. BACK
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. BACK
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. BACK
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 crackable passwords. BACK

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. BACK
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. BACK
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. BACK
PERFORMANCE MEASUREMENT	The use of measures for monitoring and assessing progress toward an effective Information Systems Security Program. BACK
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. BACK

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 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). BACK
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. BACK
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. BACK
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. BACK
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. BACK
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. BACK
QUALITATIVE RISK ASSESSMENT	A methodology used to assess risk based on descriptions and rankings. BACK
QUANTITATIVE RISK ASSESSMENT	A methodology used to assess risk based on computational means. BACK
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. BACK

REMOVABLE STORAGE MEDIA	USB/Flash drive, External hard drive, CD and DVD, Floppy Disks and Back-up Tapes BACK
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. BACK
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. BACK
RISK MANAGEMENT	Process concerned with the identification, measurement, safeguard, and control of security risks in the FNCS system. BACK
RISK MITIGATION	The selection and implementation of security controls to reduce risk to a level acceptable to management. BACK
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. BACK
SECURITY	Measures, safeguards and controls that ensure confidentiality, integrity, availability, and accountability of information transmitted, processed, and stored on FNCS IT systems. BACK
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. BACK
SECURITY CERTIFICATION	A formal testing of the security safeguards implemented in and about the computer system to determine whether it meets applicable requirements and specifications. BACK
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. BACK
SECURITY MANAGEMENT	Supporting services that oversee to the protection of Information and resources in accordance with applicable security Guidance. BACK
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. BACK

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. BACK
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." BACK
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. BACK
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. BACK

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. BACK
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 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. BACK
SPECIALIZED (CUSTOM) SYSTEMS	Software that is developed for a specific function/project by a vendor or internal source. BACK
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). BACK
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. BACK
SYSTEM INTERCONNECTION	The state of systems being mutually connected to each other. BACK
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. BACK
SYSTEM SECURITY PLAN	A formal document that fully describes the in place security features and procedures and the planned security tasks required to meet security requirements and eventualities. BACK
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. BACK

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. BACK
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". BACK
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. BACK
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. BACK
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). BACK
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. BACK
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. BACK
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. BACK
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). BACK

Wi-Fi	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. BACK
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. BACK
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. BACK
WLAN – Wireless LAN	A wireless LAN (or WLAN, for wireless local area network, 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. BACK
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. BACK

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. BACK