



OCIO-ITS Security Policy Manual

Office of the Chief Information Officer (OCIO), Information Technology Services (ITS)

- Farm Service Agency
- Natural Resources Conservation Service
- Rural Development

November 29, 2004

**Administrative Bulletin
DR 3602-001**

**Final
Version 1.0**

UNITED STATES DEPARTMENT OF AGRICULTURE
Office of the Chief Information Officer (OCIO), Information Technology Services (ITS)
Washington, DC 20250

FOR OFFICIAL USE ONLY

Revision History

Release No.	Date	Revision Description
Original Draft Version	09/04/2003	Original Draft
Final Version 1.0	11/29/2004	Incorporated suggestions made by review team.
Final Version 1.0	12/02/2004	Assigned Directives System Numbering scheme for Security documents. Document's first release as an Administrative Bulletin.

Table of Contents

INTRODUCTION TO THE OCIO-ITS SECURITY POLICY MANUAL	1
1. Purpose	1
2. Scope	1
3. Special Instructions/Cancellations	1
4. Authorities	1
a. Executive Branch Policy.....	1
b. Applicable Laws, Guidelines, Regulations, and Guidance Directives.....	2
c. National Institute of Standards and Technology (NIST) Special Publications	4
d. USDA Cyber Security Policy	4
5. OCIO-ITS Security Policy Summary	4
6. Security Policy Administration.....	8
a. Security Policies	8
b. Security Program Plans, Procedures, Standards and Guidelines.....	9
c. Security Administration.....	9
d. Security Violations	9
7. Waiver Requirements	9
8. Roles and Responsibilities	10
a. USDA Associate OCIO for Cyber Security.....	10
b. OCIO-ITS Chief Information Officer (CIO)	10
c. OCIO-ITS Information Systems Security Program Manager (ISSPM).....	10
d. Senior Management, Line Managers, Division Directors, System Managers, and Supervisors	11
e. System, Network, and Firewall Administrators.....	11
f. End Users.....	12
1. CHAPTER ONE: ACCEPTABLE USE SECURITY POLICY	14
a. General Policy Statement	14
b. Policy Detail	14
(1). Official Business.....	14
(2). Rules of Behavior	14
(3). Personal Use	15
(4). E-Mail Use.....	16
(5). Internet Use.....	17
2. CHAPTER TWO: AUDIT SECURITY POLICY	19
a. General Policy Statement	19
b. Policy Detail	19
(1). Security Audit.....	19
(2). Security Audit Follow-Up	20
3. CHAPTER THREE: AUTHORIZATION AND ACCESS CONTROL SECURITY POLICY	21
a. General Policy Statement	21
b. Policy Detail	21
(1). Authorization and Access Guidelines.....	21
(2). User Account and Password Guidelines	21
(3). Administrative and Non-User Account and Password Guidelines	23
(4). Periodic Validation of User Access and Account Privileges	24
(5). Administrative Guidance for User Passwords	25
4. CHAPTER FOUR: CAPITAL PLANNING AND INVESTMENT CONTROL (CPIC) SECURITY POLICY	26

a.	General Policy Statement	26
b.	Policy Detail	26
5.	CHAPTER FIVE: CERTIFICATION AND ACCREDITATION SECURITY POLICY	27
a.	General Policy Statement	27
b.	Policy Detail	27
(1).	Security Certification and Accreditation.....	27
(2).	Federal Information Security Management Act.....	27
(3).	Certification and Accreditation Program	27
(4).	Identification of Included Information Systems	27
(5).	Participation.....	27
(6).	Site Certification and Accreditation.....	28
(7).	New Information Systems	28
(8).	Commercial Off-The-Shelf and Government Off-The-Shelf Applications	28
(9).	Existing and Outdated Information Systems	28
(10).	Periodic Review of Information Systems	28
(11).	Non-OCIO-ITS Systems.....	28
(12).	Non-OCIO-ITS Sites and Facilities	29
6.	CHAPTER SIX: CONTINGENCY AND DISASTER RECOVERY SECURITY POLICY	30
a.	General Policy Statement	30
b.	Policy Detail	30
(1).	Contingency and Disaster Recovery Planning.....	30
(2).	Alternate Operating Capability, System Redundancy, and Back-Up/Recovery	31
7.	CHAPTER SEVEN: DATA MANAGEMENT SECURITY POLICY	33
a.	General Policy Statement	33
b.	Policy Detail	33
(1).	Data Security	33
(2).	Data Usage.....	34
(3).	Data Ownership	34
(4).	Data Media Marking.....	34
(5).	Data Protection	34
(6).	Data Sharing	35
(7).	Data Transmission	35
(8).	Data Storage.....	35
(9).	Data Disposal.....	35
(10).	Data Content	35
(11).	Data Classification.....	35
8.	CHAPTER EIGHT: FIREWALL MANAGEMENT SECURITY POLICY	36
a.	General Policy Statement	36
b.	Policy Detail	36
(1).	Firewall Protocols.....	36
(2).	Firewall Management Access.....	36
(3).	Firewall Configuration.....	36
(4).	Firewall Physical Security	37
(5).	Firewall Logs.....	37
(6).	Incident Reporting	37
9.	CHAPTER NINE: GOVERNMENT-OWNED LAPTOP COMPUTERS AND PED SECURITY POLICY	38
a.	General Policy Statement	38

b.	Policy Detail	38
(1).	Classification of Government-Owned Laptop Computers.....	38
(2).	Government-Owned Laptop Computer Security	38
(3).	Government-Owned Portable Electronic Devices (PED)	40
10.	CHAPTER TEN: INCIDENT IDENTIFICATION, DECLARATION, REPORTING, AND HANDLING SECURITY POLICY.....	42
a.	General Policy Statement	42
b.	Policy Detail	42
(1).	Computer Security Incidents.....	42
(2).	Reporting Process	43
11.	CHAPTER ELEVEN: INFORMATION CLASSIFICATION SECURITY POLICY.....	44
a.	General Policy Statement	44
b.	Policy Detail	44
(1).	Sensitive But Unclassified (SBU) Information Protection	44
(2).	For Official Use Only (FOUO) Information Protection.....	45
(3).	Encryption	45
12.	CHAPTER TWELVE: INTRUSION DETECTION MANAGEMENT SECURITY POLICY.....	48
a.	General Policy Statement	48
b.	Policy Detail	48
(1).	IDS Access.....	48
(2).	IDS Configuration Standards.....	48
(3).	IDS Physical Security	48
(4).	IDS Logs.....	48
(5).	IDS Implementation.....	49
(6).	Change Request	49
13.	CHAPTER THIRTEEN: MEDIA SANITATION AND DISPOSAL SECURITY POLICY.....	50
a.	General Policy Statement	50
b.	Policy Detail	50
(1).	Sanitization of IT Equipment and Electronic Media.....	50
(2).	Sanitization of Hard Drives	50
(3).	Overwriting Specifications	50
(4).	Degaussing Specifications	51
(5).	Physical Destruction	51
(6).	Sanitization of Other Computer Media.....	51
(7).	Disposal of OCIO-ITS Equipment.....	51
14.	CHAPTER FOURTEEN: NETWORK ACCESS SECURITY POLICY	52
a.	General Policy Statement	52
b.	Policy Detail	52
(1).	Warning Banners	52
(2).	Remote Access.....	52
(3).	Telework.....	54
(4).	Wireless Technology	56
15.	CHAPTER FIFTEEN: NON-GOVERNMENT OWNED LAPTOP COMPUTER AND PED SECURITY POLICY.....	57
a.	General Policy Statement	57
b.	Policy Detail	57

(1).	Non-Government Owned Laptop Computers Security	57
(2).	Non-Government Owned Portable Electronic Devices (PED)	58
16.	CHAPTER SIXTEEN: PATCH MANAGEMENT SECURITY POLICY	59
a.	General Policy Statement	59
b.	Policy Detail	59
(1).	Patch Prioritization and Scheduling	59
(2).	Patch Testing	59
(3).	Change Management	59
(4).	Audit and Assessment	60
(5).	Notification of Users	60
17.	CHAPTER SEVENTEEN: PHYSICAL ACCESS SECURITY POLICY	61
a.	General Policy Statement	61
b.	Policy Detail	61
(1).	Large IT Facility Security Requirements	61
(2).	IT Restricted Space within Large Office IT Facilities	61
(3).	Facility Security for Field Offices	64
18.	CHAPTER EIGHTEEN: PRINTER MANAGEMENT SECURITY POLICY	66
a.	General Policy Statement	66
b.	Policy Detail	66
(1).	Printer Management Access	66
(2).	Waiver and Configuration Change Requests	66
(3).	Network and Multipurpose Printer Services	66
(4).	Special Provisions for Large Scale Printer/Copy Stations	66
(5).	Incident Reporting and Response	67
19.	CHAPTER NINETEEN: PRIVACY IMPACT ASSESSMENT SECURITY POLICY	68
a.	General Policy Statement	68
b.	Policy Detail	68
(1).	Privacy Impact Assessment	68
(2).	SDLC Methodology	68
20.	CHAPTER TWENTY: RISK MANAGEMENT SECURITY POLICY	70
a.	General Policy Statement	70
b.	Policy Detail	70
21.	CHAPTER TWENTY-ONE: ROUTER AND SWITCH MANAGEMENT SECURITY POLICY	71
a.	General Policy Statement	71
b.	Policy Detail	71
(1).	Router and Switch Configuration	71
(2).	Router and Switch Management	71
(3).	Router and Switch Management Access	72
(4).	Router and Switch Information Access	72
(5).	Router and Switch Logs	72
(6).	Change Request	72
(7).	Router and Switch Implementation	72
(8).	Implied Authority	73
(9).	Incident Reporting and Response	73

22. CHAPTER TWENTY-TWO: SECURITY ARCHITECTURE FRAMEWORK MANAGEMENT SECURITY POLICY.....	74
a. General Policy Statement	74
b. Policy Detail	74
23. CHAPTER TWENTY-THREE: SECURITY AWARENESS, TRAINING, AND EDUCATION SECURITY POLICY.....	75
a. General Policy Statement	75
b. Policy Detail	75
24. CHAPTER TWENTY-FOUR: SECURITY PLAN MANAGEMENT SECURITY POLICY.....	76
a. General Policy Statement	76
(1). Federal Requirements	76
(2). Security Plans	76
b. Policy Detail	76
(1). Security Plan Development	76
(2). Determining General Support Systems and Major Applications	77
25. CHAPTER TWENTY-FIVE: SERVER MANAGEMENT SECURITY POLICY	78
a. General Policy Statement	78
b. Policy Detail	78
(1). Server Configuration.....	78
(2). Server Specification Settings	78
(3). Server Management Access.....	79
(4). Server Classification	79
(5). Server Information Access.....	79
(6). Server Logs.....	79
(7). Server Implementation.....	80
(8). Server Change Requests	80
(9). Server Services	80
(10). Implied Authority	80
(11). Incident Reporting and Response	80
26. CHAPTER TWENTY-SIX: SYSTEMS DEVELOPMENT LIFE CYCLE SECURITY POLICY.....	81
a. General Policy Statement	81
b. Policy Detail	81
(1). Initiation Phase	81
(2). Development Phase.....	82
(3). Implementation Phase.....	83
(4). Operations and Maintenance Phase	83
(5). Disposition Phase.....	84
27. CHAPTER TWENTY-SEVEN: VIRUS PROTECTION SECURITY POLICY	85
a. General Policy Statement	85
b. Policy Detail	85
(1). Virus Protected Systems	85
(2). Virus Software Configurations and Scanning Policy.....	85
28. CHAPTER TWENTY-EIGHT: VULNERABILITY SCAN SECURITY POLICY	87
a. General Policy Statement	87
b. Policy Detail	87
(1). New Equipment/Equipment Upgrade	87

(2). Routine Scans 87

APPENDICES 89

Appendix A: Acronyms 89

Appendix B: Definitions 94

Appendix C: OCIO-ITS Security Waiver Form 109

Introduction to the OCIO-ITS Security Policy Manual

INTRODUCTION to the OCIO-ITS SECURITY POLICY MANUAL

1. Purpose

This policy manual establishes policy for the management and administration of information technologies for the United States Department of Agriculture (USDA) Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) that supports the Farm Service Agency (FSA), Natural Resources Conservation Service (NRCS), and Rural Development (RD) including Large Offices (Beltsville, Fort Collins, Fort Worth, Kansas City, Lincoln, Portland, Salt Lake, St. Louis, and Washington D.C. -- hereafter referred to as “Large Offices”) and Service Centers (including State, District, Area, County, and Local Field Service Offices -- hereafter referred to as “Field Offices”), and their partners.

2. Scope

This policy manual is directed to and applies to all Federal employees, partners, Government contractors, and all others responsible for managing, administering, supporting, or accessing information technology for the OCIO-ITS which supports the Service Center Agencies (SCA) including Large Offices, Field Offices, and their partners. Any persons having a position or title listed in the Roles and Responsibilities, Section 8, is required to read, understand, and comply with the content of this policy manual. For the purposes of this policy manual, the Service Center Agencies includes the Farm Service Agency (FSA), Natural Resources Conservation Service (NRCS), and Rural Development (RD) agencies including each of these agencies’ Large Offices and Field Offices. The Service Center Agency partners include conservation districts, state conservation agencies, farmer-elected committees, county extension agents, co-operatives, lenders, realtors, growers associations, and agriculture industry groups.

3. Special Instructions/Cancellations

This policy manual conforms to current Government-wide and USDA policies, standards, and procedures listed in Section 4, Authorities.

Security Policy Replacement

a. Federal and Departmental Security Policy vs. OCIO-ITS Security Policy

Where current or newly-issued Government-wide or USDA policies conflict with this policy manual, those policies will supersede the conflicting sections of this policy manual, which will be amended to conform to Government-wide or USDA policy.

b. OCIO-ITS Security Policy vs. Service Center Agency Security Policy

Where Service Center Agency policy exists on these topics, this policy manual supersedes all previous Service Center Agency security manuals, policies, and guidelines. The OCIO-ITS and the Service Center Agencies shall collaborate on the creation of security policy and resolve any differentiation that may exist. This policy manual shall remain in effect until superseded by a signed policy manual with adequate authority and scope. This policy manual shall accept signed authority amendments.

4. Authorities

a. Executive Branch Policy

This policy is established through directives published by the OMB based on the applicable laws passed by congress and includes the following policy issuances:

Introduction to the OCIO-ITS Security Policy Manual

OMB Circular	Description
A-123, Management Accountability and Control, 21 June 1995	This directive specifies the policies and standards for establishing, assessing, correcting, and reporting on management controls in Federal agencies.
A-127, Financial Management Systems, as revised by Transmittal Memorandum Number 2, June 1999	This directive prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems.
A-130, Appendix III, Security of Federal Automated Information Resources, as revised by Transmittal Memorandum Number 4, 30 November 2000	This directive stipulates that each Agency shall implement a comprehensive automated information security program. The appendix establishes basic managerial and procedural control that shall be included in Federal automated information systems.

b. Applicable Laws, Guidelines, Regulations, and Guidance Directives

A number of laws, policy guidelines, regulations and guidance directives mandate protection of Federal computers and related resources. Federal managers are responsible for familiarity and compliance with applicable legal requirements. Applicable laws passed by congress include:

Authority	Description
Public Law 93-502, Freedom of Information Act (FOIA) of 1980	This law requires that Federal information be made available to the public except under certain specified conditions.
Public Law 99-474, Computer Fraud and Abuse Act of 1986	This law provides for the punishment of individuals who access Federal computer resources without authorization, attempt to exceed access privileges, abuse Government resources, and/or conduct fraud on Government computers.
Public Law 100-235, Computer Security Act of 1987	This law requires Federal agencies to identify those computer systems that process sensitive information, prepare and maintain computer security plans for sensitive systems, and conduct computer security training for users involved in the operation or use of sensitive systems.
Public Law 103-62, Government Performance and Results Act (GPRA) of 1993	This law establishes policies for managing Agency performance of mission, including performance of its practices.
Public Law 104-13, Paperwork Reduction Act of 1995, Revised	This law provides for the administration and management of computer resources.

Introduction to the OCIO-ITS Security Policy Manual

Authority	Description
Public Law 104-106, Clinger-Cohen Act – Information Technology Management Reform Act of 1996	This law improves the acquisition, use, and disposal of Information Technology (IT) by the Federal Government.
Public Law 104-294, National Infrastructure Protection Act of 1996	This law provides for the protection of computer resources.
Public Law 105-277, Government Paperwork Elimination Act (GPEA) of 1998	This law provides for Federal agencies, by October 21, 2003, to give persons who are required to maintain, submit, or disclose information, the option of doing so electronically when practicable as a substitute for paper and to use electronic authentication methods to verify the identity of the sender and the integrity of electronic content.
Executive Order 10450, Security Requirements for Government Employees, April 1953	This order establishes that the interests of national security require all Government employees be trustworthy, of good character, and loyal to the United States.
Executive Order 13011, Federal Information Technology, July 1996	This order establishes policy for the head of each Agency to effectively use information technology to improve mission performance and service to the public.
Executive Order 13103, Computer Software Piracy, October 1998	This order establishes policy that each executive Agency shall work diligently to prevent and combat software piracy in order to give effect to copyrights associated with computer software.
Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 2001	This order establishes policy that ensures protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such information systems.
Presidential Decision Directive 63: Critical Infrastructure Protection, May 1998	This directive requires that the United States take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on critical infrastructures, including our cyber systems.
Paperwork Reduction Act, Revised 1995	This law provides for the administration and management of computer resources.
Privacy Act of 1974, Revised	This law imposes security requirements on agencies that maintain personal information in a “system of records” as defined herein (refer to Public Law 93-579, Privacy Act of 1986).

Introduction to the OCIO-ITS Security Policy Manual

Authority	Description
Federal Managers Financial Integrity Act (FMFIA) of 1982	This law mandates that Federal agencies establish and maintain an internal control program to safeguard data processing resources, assure their accuracy and reliability, and protect the integrity of information resident on such systems.
Federal Financial Management Improvement Act (FFMIA) of 1996	This law mandates Federal agencies to implement and maintain financial management systems that comply substantially with federal systems requirements, federal accounting standards, and the U.S. Government Standard General Ledger (SGL). FFMIA also requires GAO to report annually on the implementation of the act.
Federal Information Security Management Act of 2002 (FISMA), P.L. 107-347, sec. 301-305.	FISMA requires Federal Agencies to establish Agency-wide risk-based information security programs that include periodic risk assessments, use of controls and techniques to comply with information security standards, training requirements, periodic testing and evaluation, reporting, and plans for remedial action, security incident response, and continuity of operations.
Standards of Ethical Conduct for Employees of the Executive Branch, by the U.S. Office of Government Ethics	These standards describe ethical conduct that is expected of each employee occupying a position of public trust.

c. National Institute of Standards and Technology (NIST) Special Publications

Please refer to the current NIST Special Publications website located at <http://csrc.nist.gov/publications/nistpubs/> for current special publications.

d. USDA Cyber Security Policy

Please refer to the current Cyber Security Policy website located at http://www.ocio.net.usda.gov/ocio/cyber_sec/policy.html for current policies and procedures.

5. OCIO-ITS Security Policy Summary

The following is a synopsis of the USDA OCIO-ITS Security Policies exhibited in this manual. The information in this table is defined according to individual policy, scope, and its intended audience.

Introduction to the OCIO-ITS Security Policy Manual

OCIO-ITS Security Policy	Scope	Audience
Chapter 1: Acceptable Use Security Policy	Defines security policy for the acceptable usage of OCIO-ITS information systems including e-mail and Internet use.	OCIO-ITS ISSPM, System Administrators, Network Administrators, Designated State Office Security Liaisons, End Users, Senior Management, Line Managers, Division Directors, System Managers, Supervisors, and all other affected users.
Chapter 2: Audit Security Policy	Defines security policy for the internal and external security audits for systems and applications within the OCIO-ITS network.	OCIO-ITS ISSPM and Senior Management, Line Managers, Division Directors, System Managers, and Supervisors
Chapter 3: Authorization and Access Control Security Policy	Defines security policy for authentication and access control processes for systems and applications within the OCIO-ITS network. This includes password policies for User, Non-User, and Administrative personnel.	OCIO-ITS ISSPM, System Administrators, End Users, and Senior Management, Line Managers, Division Directors, System Managers, and Supervisors
Chapter 4: Capital Planning and Investment Control Process (CPIC) Security Policy	Defines security policy for managing and controlling IT investments and establishing a formal Capital Planning and Investment Control Process for the OCIO-ITS.	OCIO-ITS ISSPM
Chapter 5: Certification and Accreditation Security Policy	Defines security policy for the Certification and Accreditation process for IT systems and applications within the OCIO-ITS network.	OCIO-ITS ISSPM and Senior Management, Line Managers, Division Directors, System Managers, and Supervisors
Chapter 6: Contingency and Disaster Recovery Security Policy	Defines security policy for the disaster recovery processes for OCIO-ITS information resources. Included topics are contingency planning and disaster recovery.	OCIO-ITS ISSPM and Disaster Recovery Coordinators
Chapter 7: Data Management Security Policy	Defines security policy for the management of data within the OCIO-ITS network.	OCIO-ITS ISSPM, Data Managers, and Data Developers

Introduction to the OCIO-ITS Security Policy Manual

OCIO-ITS Security Policy	Scope	Audience
Chapter 8: Firewall Management Security Policy	Defines security policy for the implementation, configuration, and management of firewalls within the OCIO-ITS network.	OCIO-ITS ISSPM, Change Control Board (CCB), and Firewall Administrators
Chapter 9: Government-Owned Laptop Computers and PED Security Policy	Defines security policy for issuing, using, and managing Government-owned laptop computers and Portable Electronic Devices (PED) within the OCIO-ITS network.	OCIO-ITS ISSPM, System Administrators, Network Administrators, Designated State Office Security Liaisons, Laptop Users, and PED Users
Chapter 10: Incident Identification, Declaration, Reporting, and Handling Security Policy	Defines security policy for the identification, declaration, reporting, and handling of IT incidents for OCIO-ITS information resources.	OCIO-ITS ISSPM, Incident Response Team (IRT), Designated State Office Security Liaisons, Security Help Desk, End Users, and Senior Management, Line Managers, Division Directors, System Managers, and Supervisors
Chapter 11: Information Classification Security Policy	Defines security policy for classifying information for OCIO-ITS information resources personnel.	OCIO-ITS ISSPM, System Administrators, and Network Administrators
Chapter 12: Intrusion Detection Management Security Policy	Defines security policy for the implementation, configuration, and management of Intrusion Detection Systems (IDS) within the OCIO-ITS network.	OCIO-ITS ISSPM, Network Administrators, System Administrators, and Senior Management, Line Managers, Division Directors, System Managers, and Supervisors
Chapter 13: Media Sanitization and Disposal Security Policy	Defines security policy for the sanitization and disposal of OCIO-ITS equipment.	OCIO-ITS ISSPM, System Owners, and Designated State Office Security Liaisons
Chapter 14: Network Access Security Policy	Defines security policy for access to OCIO-ITS information resources and networks. This includes remote access, Telework, and internet access points.	OCIO-ITS ISSPM, OCIO-ITS Telecommunications, Network Administrators, System Administrators, Designated State Office Security Liaisons, Remote Access Users, and Telework Supervisors and Participants
Chapter 15: Non-Government Owned Laptop Computer Security Policy	Defines security policy for scanning and managing computer laptops not issued by the Government for operation within the OCIO-ITS networks.	OCIO-ITS ISSPM, Designated State Office Security Liaisons, Security Help Desk, and Non-Government issued Laptop Users

Introduction to the OCIO-ITS Security Policy Manual

OCIO-ITS Security Policy	Scope	Audience
Chapter 16: Patch Management Security Policy	Defines security policy for the patch management process of OCIO-ITS information systems.	OCIO-ITS ISSPM, CCB, CCE, IO Lab, System Administrators, Network Administrators, Designated State Office Security Liaisons
Chapter 17: Physical Access Security Policy	Defines security policy for physical access to OCIO-ITS information resources.	OCIO-ITS ISSPM, CCE, IO Lab, Data Centers, Web Farms, Designated State Office Security Liaisons, IT Personnel, and Senior Management, Line Managers, Division Directors, System Managers, and Supervisors
Chapter 18: Printer Management Security Policy	Defines security policy for securing printers and printing systems for all OCIO-ITS information resources.	OCIO-ITS ISSPM, CCE, IO Lab, Data Centers, Web Farms, Network Administrators, Designated State Office Security Liaisons, and Senior Management, Line Managers, Division Directors, System Managers, and Supervisors
Chapter 19: Privacy Impact Assessment Security Policy	Defines security policy for the Privacy Impact Assessment (PIA) process for systems within the OCIO-ITS network.	OCIO-ITS ISSPM, System Owners, Application Developers, and Privacy Policy Analysts
Chapter 20: Risk Management Security Policy	Defines security policy for the overall risk management process for OCIO-ITS.	OCIO-ITS ISSPM
Chapter 21: Router and Switch Management Security Policy	Defines security policy for the implementation, configuration, and management of routers and switches within the OCIO-ITS network.	OCIO-ITS ISSPM, CCE, IO Lab, Data Centers, Web Farm, System Administrators, and Network Administrators
Chapter 22: Security Architecture Framework Management Security Policy	Defines security policy for the development of a Security Architecture Framework (SAF) for the OCIO-ITS.	OCIO-ITS ISSPM
Chapter 23: Security Awareness, Training, and Education Security Policy	Defines security policy for security awareness and security awareness training within the OCIO-ITS.	OCIO-ITS ISSPM, HR Management, End Users, and Senior Management, Line Managers, Division Directors, System Managers, and Supervisors

Introduction to the OCIO-ITS Security Policy Manual

OCIO-ITS Security Policy	Scope	Audience
Chapter 24: Security Plan Management Security Policy	Defines security policy for the development and maintenance of an Overall Program Security Plan and individual Security Plans for all General Support Systems (GSS) and Major Applications (MA) within the OCIO-ITS.	OCIO-ITS ISSPM
Chapter 25: Server Management Security Policy	Defines security policy for the implementation, configuration, and management of servers within the OCIO-ITS network.	OCIO-ITS ISSPM, CCE, IO Lab, Data Centers, Web Farms, Network Administrators and System Administrators
Chapter 26: Systems Development Life Cycle (SDLC) Security Policy	Defines security policy for the system development life cycle process for systems within the OCIO-ITS network.	OCIO-ITS ISSPM, Data Managers, Application Developers, System Administrators, and Network Administrators
Chapter 27: Virus Protection Security Policy	Defines security policy for implementing, administering, and managing virus protection for systems within the OCIO-ITS network.	OCIO-ITS ISSPM, CCE, IO Lab, Network Administrators, System Administrators, Designated State Office Security Liaisons, and Security Help Desk
Chapter 28: Vulnerability Scan Security Policy	Defines security policy for scanning (routine and new equipment) OCIO-ITS operational networks, systems, and servers.	OCIO-ITS ISSPM, CCB, CCE, IO Lab, Data Centers, Web Farms, Network Administrators, System Administrators, and Designated State Office Security Liaisons

6. Security Policy Administration

a. Security Policies

OCIO-ITS Security Policies are statements made by the OCIO-ITS to establish overall policy on information access and safeguards. These statements include directives to create an information security program, establish its goals, and assign responsibilities. The term policy is also used to refer to the specific security rules for particular systems. Additionally, policy is defined as the documentation of information security decisions. The OCIO-ITS uses three basic types of policies:

- (1). Program Policy
These policies are used to create an information security program.
- (2). Issue-Specific Policies
These policies address specific concerns of the organization.
- (3). System-Specific Policies
These policies focus on decisions taken by management to protect a particular system.

Introduction to the OCIO-ITS Security Policy Manual

b. Security Program Plans, Procedures, Standards and Guidelines

Security program plans, procedures, standards, and guidelines are used to describe how policies will be implemented within the OCIO-ITS. These additional documents will offer users, managers, and others with a clearer approach to implementing policy and meeting organizational goals. Standards and guidelines specify the type of technologies and methodologies to be used to secure systems. Procedures provide additional detailed steps to be followed to accomplish particular security related tasks. Standards, guidelines, and procedures may be promulgated throughout an organization via handbooks, regulations, or manuals. NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, provides more detailed information on the development of procedures, standards and guidelines.

c. Security Administration

The OCIO-ITS ISSPM will administer all programs and projects designed to implement or maintain information security requirements. Administrative activities include, but are not limited to, the following:

- (1). Develop security policies, processes, standards and procedures
- (2). Determine roles and responsibilities for information security within the OCIO-ITS
- (3). Develop and implement information security plans for applications, systems, and operating locations as required by federal regulations and USDA directives
- (4). Evaluate OCIO-ITS infrastructure compliance with information security policies, processes, standards and procedures
- (5). Establish processes and procedures for access to sensitive systems and information
- (6). Establish processes and procedures to minimize the likelihood of disruptions, to recover from disasters, and to respond to security incidents
- (7). Develop programs to increase awareness among OCIO-ITS participants of information security issues and responsibilities
- (8). Develop the information security architecture and apply appropriate standards to secure OCIO-ITS information resources

d. Security Violations

Violation of any provision of OCIO-ITS Security Policies may result in one or more of the following actions:

- (1). Limitation of an individual's access to some or all OCIO-ITS systems
- (2). Disciplinary actions in accordance with USDA policy and the policies of the sponsoring Agency
- (3). Requirement of the violator to provide restitution for any improper use of information/service
- (4). Initiation of legal action by the USDA including, but not limited to, criminal or civil prosecution under appropriate federal laws

7. Waiver Requirements

- a. Any system, function, application, or resource not compliant to OCIO-ITS Security Policies within 30 days past the policy effective date shall require an approved exception waiver.
- b. Requests for exceptions to all OCIO-ITS Security Policies shall require the completion and submission of a waiver package (refer to Appendix C: OCIO-ITS Security Waiver Form) to the OCIO-ITS ISSPM. Waiver packages require OCIO Cyber Security review and approval. Additionally, all waiver packages are subject to review by the OIG and other audit bodies.

Introduction to the OCIO-ITS Security Policy Manual

8. Roles and Responsibilities

a. USDA Associate OCIO for Cyber Security

- (1). Ensures a comprehensive, cost-effective security program is in place to protect OCIO-ITS information systems.
- (2). Works with the OCIO-ITS to develop necessary security functionality.
- (3). Performs reviews of all major information technology investments to ensure that security requirements have been met and costs have been adequately formulated.
- (4). Provides recommendations to Agency CIOs and for security improvements.
- (5). Performs oversight reviews of the OCIO-ITS to ensure compliance with this security policy manual.
- (6). Formulates and publishes policy and procedures for the protection, handling, and storing of OCIO-ITS information.
- (7). Conducts reviews to ensure OCIO-ITS compliance with the policies listed in this security policy manual.

b. OCIO-ITS Chief Information Officer (CIO)

- (1). Responsible for developing and maintaining a comprehensive, state-of-the-art, cost-effective, and automated information system security program for the OCIO-ITS that will assure compliance with established laws, policies, and regulations.
- (2). Delegates the operational responsibility for the Agency information system security program to the ISSPM.
- (3). Staffs and funds the OCIO-ITS Information Security Program to ensure compliance with established and mandated federal laws and OCIO-ITS Security Policies.
- (4). Exercises responsibility for managing, budgeting, directing, supporting, and implementing the program with cooperation and support from all offices.

c. OCIO-ITS Information Systems Security Program Manager (ISSPM)

- (1). Provides overall management, leadership and direction for the OCIO-ITS ISSPMs and deputies.
- (2). Formulates, coordinates, maintains, implements and enforces appropriate security policies and standards to protect information resources from unauthorized access and disclosure.
- (3). Monitors and reports on compliance with federal laws and OCIO-ITS Security Policies.
- (4). Creates, updates, administers, and implements policies and procedures governing the information security practices of all OCIO-ITS participants and information resources.
- (5). Establishes projects and programs within the OCIO-ITS to achieve the information security objectives identified by the federal Government, the USDA Associate OCIO for Cyber Security, and the Agency Chief Information Officers (CIO).
- (6). Assists Agency participants to comply with OCIO-ITS information security policies, processes, standards and procedures.
- (7). Acts as principal point of contact on information systems security activities with the OCIO-ITS management officials, other Federal agencies, and industry.
- (8). Develops and implements a computer security awareness-training program for all employees and contractors.
- (9). Serves as a member of the OCIO-ITS acquisition review team to ensure that adequate and cost-effective security requirements are addressed.
- (10). Participates in internal and external reviews, inspections, and audits to ensure compliance with federal laws and OCIO-ITS Security Policies.
- (11). Monitors management decisions for corrective actions of deficiencies that were identified in audit reports.

Introduction to the OCIO-ITS Security Policy Manual

- (12). Investigates and reports all suspected and actual computer viruses, incidents, breaches and violations to appropriate OCIO-ITS officials, such as the CIO, Federal Protective Service (FPS) and Office of Inspector General (OIG).
- (13). Formulates, coordinates, and publishes the OCIO-ITS Annual Security Plans and the Security Strategic Plan.
- (14). Monitors the usage of wireless technology within the ITS and SCA environments.

d. Senior Management, Line Managers, Division Directors, System Managers, and Supervisors

- (1). Implements and enforces OCIO-ITS Security Policies and procedures to protect information resources within their areas of responsibility.
- (2). Monitors and reports on compliance with Federal laws and OCIO-ITS Security Policies.
- (3). Assists in the development and implementation of a comprehensive risk management program to identify and evaluate security risks and vulnerabilities.
- (4). Promotes and supports computer security awareness training for employees and contractors.
- (5). Reviews proposed procurement requests to ensure that adequate and cost-effective security measures and safeguards are addressed.
- (6). Participates in internal and external reviews and inspections to ensure compliance with established policies and procedures, and monitors the correction of deficiencies identified in audits and reports.
- (7). Issues appropriate instructions needed to implement provisions of information systems security policies and standards.
- (8). Investigates and reports all suspected and actual computer viruses, incidents, violations or attempts to gain unauthorized access to information resources to appropriate officials, such as the immediate supervisor, CIOs, the local information systems security officer, FPS and OIG (if required).

e. System, Network, and Firewall Administrators

- (1). Reads and complies with this OCIO-ITS Security Policy Manual.
- (2). Restricts authorization and access to OCIO-ITS information resources based on a need-to-know basis to enterprise directories, files, and administrative/non-user/user accounts.
- (3). Configures the information resources environment ensuring adequate security measures are in place in accordance with the OCIO-ITS Security Policy Manual.
- (4). Documents and certifies corrective actions for OCIO-ITS information resources have been accurately taken and forwarded to the OCIO-ITS ISSPM for reporting purposes.
- (5). Ensures all information resources are in compliance with this OCIO-ITS Security Policy Manual.
- (6). Ensures all OCIO-ITS information resources have been hardened, configured, and scanned to ensure protection requirements are in place and working properly.
- (7). Implements information system upgrades and patches for OCIO-ITS enterprise resources.
- (8). Monitors and reviews information system events and auditing logs on a timely and consistent basis.
- (9). Participates in establishing security controls for information resources and controlled access and configuration management procedures in accordance with this OCIO-ITS Security Policy Manual.
- (10). Participates in the central management of all OCIO-ITS information resource connections ensuring that users of networking services are fully authenticated.

Introduction to the OCIO-ITS Security Policy Manual

- (11). Actively participates in the preparation of waiver packages for OCIO-ITS information resources as required and promptly identifies the need for waivers for any information resource not in compliance with this OCIO-ITS Security Policy Manual.
- (12). Provides appropriate administrative access and permissions to information resources based in accordance with Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (13). Provides information system, environment, and data recovery support for OCIO-ITS information resources.
- (14). Reports non-compliance of this OCIO-ITS Security Policy Manual in accordance with the Chapter 10: Incident Identification, Declaration, Reporting, and Handling Security Policy or its replacement.
- (15). Requests or performs vulnerability scans for all new or modified systems and equipment prior to deployment into the OCIO-ITS environment.
- (16). Reviews all OCIO-ITS encryption implementations to ensure they comply with this OCIO-ITS Security Policy Manual.
- (17). Verifies appropriate OCIO-ITS security controls are in place using the appropriate checklists.

f. End Users

- (1). Becomes familiar and complies with all established OCIO-ITS Security Policies and practices.
- (2). Learns and adheres to security guidance including local security directives and operating instructions.
- (3). Attends initial security training and participates in annual refresher training as coordinated by their manager and ISSPM.
- (4). Recognizes and reports suspected and actual security incidents to their immediate supervisor, manager, or designated security liaison.
- (5). Protects OCIO-ITS data and resources from unauthorized disclosure, modification, or deletion.
- (6). Marks, protects, and stores Sensitive But Unclassified (SBU) output appropriately.
- (7). Protects all passwords as SBU information and does not attempt to share them.
- (8). Protects all Government-owned equipment and uses antivirus software appropriately.
- (9). Positions computer screens and printers so that casual passersby do not have visual access to sensitive information.
- (10). Locks their assigned workstation (using Alt-Ctrl-Del and selecting "Lock Workstation") or laptop or invokes a password protected screensaver when leaving it unattended for any period of time.
- (11). Protects OCIO-ITS information resources by not downloading streaming video, music, and radio unless designated authorized government business (i.e. IT vendor supported Webcasts are considered government business), as personal use could cause congestion, delay, or disruption of service due to bandwidth constraints.
- (12). Uses the automatic password protected screen saver with a time limit of no greater than 15 minutes.
- (13). Protects OCIO-ITS information resources by not attempting to download or install commercial and business software from the Internet or personally-owned software to their workstation or laptop except where authorized and pre-approved by the ISSPM.
- (14). Protects OCIO-ITS information resources by not attempting to modify or change official hardware or software configuration of workstations or laptops by adding unapproved hardware or software.
- (15). Protects OCIO-ITS information resources by not attempting to bypass any surge protection or power line conditioning devices installed on your system.

Introduction to the OCIO-ITS Security Policy Manual

- (16). Uses access privileges to information systems for the intended purpose only.
- (17). Addresses all security-related questions their supervisor, manager, designated security liaison, or ISSPM for resolution.

Chapter One: Acceptable Use Security Policy

1. CHAPTER ONE: ACCEPTABLE USE SECURITY POLICY

a. General Policy Statement

This policy establishes the acceptable use of USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) information systems that support the Service Center Agencies (SCA) including Large Offices, Field Offices, and their partners. This includes the use of information systems, Internet access, and electronic mail (e-mail). OCIO-ITS information systems provide critical support to the Service Center Agencies. Using OCIO-ITS information resources for inappropriate, unauthorized, or unlawful activities can seriously undermine the ability to accomplish the organizational function. Users shall make every effort to employ OCIO-ITS information resources in an appropriate and acceptable manner, according to the guidelines defined in this policy.

b. Policy Detail

(1). Official Business

- (a). The OCIO-ITS provides information resources to the Service Center Agencies for the purpose of transacting official business. Official business may be defined as any information processing that is required to perform associated work responsibilities.
- (b). Official business includes, but is not limited to, the performance of OCIO-ITS work-related duties in position descriptions, professional training, and tasks directed via contracts and support activities related to contract tasking. However, USDA DR 3300-1 authorizes limited personal use provided this use involves minimal expense to the Government and does not interfere with official business.

(2). Rules of Behavior

Rules of behavior guidelines for the use of OCIO-ITS information systems include, but are not limited to, the following:

- (a). Users shall protect their UserIDs and passwords from disclosure in accordance with Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (b). Participants shall ensure that password resets are performed securely in accordance with Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (c). Users shall change their password if compromised, i.e., someone else knows their password. Users shall immediately notify their supervisor or security administrator for all suspected or confirmed password compromises. Passwords will be changed in accordance with Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (d). Participants shall not program their login or password into automatic script routines or programs in accordance with Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (e). Users shall log off, sign off, or lock the computer system when going to lunch or a break, or any time they leave their computer or terminal.
- (f). Participants shall retrieve all hard-copy printouts in a timely manner. If the originator or receiver of a printout cannot be determined, dispose of it accordingly.
- (g). Users shall inform their supervisor about all sensitive applications or data that will be placed on a system and on any equipment processing sensitive information, so that appropriate security measures can be implemented.
- (h). Participants must not use OCIO-ITS computers or licensed software for personal use beyond those set by the limited personal use policy.

Chapter One: Acceptable Use Security Policy

- (i). Users shall not use personal equipment or software for official business without their supervisor's written approval; sensitive information is not permitted on personal computers.
- (j). Participants will not install or use unauthorized software on OCIO-ITS equipment to include the use of freeware, shareware, or public-domain software without their supervisor's permission and without scanning it for viruses.
- (k). Participants shall comply with local office policy on the use of antivirus software in accordance with Chapter 27: Virus Protection Security Policy or its replacement.
- (l). Users shall observe all software license agreements and will not violate federal copyright laws.
- (m). Participants will not move equipment or exchange system components without their manager's or supervisor's approval.
- (n). OCIO-ITS computer equipment shall be physically protected from hazards such as liquids, food, staples, and paper clips. Refer to Chapter 17: Physical Access Security Policy, or its replacement, for additional information.
- (o). Users shall properly protect and label magnetic media in accordance with Chapter 7: Data Management Security Policy or its replacement.
- (p). Participants must not disclose any dial-in telephone numbers or procedures that permit system access from a remote location. Refer to Chapter 14: Network Access Security Policy, or its replacement, for additional information.
- (q). Users shall not disclose or discuss any OCIO-ITS information, whether sensitive or non-sensitive, with unauthorized individuals. The Privacy Act of 1974, 5 U.S.C. 552a, prohibits such disclosure. Refer to Chapter 11: Information Classification Security Policy, or its replacement, for additional information.
- (r). Participants shall be cognizant of the nature of security incidents and must promptly report them to their supervisor in accordance with Chapter 11: Incident Identification, Declaration, Reporting, and Handling Security Policy or its replacement. Examples include, but are not limited to, unauthorized disclosure of information, computer viruses, theft of equipment, software, or information, inappropriate use, and deliberate alteration or destruction of data or equipment.

(3). Personal Use

- (a). Appropriate Use
Limited personal use of OCIO-ITS information systems is permitted if it is determined that such communication:
 - 1. Does not adversely affect the performance of official duties
 - 2. Are of reasonable duration and frequency
 - 3. Serve a legitimate public interest, such as researching and gathering information from other U.S. Government Agency websites or partner websites.
 - 4. Does not put Federal Government telecommunication systems to uses that would reflect adversely on the OCIO-ITS, to include activities that are illegal, inappropriate, or offensive to fellow employees, partners, contractors or the public.
- (b). Inappropriate Use
Inappropriate personal use of OCIO-ITS information systems include, but are not limited to:
 - 1. Any personal use that could cause congestion, delay, or disruption of service to any Government system or equipment, to include:
 - a. Use of any personal remote access device while connected to any OCIO-ITS LAN to include the use of modems, cellular modems, PDAs, etc.
 - b. Playing online electronic games

Chapter One: Acceptable Use Security Policy

- c. Use of “Push” technology on the Internet and other continuous data streams, i.e., streaming video/music/radio broadcasts, and ticker tape banners such as stock quotes, weather, etc., that would degrade the performance of the entire network
 - d. Creating, copying, transmitting, or retranslating chain letters or other unauthorized mass mailings
 - e. Use of instant messaging to include AOL Instant Messenger, Yahoo Instant Messenger, ICQ, Microsoft, etc.
 - f. Use of peer-to-peer file sharing applications such as Gnutella, KaZaA, Musiccity.com, BearShare, LimeWire, XoloX, Auto galaxy, Direct Connect, ToadNoad, WinMx, Napigator, Morpheus, CuteMx, Scour Exchange, FreeNetfile, eDonkey, and iMesh
2. Activities that are illegal, inappropriate, or offensive to fellow employees, partners, contractors or the public
 3. Creating, downloading, viewing, storing, copying, or transmitting; sexually explicit or sexually oriented materials, material related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities otherwise prohibited
 4. Use of OCIO-ITS information systems for commercial profit-making activities in support of other outside employment or business activities
 5. Engaging in any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity
 6. Use for posting OCIO-ITS information to external newsgroups, bulletin boards, or other public forums without authority
 7. The unauthorized acquisition, use, reproduction, transmission, and distribution of computer software or other material protected by national or international copyright laws, trademarks, or other intellectual property rights
 8. Representing one’s self as someone else
 9. Soliciting Government employees or providing information about or lists of OCIO-ITS employees to others outside the Government without authorization
 10. Interfering with the employee’s job, the jobs of other employees, or the operation of the Internet gateways
 11. Any type of personal solicitation
 12. Modifying Government office equipment for non-Government purposes, including loading personal software or making configuration changes
 13. Intentionally or negligently causing the propagation of viruses, Trojan horses, or other malicious software

(4). E-Mail Use

(a). Appropriate E-Mail Use

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

1. Limited personal use of the OCIO-ITS e-mail system during an employee’s non-work time, such as break times and lunch periods
2. Any message containing information exchanged by employees for the purpose of accomplishing government business
3. Use of the OCIO-ITS e-mail system by authorized users that does not interfere with official business nor reflect adversely on the OCIO-ITS
4. E-mail message forwarding or some other method shall be employed when an addressee is unavailable to receive mail that is required to move business processes

Chapter One: Acceptable Use Security Policy

5. The use of Notepad to open e-mail attached files ending with the extensions .vb, .vbe, .vbs, .wsc, .wsh, .wsf, .pif, .scr, .reg, .js, and jse to limit the spread of various VBScript viruses and worms
 6. Access to the OCIO-ITS e-mail system by users when they are not at their duty station site, or at another installed site, shall only occur through the secured OCIO-ITS dial-up or VPN access points
 7. Transmitting sensitive information that is encrypted and password protected to include, but not limited to, the following:
 - a. Proprietary USDA and OCIO-ITS information
 - b. U.S. Government credit card numbers
 - c. Designated For Official Use Only (FOUO), Sensitive But Unclassified (SBU), or Sensitive Security Information (SSI) information
 - d. Risk assessments, audit findings, or any other documentation containing known OCIO-ITS information system vulnerabilities
 - e. Privacy Act data
 - f. OCIO-ITS network access information to include, but not limited to, IP addresses and local/remote workstation IP addresses, port numbers, dial-in access numbers, or associated system passwords used for gaining entry to networks
- (b). Inappropriate E-Mail Use
1. Inappropriate e-mail use includes, but is not limited to:
 - a. Sharing a UserID and password to obtain access to another user's mail for any purpose
 - b. Opening attached file extensions on OCIO-ITS e-mail servers to include .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, and .shs
 - c. Using a personal Internet Service Provider (ISP) to gain access to the OCIO-ITS e-mail system or for any other system operation or service
 - d. Using wireless service providers outside of OCIO-ITS approved Federal facilities is forbidden
 - e. Transmission of any unencrypted and non-password protected sensitive information
 2. E-mail privileges will be removed immediately if other than acceptable or appropriate use is discovered.

(5). Internet Use

- (a). Appropriate Internet use includes, but is not limited to:
1. Limited personal use of the Internet during an employee's non-worktime
 2. 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
 3. Development of Internet Web-based projects as established by business need
 4. Sharing of information without compromising OCIO-ITS secured data
 5. Exchange of any inter-Agency non-sensitive data in support of departmental mission, OCIO-ITS missions, or other official purposes
 6. Distribution and collection of information related to official program delivery.
 7. Transmitting U.S. Government credit card numbers for legitimate official business, i.e., booking air, car, or hotel information at a secured website for purposes of official Government travel

Chapter One: Acceptable Use Security Policy

(b). Inappropriate Internet Use

Inappropriate Internet use includes, but is not limited to:

1. Purposely visiting adult entertainment, pornographic, and gambling websites
2. Downloading, copying, sharing, or sending software, music videos, movies, or pictures (whether purchased or not purchased) that are not job related as use of these constitutes copyright violations and is a non-business use of limited network bandwidth
3. Peer-to-peer software and file sharing products not expressly identified for authorized use may not be used on or through OCIO-ITS servers and workstations
4. Subscribing to 'list servers', 'use groups', or 'bulletin boards' that do not align to authorized business needs
5. Personal use of streaming video, music and radio consumes bandwidth could cause congestion, delay, or disruption of service due to bandwidth constraints

2. CHAPTER TWO: AUDIT SECURITY POLICY

a. General Policy Statement

This policy establishes the Security Auditing program for information systems (hardware, software, and networks) supporting the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) that supports the , Field Office, and their partners. This policy describes security audit methods required to ensure the confidentiality, integrity, and availability of OCIO-ITS information resources. Security auditing shall be used to detect or investigate actual or attempted security violations in any OCIO-ITS information system by recording security relevant events as they occur. Security auditors, with assistance from administrator staff and other Human Resources (HR) approved personnel, may monitor users or system activities upon the approval of HR and ensure conformance to OCIO-ITS Security Policies based on their findings.

b. Policy Detail

OCIO-ITS Security Auditing will be performed in a two-part process that includes the Security Audit and the Security Audit Follow-Up.

(1). Security Audit

- (a). Security audits shall be conducted on a defined frequency to ensure compliance with established security policy, guidelines, and procedures, and to determine the minimum set of controls required to reduce risk to an acceptable level.
- (b). Audit steps shall include defining the audit scope and objectives, planning the audit, collecting audit data, performing audit tests, reporting for audit results, protecting audit data and tools, making enhancements, and follow-up.
- (c). Security audits for the installation and/or enhancements to a new or existing information system shall be performed prior to implementation to ensure conformance to security policies and procedures.
- (d). Security audits for existing systems shall be conducted on a defined basis by either manual or computerized processes using automated tools to detect security loopholes or vulnerabilities.
- (e). Security audits shall include general control reviews, system reviews, and penetration testing.
- (f). Random audits shall be performed using arbitrary inspections to ensure adherence to OCIO-ITS security policies and procedures.
- (g). Annual assessments of the security of OCIO-ITS information systems shall be performed using guidelines established in the OCIO-ITS Security Procedures Manual, Chapter 2: Audit Security Procedures or its replacement. These assessments will include a review of the resource's audit functions and activities.
- (h). If a security issue is identified during the weekly audit review or through other means, the incident shall be reported in accordance with Chapter 10: Incident Identification, Declaration, Reporting, and Handling Security Policy or its replacement.
- (i). Consistent with their responsibilities for oversight of proper use of OCIO-ITS information systems, the USDA Associate CIO for Cyber Security, the OCIO-ITS CIO, or the OCIO-ITS Information Systems Security Program Manager (ISSPM) may audit any OCIO-ITS information system at any time.
- (j). At a minimum, security audits shall be performed as necessary for backup controls, system and transaction controls, data library procedures, systems development standards, physical security of information systems, contingency plans, and database management.

Chapter Two: Audit Security Policy

- (k). Audit Logs of information systems shall be reviewed on a weekly basis. Established reporting mechanisms shall be used to convey the results of the weekly audit. Audit logs shall be archived on a weekly basis and shall be retained until deemed unnecessary. Audit logs no longer needed may be disposed of as defined in Chapter 13: Media Sanitation and Disposal Security Policy or its replacement.
- (l). OCIO-ITS information systems shall incorporate capabilities to log resource use with all logged activities identified by date and time of occurrence. Logs of activities related to the use of information systems shall be protected at the same level of the information being processed by the resource and released only to authorized individuals.
- (m). Audit reports shall contain sufficient information to enable the review staff, with no previous connection with the audit, to ascertain the evidence that supports the auditors' significant conclusions and judgments.

(2). Security Audit Follow-Up

- (a). The effective implementation of audit recommendations is a major benefit of security auditing. When a security auditor provides a recommendation, management is responsible for placing it into practice. If management has made the decision to not implement a recommendation for medium and high-risks, they may accept the associated security risk. This acceptance of the risk(s) must be documented and signed by the appropriate level of management.
- (b). The two major areas of concern with regard to recommendations made in the security risk assessment and audit include:
 - 1. Effective and qualified recommendations presented by security auditors
 - 2. Monitoring and follow-up of security audit results by management

3. CHAPTER THREE: AUTHORIZATION and ACCESS CONTROL SECURITY POLICY

a. General Policy Statement

This directive establishes policy for managing user accounts, non-user accounts, and administrative accounts with access to information systems (hardware, software, and networks) supporting the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) that supports the Service Center Agencies (SCA) including Large Offices, Field Offices, and their partners. The purpose of this policy is to ensure that necessary authorization and access controls are in place for controlling the actions, functions, applications, and operations of legitimate users. The aim is to protect the confidentiality, integrity, and availability of all OCIO-ITS information resources.

b. Policy Detail

(1). Authorization and Access Guidelines

- (a). The OCIO-ITS Information Systems Security Program Manager (ISSPM) has authorization to restrict access to system objects such as files, directories, devices, databases, and programs, based on user identity, least privilege, and a need-to-know. All access to OCIO-ITS information systems shall be limited to only the resources that a user needs to complete or facilitate official duties. Need-to-know may be modified based on temporary assignments or projects with modifications requested or initiated by the manager of the information system.
- (b). Access control mechanisms shall, either by explicit user (manager) action or documented default, provide that objects are protected from unauthorized access. These controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing permission(s) to access sensitive information shall be granted only by the assigned manager. Access control includes the construction of Access Control Lists (ACL) or modification of system/object parameters. ACLs shall be documented by the system administrator, updated each time there is a change in an object's accessibility, and deleted when no longer needed.

(2). User Account and Password Guidelines

- (a). Procedures for the administration of user passwords are located in section (5). Administrative Guidance for User Passwords.
- (b). Account Management
 1. All authorizations to access and use OCIO-ITS information systems will be granted based on official business need. All managers of OCIO-ITS information resources will ensure access to information is properly authorized and granted with correct access levels and least privileges applied. Each user access will be identified to an individual and will not be shared. If a process cannot be specifically tied to an individual, then the password lifetime will be issued for the period of the session.
 2. All user accounts must be unique and traceable to the assigned user. All OCIO-ITS participant organizations will take appropriate measures to protect the privacy of user information associated with user accounts. The use of group accounts and group passwords is not permitted unless specifically approved by the system owner.
 3. Each OCIO-ITS participant organization manages user account access for OCIO-ITS systems within their area of responsibility. OCIO-ITS guidelines for account setup and management must be applied consistently to be effective. The following

Chapter Three: Authorization and Authentication Control Security Policy

guidelines shall be adhered to when establishing or modifying a non-administrative account:

- a. The creation of a user account must be initiated through a request form and be authorized by pertinent levels of management.
 - b. Modification to an existing account, i.e., to increase responsibility, must be initiated through a request form and authorized by pertinent levels of management.
 - c. Records of processed and denied requests for the creation and/or modification of user accounts must be kept for auditing purposes. Records will be retained for one year, unless otherwise specified by USDA.
 - d. Granting access levels to resources shall be based on the principle of least privilege, job responsibilities, and separation of duties.
 - e. Accounts will be disabled after an identified period of inactivity.
 - f. All requests for temporary user accounts shall provide an expiration date to be applied at the time the account is created.
 - g. Management access to user accounts will be limited to business purposes only, such as during an emergency or contingency situation, cases of extended user absence, or user abuse of OCIO-ITS information resources.
 - h. Personnel transferring from one area of responsibility to another shall have their access accounts modified to reflect their new job responsibilities.
 - i. Each OCIO-ITS participant organization will create procedures to immediately cancel account access and physical access for users whose relationship with the OCIO-ITS has concluded, either on friendly or unfriendly terms.
 - j. User account sessions will time-out in the event of inactivity. This includes user connections to the Internet or to specific applications.
 - k. User account access points for remote computing devices shall be configured using necessary identification and authentication technologies to meet security levels of physically connected computers. Refer to Chapter 14: Network Access Security Policy or its replacement.
 - l. All new information systems acquired or developed by OCIO-ITS and Service Center Agency (SCA) organizations to support program requirements will incorporate access controls to properly protect the OCIO-ITS information systems.
 - m. Temporary access to resources categorized as sensitive (i.e., SBU/SSI) will be set with expiration dates where possible.
- (c). Account Guidelines
1. OCIO-ITS information systems must require each user to uniquely identify themselves and successfully authenticate to gain access.
 2. OCIO-ITS information systems must not allow anonymous, guest, or shared account access unless authorized by the ISSPM.
 3. UserID configuration will be established based on the requirements of the information system.
 4. The naming convention for accounts must be standardized per system.
 5. Users shall not have different account IDs on the same system, i.e., one user account per user per system, unless authorized by the ISSPM; users with administrative privileges may have a second account specifically for the purpose of system administration.
 6. The system shall disable a user's account following consecutive failed login attempts. Once disabled, the account must be locked from access and scheduled to reset automatically or by administrator intervention.

Chapter Three: Authorization and Authentication Control Security Policy

7. The system must invoke an automatic password-protected screen saver and provide users with the ability to invoke a password-protected screen saver on demand.
- (d). Password Guidelines
1. Each OCIO-ITS participant organization will implement appropriate password procedures and technology to enforce this policy.
 2. Strong passwords shall be selected that are not the same or reverse as their UserID, are not the user's name or initials, and are not words commonly found in a dictionary.
 3. A USDA mandatory minimum password length of at least 8 alphanumeric characters with a mixture of letters, numbers and special characters will be established.
 4. Passwords shall not include vendor/manufacturer-supplied passwords, names (i.e., system user names, family names, words spelled forward or backward), addresses or birthdays, or common character sequences (i.e., 3456, ghijk, 2468). Vendor and/or manufacturer-supplied default passwords, such as "SYSTEM", "Password", "Default", "USER", "Demo", or "TEST", shall be replaced immediately upon implementation of a new system.
 5. Passwords shall not be shared unless approved by the established waiver process as described in Appendix C. In the event a password is used for administration or to facilitate testing, it shall be changed immediately upon completion of the test effort.
 6. Known or suspected compromises of passwords shall be immediately reported to a supervisor, manager, help desk, or appropriate security representative.

(3). Administrative and Non-User Account and Password Guidelines

- (a). Non-user accounts include system service and application-required accounts, and accounts that will be used to run administrative system services as well as regularly scheduled "jobs" or tasks. Most services will use SYSTEM/LOCAL accounts unless a domain level account is required.
- (b). In addition to the guidelines for non-administrative accounts and passwords, system administrators, system owners, and system developers shall also follow the policy in the sections below for administrative and non-user accounts.
 1. Administrative Account Management
 - a. Administrative accounts shall only be used for discriminate purposes to ensure that each administrative user is accountable for their actions by ensuring specific events can be associated with an authenticated UserID (i.e., non-repudiation). Login under generic system and administrative accounts is prohibited.
 - b. Administrative accounts shall be limited and access controlled in accordance with Departmentally-established need-to-know concepts.
 2. Administrative Password Guidelines
 - a. Each OCIO-ITS information system shall have a unique administrative password and the system must prompt for a change of the administrative password at least once every 60 days.
 - b. Administrative passwords must not be passed in clear text across an internal OCIO-ITS network or an external network.
 - c. System administrators will change the administrative password when they revoke an administrative user's account.
 - d. Prior to a system being put into production, default or temporary passwords used in testing shall be changed and documented.

Chapter Three: Authorization and Authentication Control Security Policy

- e. Careful precautions shall be exercised by system administrators to the prevent loss and/or compromise of administrative passwords. Each OCIO-ITS organization must enact procedures for the secure archival and retrieval of administrative passwords in cases of emergency. These guidelines are as follows:
 - (1). A copy of the current administrative password(s) for each system shall be archived in a physically secure location that prevents undetected and unauthorized access to the password (i.e., stored in an operational electronic-media or physical safe).
 - (2). The ISSPM shall maintain control of the administrative password archive. This archived password is for emergency use only. The ISSPM must authorize and track access to the archived password under emergency procedures. The administrative password shall be changed immediately after emergency access to the archived password has been made.
3. Non-User Account Management
- a. Non-user accounts will be granted the appropriate security options to support the process on the server, workstation, or laptop where the service is operational.
 - b. Non-user accounts, though they may be members of a domain administration level group, will never be granted domain administration authority.
 - c. Non-user accounts will never be directly accessible by users.
 - d. Non-user accounts will have descriptive text that minimally explains the purpose of the account and where it is used.
 - e. Non-user accounts within the OCIO-ITS environment will have descriptive text in the Active Directory (AD) that minimally explains the purpose of the account, and where it is used.
 - f. The true identification of the account will be maintained in a secured document outside of the environment.
 - g. The creation of a non-user account requires use of the Change Management (CM) process for any account requested.
 - h. Non-user accounts contained within the OCIO-ITS environment that are not defined via current documentation or were not created as part of the CM process are subject to removal or being disabled.
4. Non-User Password Guidelines
- a. Passwords for non-user accounts will not have expiration dates.
 - b. Passwords for non-user accounts will be computer generated.
 - c. Passwords for non-user accounts will be a minimum 14 characters in length.
 - d. Non-user passwords must contain 4 levels of complexity.
 - e. Any reduction of the level of complexity for applications that do not support 4 levels of complexity must follow the CM and/or waiver process.

(4). Periodic Validation of User Access and Account Privileges

- (a). System owners and system administrators are responsible for performing a review of access authorization listings at least quarterly to determine whether they remain appropriate. This applies to operating systems and applications.
- (b). System owners and system administrators are responsible for requesting weekly and monthly updates on user employment status from the Human Resources Department to ensure access and account privileges are valid.

Chapter Three: Authorization and Authentication Control Security Policy

- (c). System administrators shall immediately remove or change access when users are terminated or transferred.
- (d). A current list of authorized system users and their associated access authorizations shall be maintained by all system administrators in a readily-accessible database that is password-protected and stored on a secure server. The password used for access to this information is to be kept under locked storage and managed by the ISSPM.
- (e). System administrators shall identify accounts that have been inactive more than 30 days. Administrators must delete the account if the user is no longer employed or contracted by OCIO-ITS or if the user no longer has a valid business need to access the system.
- (f). Access authorizations shall be documented on standard forms and maintained on file; approved by the appropriate level of management; and securely transferred to local security administrators.

(5). Administrative Guidance for User Passwords

- (a). Passwords shall not be distributed through non-encrypted electronic mail, voice-mail, or left on answering machines.
- (b). Passwords used for dial-up authentication shall be changed at a minimum of every 30 days.
- (c). Passwords for all systems, applications or processes shall be changed every 60 days for non-administrative users.
- (d). The use of automatic logon software to circumvent password entry shall not be allowed, except with specific approval from the ISSPM, for special tasks such as automated backups.
- (e). Passwords for servers, mainframes, telecommunications devices, i.e., routers and switches, and devices used for IT security functions, i.e., firewalls, intrusion detection, and audit logging, shall be encrypted when stored electronically.
- (f). Passwords shall be encrypted when transmitted across a local area network, wide area network, or the Internet.
- (g). Passwords used to access Internet or remote systems shall be different from passwords used to access internal systems and applications.
- (h). Passwords for access to individual workstations (such as passwords for screen savers) shall be encrypted when stored electronically.
- (i). The system shall provide users with a warning before their password expires.
- (j). The system must require new users to change their temporary/default password after the first use of their account and/or after the password has been reset to a temporary/default password.
- (k). If using automated login scripts for system access, the script shall not contain the user's login password with the exception of non-user access.
- (l). Compromised passwords shall be disabled immediately upon detection and a new password issued.
- (m). Before placing a system into a production environment, system administrators must change all default passwords and all passwords that were used in the development environment.

4. CHAPTER FOUR: CAPITAL PLANNING and INVESTMENT CONTROL (CPIC) SECURITY POLICY

a. General Policy Statement

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 updated 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 Federal Information Security Management Act (FISMA), have established a clear and convincing need for a systematic capital planning and investment process for the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS).

b. Policy Detail

- (1). The OCIO-ITS shall institute a formal Capital Planning and Investment Control process and execute all CPIC responsibilities. CPIC shall be used to plan costs for both the overall security program and all major information technology investments.
- (2). This policy is a reference document to be used in maintaining a comprehensive planning process for the security costs of information systems within the OCIO-ITS. Actions taken during the CPIC process supports the development of security plans, FISMA reporting, and security administration within the OCIO-ITS throughout the system development life cycle. Refer to the Guide to CPIC for the Cyber Security Infrastructure of CS-024, Cyber Security Guidance Regarding Security Requirements for Capital Planning and Investment Control (CPIC) or its replacement for information on cost categories, strategic security criteria, and information on security requirements for each CPIC phase. Implementation of a formal IT Capital Planning and Investment Control Process is required by law and is essential for making enhanced security investment and program decisions.
- (3). The OCIO-ITS shall follow the instructions listed in the Guide to CPIC for the Cyber Security Infrastructure in planning costs for security programs and investments. Cost data shall be entered into the Information Technology Investment Portfolio System (I-TIPS) on an annual basis or as an investment is initiated. These figures shall be updated as the figure change during the system development life cycle or on an annual basis for the overall security program. Refer to the Guide to CPIC for the Cyber Security Infrastructure of CS-024, Cyber Security Guidance Regarding Security Requirements for Capital Planning and Investment Control (CPIC) or its replacement for the necessary spreadsheets that shall be downloaded for cost figures and uploaded to the I-TIPS Resource Library when completed.

5. CHAPTER FIVE: CERTIFICATION and ACCREDITATION SECURITY POLICY

a. General Policy Statement

- (1). This policy establishes requirements for the Certification and Accreditation (C&A) process for information systems supporting the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) in accordance with the Computer Security Act of 1987, OMB Circular A-130, Appendix III. The C&A process must be completed on all OCIO-ITS applications and systems in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004.
- (2). The OCIO-ITS Certification and Accreditation program applies to all applications and systems as defined by the Federal Information Security Management Act (FISMA) of 2002. The OCIO-ITS Certification and Accreditation program includes activities to support the implementation of USDA and FISMA directives.

b. Policy Detail

(1). Security Certification and Accreditation

Security certification is the technical evaluation of the risks associated with system operations while accreditation is the management acceptance of the evaluated risk factors and the resulting approval or denial to operate the system. The C&A process will implement the policies and guidelines of the USDA and NIST as they apply to the OCIO-ITS. Federal information technology regulations require OCIO-ITS information systems to undergo a security certification and accreditation process to identify the risks associated with their operation. OCIO-ITS information system integrity protects Federal Government and private resources used to execute and administer business activities while allowing effective access to program information by the general public.

(2). Federal Information Security Management Act

The OCIO-ITS certification and accreditation program includes responsibility for activities to comply with FISMA which is the follow-on legislation to the Government Information Security Reform Act (GISRA) of 2000. Where possible, the C&A program will integrate FISMA requirements into its overall structure. Any FISMA requirements not integrated will still be managed under the C&A program.

(3). Certification and Accreditation Program

The OCIO-ITS Information Systems Security Program Manger (ISSPM) will establish a program to certify and accredit the USDA-funded information systems used within the program. The program will include a process for certifying and accrediting systems, and procedures to guide information system managers through the process.

(4). Identification of Included Information Systems

The OCIO-ITS ISSPM will establish and maintain a list of major applications and general support systems. The list will be updated annually or when major changes occur. Copies will be submitted to the Associate OCIO for Cyber Security to comply with USDA policies.

(5). Participation

Chapter Five: Certification and Accreditation Security Policy

All OCIO-ITS Service Center Agencies, Large Offices, Field Offices, and their partners along with their Federal employees and contractors, will support the C&A program in an appropriate manner.

(6). Site Certification and Accreditation

The ISSPM, with support from the Information Technology (IT) Manager and System Owners, will create a site certification package for each OCIO-ITS site. The package will contain the same elements required for system certification by NIST guidelines. The package will be reviewed every year to comply with USDA and FISMA requirements, and will be updated every three years, or after major changes occur at the locations.

(7). New Information Systems

To comply with OMB Circular A-130, all new information systems acquired or developed by any OCIO-ITS participant organization to support program requirements will incorporate provisions for security certification and accreditation in their project and System Development Life Cycle (SDLC) planning. All new information systems acquired or developed by any OCIO-ITS participant organization will be checked against the criteria for major applications or general support systems provided by the USDA Associate OCIO for Cyber Security. If the new information system is determined to be a major application or a general support system, the project to acquire the system will include funding in the system development plans to accomplish the system certification and accreditation.

(8). Commercial Off-The-Shelf and Government Off-The-Shelf Applications

Commercial Off-The-Shelf (COTS) and Government Off-The-Shelf (GOTS) applications are covered by the C&A activities for the general support system on which they reside, unless the COTS or GOTS product is identified as a major application. If the security configurations for the COTS or GOTS package are customizable, the implementation of the package may need to be certified. The OCIO-ITS ISSPM shall make this final determination.

(9). Existing and Outdated Information Systems

Some OCIO-ITS information systems that play a critical role in mission accomplishment entered into operation prior to implementation of this policy and may have exceeded their design life. Where replacement systems have been identified and are under development, the C&A process will focus on the replacement system. Where no replacement has been identified, the C&A process will evaluate the existing system.

(10). Periodic Review of Information Systems

Federal guidelines direct that the USDA perform an independent review or audit of the security controls in each major application or general support system at least every three years, or with a major change and based on these results, perform an annual review of the overall USDA-wide information security program. These periodic reviews will include the OCIO-ITS operating locations. At the start of each fiscal year, the ISSPM will identify the systems to be reviewed in that fiscal year. This information will be included in the OCIO-ITS Information Security Plan.

(11). Non-OCIO-ITS Systems

Any non-OCIO-ITS system connected to the OCIO-ITS information network must be evaluated to determine if a certification is required as part of the interconnection arrangements.

Chapter Five: Certification and Accreditation Security Policy

(12). Non-OCIO-ITS Sites and Facilities

A non-OCIO-ITS site or facility supports the OCIO-ITS mission in some form, but is outside the direct management responsibility of the USDA. This C&A policy applies to non-OCIO-ITS locations only to the extent required by federal law, or the grant, contract or other operating agreement in place between USDA and the party responsible for the non-OCIO-ITS location.

6. CHAPTER SIX: CONTINGENCY and DISASTER RECOVERY SECURITY POLICY

a. General Policy Statement

- (1). This policy establishes that Information Technology (IT) Contingency and Disaster Recovery Plans shall be developed and maintained for the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS). This process includes contingency and disaster recovery planning for information systems supporting OCIO-ITS operational and business activities. These plans will be tested periodically to ensure they reflect current operating conditions and address current threats.
- (2). The following Federal and Departmental guidelines require OCIO-ITS information systems to have plans for contingencies and disaster recovery in determination of the proper actions to accomplish in the event of a disaster:
 - (a). OMB Circular A-130, Appendix III requires agencies have the ability to recover and provide service sufficient to meet the minimal needs of users.
 - (b). DM3140-1 states that agencies shall develop contingency plans to meet emergencies and shall assure that the plans cover all critical processing.
 - (c). PDD-63 requires a continuity of support plan to sustain an organization's essential functions at an alternate site and perform those functions for up to 30 days before returning to normal operations.
 - (d). NIST Publication 800-34, Contingency Planning Guide for Information Technology Systems, provides guidance that is used to establish the USDA Information Survivability Program.
- (3). These contingency and disaster recovery plans require the involvement of all OCIO-ITS participants to ensure an effective response to contingencies and disasters; it must incorporate the physical and logistical limitations of the OCIO-ITS operating locations; and will be aligned with existing USDA policy.

b. Policy Detail

(1). Contingency and Disaster Recovery Planning

(a). IT Contingency and Disaster Recovery Plans

The OCIO-ITS shall develop IT contingency and disaster recovery plans to meet the needs of critical operations and essential functions during any emergency or situation that may disrupt normal operations. These plans shall describe the actions to be taken before, during, and after events that disrupt critical information systems operations. The contingency and disaster recovery plans should be reviewed for accuracy and completeness at least annually as well as upon significant changes to any element of the plan, system, or resources used for recovery procedures. Testing should occur at least annually or when significant changes are made to the information system or the disaster recovery plan.

1. IT Contingency Plan

An IT contingency plan is the same as the continuity of support plan required by OMB Circular A-130. This plan provides procedures and capabilities for recovering a critical application or general support system following a minor or serious disruptive event.

2. Disaster Recovery Plan

A disaster recovery plan provides detailed procedures for recovering operability of the target system, application, or computer facility at an alternate location.

Chapter Six: Contingency and Disaster Recovery Security Policy

3. It is the responsibility of OCIO-ITS, including large offices and field service offices, to develop, test, implement, and maintain IT contingency and disaster recovery plans for all mission critical systems in support of critical business functions.
4. All contingency and disaster recovery plans must be well written, routinely reviewed, tested, and updated to provide for reasonable continuity of information systems support in the event of a disaster.
5. Contingency and disaster recovery measures shall be identified and integrated into all phases of the System Development Life Cycle (SDLC).

(b). **Prioritization of Recovery**

Activities and their supporting information systems at each location will be prioritized by OCIO-ITS management to determine the criticality of each system and the order of restoration during a contingency or disaster situation. Mission critical operation systems and their components will be established and maintained for each site. This list will be part of the contingency plan. Prioritization will address the categorization of information systems including hardware, software, and networks.

(c). **Contingency Response Team**

1. Each contingency plan will establish a contingency response team and will assign staff to functional contingency and disaster recovery teams in accordance with the needs of the facility. Each staff member must know the activities assigned to them under the contingency and disaster recovery plan.
2. Contingency team members may not necessarily be the same resources as assigned to the Incident Response Team (IRT). A checklist for each team position that assigns responsibility for the tasks each team member will be completed during a contingency or disaster. Personnel assigned to the contingency response team, as well as those responsible for specific systems, will be trained.

(d). **Contingency Plan Testing**

The contingency plan will be tested at least annually. The testing process will be organized to examine all plan elements and related operational procedures at least once annually. Where possible, testing will be integrated with the testing of other site response plans. After action reports will include lessons learned from the testing, deficiencies noted during the testing, and a plan to remedy those deficiencies. The OCIO-ITS ISSPM will ensure funding is included in the annual budget to support the contingency testing program.

(2). Alternate Operating Capability, System Redundancy, and Back-Up/Recovery

(a). **Alternate Operating Capability**

Each OCIO-ITS operating location will have a designated alternate location for establishing temporary control of information resources during a contingency or disaster. Normally such a site will be geographically removed from the immediate disaster location, if possible.

(b). **System Redundancy**

System owners will determine and implement a cost-effective means for providing redundant operations at all locations affected. This includes maintaining suitable spares or replacement equipment for all mission critical systems.

Chapter Six: Contingency and Disaster Recovery Security Policy

(c). Information Back-Up and Recovery

The OCIO-ITS Information Security Office will establish operations procedures for creating, maintaining, and storing information backup media to support contingency response and disaster recovery activities at each operating location. Each location's procedures for data backup will include a schedule for daily, weekly, and monthly backups. Each facility shall establish media control procedures that include steps for the preparation of media for reuse, or destruction. Additionally, each facility will prepare an information backup plan that ensures information is saved according to its priority for recovery.

(d). Information Retention and Archive

Backup media should be retained on-site for operational use until no longer required. Backup media will be periodically reviewed, and if appropriate, archived to comply with guidance from the National Archives and Records Administration. The facility's IT manager shall review all backup media to identify archival data. Archival data will be removed for disposition and storage. Backup media that is not scheduled for archiving will be prepared for reuse or destroyed if appropriate. IT managers may forward their backup media to the program headquarters for storage if space limitations preclude onsite storage.

(e). Off-Site Storage Of Backup Material

Backup media will be stored at a suitable off-site location. For locations where commercial off-site storage is not practicable, the system owner or IT manager will designate an appropriate facility to serve as the off-site storage of backup media. A suitable facility (commercial or non-commercial) is one within reasonable distance, but not likely to be immediately threatened by the contingency or disaster.

7. CHAPTER SEVEN: DATA MANAGEMENT SECURITY POLICY

a. General Policy Statement

- (1). This policy collectively applies to all data assets that exist in USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) processing environments. Other than public data, all data and processing resources are only accessible on a need to know basis to specifically identified, authenticated, and authorized entities. This embodies the principle of least privilege. Access control mechanisms shall be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights.
- (2). Data shall be protected in all of its forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. Data is considered a primary asset and shall be protected in a manner commensurate to its value. Data security is necessary because data processing represents a concentration of valuable assets in the form of information.

b. Policy Detail

(1). Data Security

- (a). OCIO-ITS data security and privacy shall focus on controlling unauthorized access to information. Data security shall be derived from three principles: confidentiality, integrity, and availability. These three principles emphasize the need for security to function properly in the OCIO-ITS processing environment.
- (b). In the context of this policy, the following provides the overall concepts and security principles for which all users are responsible. It is the responsibility of the Information Systems Security Program Manager (ISSPM) to define the specific mechanisms necessary to support these principles.
 1. Accountability
All network, system, and application events shall be attributable to a specific and unique individual. A responsible individual must be assigned to every event using an identification service. An authentication service shall provide verification of this assignment and an audit service will trace any event, reconstructing the time, place, and circumstances surrounding it. In this context, identification refers to a security service that recognizes a claim of identity by comparing a UserID offered with stored security information.
 2. Authorization
 - a. All network, system, and application events shall only result from allowable actions through access control mechanisms. Permission may be derived directly from an individual's identity or from a job classification or administrative privilege based on that individual's identity. The principle of least privilege specifies that individuals only be granted permission for actions necessary to perform their jobs.
 - b. Limiting actions to those properly authorized protects the confidentiality and integrity of data within the OCIO-ITS processing environment. In this context, access control refers to a security service that allows or denies a user request based on privilege, group information, or context.
 3. Availability
All permitted activity shall operate with reliability. Users must be able to retrieve the correct data necessary to perform such events. All event results shall be

Chapter Seven: Data Management Security Policy

completed unless the event is totally aborted. Event results must not depend on unforeseen aspects of other simultaneous events. The security services themselves shall be documented and easily administered. In this context, reliability refers to a security service that guarantees data has not been altered, deleted, repeated, or rearranged during transmission, storage, processing, or recovery.

(2). Data Usage

- (a). Each user shall ensure that OCIO-ITS and Agency data assets under their direction or control are properly labeled and safeguarded according to their sensitivity, proprietary nature, and criticality.
- (b). Users of data assets are personally responsible for complying with all OCIO-ITS policy. All users will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access. Data shall only be used in a manner consistent with OCIO-ITS and Agency policy.

(3). Data Ownership

The owner of data is responsible for classifying their data in accordance with Federal guidelines. If an owner cannot be determined for a data asset, the OCIO-ITS or Agency ISSPM shall act as its custodian. The ISSPM is responsible for developing, implementing, and maintaining procedures for identifying all data assets and associated owners. The owner of all customer data is the individual owner that generates or is assigned ownership of that data.

(4). Data Media Marking

- (a). Marking of hard copy output and magnetic media must reflect the sensitivity of the information. Appropriate markings must be applied, i.e., For Official Use Only (FOUO), Sensitive But Unclassified (SBU), or Sensitive Security Information (SSI). Refer to Chapter 11: Information Classification Security Policy or its replacement.
- (b). Magnetic media must be marked as sensitive (SBU/SSI) unless it is determined to not contain sensitive information. Backup disks/tapes must be marked as FOUO.
- (c). Graphic media, such as photographs, films, tapes, disks or slides must be marked "For Official Use Only" or "FOUO" in a manner that ensures that a recipient or viewer is aware of the status of the information therein.
- (d). FOUO material transmitted outside the OCIO-ITS requires application of an expanded marking to explain the significance of the FOUO marking.
- (e). Permanently bound volumes need to be marked only on the outside of the front and back covers, title page, and first and last pages. Volumes stapled by office-type hand or electric staples are not considered permanently bound.

(5). Data Protection

- (a). External data (hard copy or magnetic media) shall be continually protected at the same level that is afforded to it while using OCIO-ITS information systems. Data administrators should also refer to their organization's local security standard operating procedures. Additionally, administrators must ensure that no unauthorized imported data, whether imported electronically or by diskette, is installed on OCIO-ITS resources.
- (b). OCIO-ITS data will be resident on various media. This media will consist of floppy diskettes, removable and non-removable hard disks, tapes, CD-ROMs, DVD-ROMS, thumb drives, and other media. OCIO-ITS operations require all storage media to be marked according to the highest sensitivity (i.e., FOUO) handled by the system. This

Chapter Seven: Data Management Security Policy

includes master document copies, archives, and backup files when they are removed for repair/exchange or simply provided secure storage.

(6). Data Sharing

Data shall be shared between interconnected systems based on written Interconnection Security Agreements (ISA) based on processes and procedures defined in NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, or its replacement.

(7). Data Transmission

Where necessary, data transmitted shall be secured via cryptographic procedures. This may include the use of confidentiality, integrity, and availability mechanisms.

(8). Data Storage

Data stored shall be secured via cryptographic mechanisms. This may include the use of confidentiality, integrity, and availability mechanisms.

(9). Data Disposal

The OCIO-ITS ISSPM shall develop and implement procedures to ensure the proper disposal of various types of data. These procedures shall be made available to all users with access to data that requires special disposal techniques. The OCIO-ITS processing environment is comprised of program and system application data, computer systems, and network resources. For additional information, see Chapter 13: Media Sanitation and Disposal Security Policy or its replacement.

(10).Data Content

This policy does not mandate or endorse particular data content. Rather, the business decision process used to evaluate the inclusion or exclusion of particular data content shall consider those items listed below. Considerations for evaluating data content include:

- (a). Legal and regulatory obligations in the locales in which the OCIO-ITS operates.
- (b). Confidentiality, availability, and integrity of data ensured to the satisfaction of customers and legal authorities.
- (c). Content is in alignment with our business goals and objectives.
- (d). Customer accessibility to specific data content on the basis of requirement and/or demand.

(11). Data Classification

Data classification is necessary to enable the allocation of resources to the protection of data assets as well as determining the potential loss or damage from the corruption, loss, or disclosure of data. The ISSPM is responsible for evaluating the data classification schema and reconciling it with new data types as they enter usage.

8. CHAPTER EIGHT: FIREWALL MANAGEMENT SECURITY POLICY

a. General Policy Statement

- (1). A firewall shall be used to establish stateful inspection of all packets inbound and outbound on all circuits, connections, or gateways that use a routable Internet address. It shall also be used to establish stateful inspection of all packets inbound and outbound on all circuits, connections, or gateways providing access to internal networks external to the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS).
- (2). All border routers shall use access control lists to block traffic not required by business needs. They shall use ingress and egress filtering to prevent IP spoofing and direct IP broadcasts.
- (3). Any changes affecting firewall implementation shall be approved through the CCB process.
- (4). All firewalls shall be backed up in a manner that permits a complete firewall recovery on a weekly basis. Archives of firewall backups shall be maintained for a minimal period of at least six weeks.
- (5). All back-up media shall be maintained on-site in a secure manner consistent with Chapter 6: Contingency and Disaster Recovery Security Policy, or its replacement, and be protected by a password. Backup media shall also be maintained in an off-site storage location and secured in a manner consistent with Chapter 6: Contingency and Disaster Recovery Security Policy, or its replacement.

b. Policy Detail

(1). Firewall Protocols

- (a). Approved protocols such as security plans and internal operating procedures must specify how each protocol will be securely operated. These include, but are not limited to FTP, SMTP, HTTP, HTTPS, DNS, POP3S, Secure FTP (FTPS), SSH, IMAPS. NTP is allowed on outbound only traffic only.
- (b). All other protocols are considered non-secure and require an approved OCIO-ITS waiver before use. These include, but are not limited to Finger, NFS, RLP, TFTP, RSH, who, BFTP, POP, SFTP, UUCP, RLOGIN, exec, Chargen, Link, POP2, Xprotocols, RCF, LPD, SunRPC, ICQ/AIM, REXEC, irc, Name, Portmap, Supdup, IMAP, IDNET, Echo, Netbios, RIP, Syslog, SNMP, and shell.
- (c). Approval to use non-secure protocols will be granted only if it can be demonstrated that the selected firewall configuration provides adequate security.

(2). Firewall Management Access

- (a). Management consoles must provide a secure (encrypted) communications path between the management console and the firewall being managed.
- (b). Access to firewall management consoles, operating systems, sub-systems, and rule-base editors shall be limited to Firewall Administrator personnel only. For security purposes, there are no exceptions to this rule. All firewall user accounts and credentials shall comply with Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (c). A Read-Only access account may only be used by the Information Systems Security Program Manager (ISSPM) or designated representative for the primary purpose of security auditing.
- (d). The original vendor-supplied administrative account of the firewall and/or firewall software must be renamed.

(3). Firewall Configuration

Chapter Eight: Firewall Management Security Policy

All firewall documentation including all configuration and rule-base standards used to control usability, efficiency and security of the overall firewall environment shall be kept in a Trusted Facilities Manual (TFM).

(4). Firewall Physical Security

- (a). All firewall consoles will be located in a physically secure area and shall require a logical security level equal to or exceeding C2 security functionality.
- (b). All firewalls are to be physically secured in accordance with Chapter 17: Physical Access Security Policy or its replacement.

(5). Firewall Logs

- (a). All firewall logs and events are to be written to drives external to the firewall and shall be managed in a manner that maintains their integrity and authenticity. These logs are to be stored or archived for a minimum of three years. Requests for access to firewall logs shall comply with the firewall information statement in this document.
- (b). Each firewall will maintain all security auditing events to logs and show successful and unsuccessful security auditing events.
- (c). All firewall administrator personnel have the implied authority and responsibility to take action(s) to protect OCIO-ITS assets from loss without CCB approval in an emergency. This authority is only justified if a direct threat or attack has been discovered and prompt action is required to reduce the risk for compromise of OCIO-ITS and participating Agency resources.
- (d). The OCIO-ITS ISSPM has the implied authority and responsibility to direct and authorize action(s) to protect OCIO-ITS and participating Agency information assets from loss without CCB approval in an emergency only. This authority is only justified if a direct threat or attack has been discovered and prompt action is required to reduce the risk for compromise of OCIO-ITS and participating Agency resources.
- (e). If this authority is exercised, the administrator shall report it as an incident and follow Chapter 10: Incident Identification, Declaration, Reporting, and Handling Security Policy or its replacement.

(6). Incident Reporting

If an event is discovered, i.e., a security breach, successful attack, or violation of this policy, the incident shall be reported in accordance with Chapter 10: Incident Identification, Declaration, Reporting, and Handling Security Policy or its replacement.

9. CHAPTER NINE: GOVERNMENT-OWNED LAPTOP COMPUTERS AND PED SECURITY POLICY

a. General Policy Statement

- (1). Government-issued laptop computers and Portable Electronic Devices (PED) shall be pre-configured with all necessary security measures in accordance with the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) for the system to be accessed by OCIO-ITS Federal employees, contractors, subcontractors, or partners.
- (2). Government-owned laptops computers and Personal Electronic Devices (PED) may be used to house Sensitive But Unclassified (SBU) and Sensitive Security Information (SSI) data only when required for official duties. This information shall be encrypted during storage to protect against unauthorized disclosure. When a computer laptop or PED is no longer required for official business, the SBU/SSI data shall be removed immediately.
- (3). For information on the use of Wireless Technology, refer to Chapter 14: Network Access Security Policy or its replacement.

b. Policy Detail

(1). Classification of Government-Owned Laptop Computers

- (a). Government-owned laptops are classified into two types. These are as follows:
 1. Docking Station-based Laptop Computers
These laptop computers are plugged into a docking station when it is at a fixed location. However, laptops can be pulled out and used as a stand-alone laptop computer.
 2. Stand-Alone Laptop Computers
These laptops do not require the use of a docking station and are be shared among many users. They can be either checked-in or checked-out to many users based on OCIO-ITS official business requirements.
- (b). Despite these variances, all Government-owned laptop computers must adhere to the guidelines outlined in this security policy.

(2). Government-Owned Laptop Computer Security

- (a). Virus Protection and Software Patches
Government-owned laptops must be adequately protected by current antivirus software and must be consistently configured to ensure security against known vulnerabilities in operating systems and application software. Refer to Chapter 16: Patch Management Security Policy and Chapter 27: Virus Protection Security Policy, or their replacements, for additional information.
- (b). Personal Usage
Off-site usage of Government-owned laptop computers, whether at home or at other locations, is restricted to business purposes. However, USDA DR 3300-1 authorizes limited personal use provided the use involves minimal expense to the Government and does not interfere with official business. Refer to Chapter 1: Acceptable Use Security Policy, or its replacement, for additional details on personal use of OCIO-ITS computer equipment.
- (c). Access Control

Chapter Nine: Government-Owned Computer Laptop and PED Security Policy

Refer to Chapter 3: Authorization and Access Control Security Policy, or its replacement, for additional details on access control for OCIO-ITS computers.

- (d). Physical and General Security Practices
1. Laptop computers are subject to all OCIO-ITS security policies and procedures. This includes, but is not limited to, virus protection, physical access, passwords, screensavers, and data cleansing.
 2. Users shall be liable for damages incurred if found negligent of not properly following established security regulations in properly securing Government equipment in accordance with this policy.
 3. Thefts shall be reported immediately to local law enforcement and the OCIO-ITS Information Systems Security Program Manager (ISSPM). The ISSPM shall immediately suspend access privileges to prevent network hacking.
 4. Users will make sure that adequate precautions are exercised to ensure that laptop computers are physically secure at all times. Security practices include, but are not limited to the following:
 - a. Laptop computers shall not be left unattended in public places. These typically include aircraft, airports, cars, hotels, restaurants, or non-Government office buildings.
 - b. Laptops shall not be used in public if sensitive data is displayed on the screen that may be viewed by others.
 - c. Laptop users shall not announce to anyone that they have a Government-owned computer in their possession.
 - d. Users are required to use laptop computer security locks (if provided) to protect Government equipment from theft. These locks shall be properly utilized to provide the utmost protection.
 - e. Non-docking laptop computers shall be shut down and stored out of sight when a user is away from the office perimeter to include precautions in meeting spaces.
 - f. Laptops being used as a primary workstation shall be fastened to a desk using a locking device such as a docking station.
 - g. Users shall attempt to minimize the amount of time the laptop computer is out of their control to deter mix-ups or theft during security screening at airports, train stations, and Federal or non-Government office buildings.
 - h. Laptop computer users shall cushion the laptop, i.e., storing the computer in a computer carrying case, to prevent damage while in travel.
 - i. While on an aircraft, the laptop computer shall be stored in the best possible location, that being under the seat in front of the user, or in an overhead compartment that is visible from the user's seat.
 - j. Laptop computers shall be stored in the hotel safe or room safe if available. If a safe is unavailable, the laptop must be stored in such a fashion that it is completely hidden from view upon leaving the hotel room.
 - k. Users must never leave their laptops in open view in a parked car. Every effort should be made to conceal the laptop from sight to include storing the laptop under the seat or in the locked trunk of the car.
 - l. Laptop computer users shall not eat, drink, or smoke at or near the laptop.
 - m. An ID label or return-to-owner notice should be attached to the underside of a laptop computer using only the official USDA business address.
 - n. If a non-Government, third party ISP network is utilized (outside of Federal facilities), then the following must be enabled to protect the laptop and its contents:

Chapter Nine: Government-Owned Computer Laptop and PED Security Policy

- (1). Personal firewall enabled and properly configured
- (2). Antivirus definitions will be updated
- (3). Encrypted VPN (non-split tunneled) will provide access to USDA network resources

(3). Government-Owned Portable Electronic Devices (PED)

A Portable Electronic Devices (PED) is any electronic device that is capable of receiving, storing, or transmitting information and does not require a permanent link to Federal networks. Handheld devices such as Personal Digital Assistants (PDA) permit users to synchronize databases using either hardwired or wireless means and provides access to network services such as e-mail, Web browsing, and Internet access. PEDs include, but are not limited to, cellular phones including picture and movie-enabled phones, pagers, text messaging devices, and wireless e-mail devices such as Blackberries, hand-held scanners, PDAs (i.e., Palm Pilots), voice recorders, and flash memory.

(a). Use of Wireless Technology

Refer to Chapter 14: Network Access Security Policy or its replacement.

(b). Virus Protection and Software Patches

Government-owned PEDs must be adequately protected by current antivirus software and must be consistently configured to ensure security against known vulnerabilities in operating systems and application software. Refer to Chapter 16: Patch Management Security Policy, and Chapter 27: Virus Protection Security Policy, or their replacement, for additional information.

(c). Personal Usage

1. Off-site usage of Government-owned PEDs, whether at home or at other locations, is restricted to business purposes. However, USDA DR 3300-1 authorizes limited personal use provided the use involves minimal expense to the Government and does not interfere with official business. Refer to Chapter 1: Acceptable Use Security Policy, or its replacement, for additional details on personal use of OCIO-ITS computers.
2. Use of Non-Government owned Portable Electronic Devices (PED) is prohibited in the OCIO-ITS information resource environment.

(d). Access Control

Refer to Chapter 3: Authorization and Access Control Security Policy, or its replacement, for additional details on access control for OCIO-ITS computers.

(e). Physical and General Security Practices

1. All PEDs, flash memory devices, and wireless devices will be provided by the Government unless an approved detailed waiver has been granted by the CIO.
2. PEDs are subject to all OCIO-ITS security policies and procedures. This includes, but is not limited to, virus protection, physical access, passwords, screensavers, and data cleansing.
3. Security for PEDs will be coordinated and managed by the OCIO-ITS ISSPM.
4. PEDs shall be screened by the ISSPM, or designated representative, at least quarterly for appropriate configurations, viruses, antivirus protection, and patch level will be updated, as required.
5. Thefts shall be reported immediately to local law enforcement and the OCIO-ITS ISSPM. The ISSPM shall immediately suspend access privileges to prevent network hacking.

Chapter Nine: Government-Owned Computer Laptop and PED Security Policy

6. The OCIO-ITS ISSPM retains the right to delete or purge data on a PED in cases of suspected compromise.
7. PEDs will be surrendered to the ISSPM immediately upon transfer, reassignment, resignation, or retirement from Federal service.
8. Users shall be liable for damages incurred if found negligent of not properly following established security regulations in properly securing Government equipment in accordance to this policy.
9. Standardized configurations will be established for all PEDs to include operating system software, firmware, and authorized applications.
10. Encryption techniques, including digital certificates/PKI/Biometrics, that conform to USDA and NIST requirements, shall be used for Infrared and wireless transmissions, and for data storage on PEDs.
11. Users will make sure that adequate security precautions are exercised to ensure that laptop computers are physically secure at all times, including any flash memory used in such devices.
12. Strict physical security standards for PEDs shall be implemented to include requirements to hand carry PEDs during travel, powering off devices not in use, tracking and tagging of PEDs, and contact information in case device is lost or stolen.
13. PED modems will remain disabled at all times.
14. Where applicable, Virtual Private Network (VPN) technology is required for the use of PEDs and split tunneling profiles will be disabled.
15. Modifications will not be made in official system configurations, operating systems, antivirus software, or remote access arrangements except those made by the OCIO-ITS ISSPM or designated representative.
16. In absence of electronic verification or auditing, physical inventories of PEDs will be performed on an annual basis. During the inventory, storage of information will be checked to confirm that only required information is maintained and that Sensitive But Unclassified (SBU) data is encrypted.
17. PEDs will be returned to the OCIO-ITS on a monthly or quarterly basis, or upon management request for system updates, patches, and accountability reasons.
18. Encryption techniques will be used for infrared and wireless transmissions of Sensitive But Unclassified (SBU) information or for storage of SBU data.
19. Unauthorized software and unauthorized copyrighted or illegal material will not be loaded or stored on PEDs.
20. Users shall exercise caution in discussions of sensitive information using wireless technology to prevent inadvertent disclosure of SBU information use or violations of the Privacy Act.
21. Floppy disks, CD-ROMs, and Flash Memory will not be used to download applications or SBU information.
22. Government-owned PEDS may not be synchronized to personal computers.
23. Personal PEDS shall not be synchronized to Government-owned computers.

10. CHAPTER TEN: INCIDENT IDENTIFICATION, DECLARATION, REPORTING, AND HANDLING SECURITY POLICY

a. General Policy Statement

- (1). This document establishes security procedures for Incident Identification, Declaration, Reporting, and Handling for USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) information systems and data resources. It is designed to enhance and compliment current USDA Incident Response and Reporting policy and procedures.
- (2). This policy is established in compliance with the requirements of the Computer Security Act of 1987, OMB Circular A-130, Appendix III, The Federal Information Security Management Act (FISMA), USDA Computer Incident Response Procedure 10/25/01, and NIST Special Publication 800-61 Computer Security Incident Handling Guide.

b. Policy Detail

(1). Computer Security Incidents

- (a). This policy establishes the OCIO-ITS Incident Handling Program (IHP). The IHP shall be assigned to the Director of Infrastructure Governance (DIG); the DIG may delegate responsibility to the Group Manager of Security Policy (GMSP); and the GMSP is responsible for establishment and continued operations of the OCIO-ITS Computer Incident Response Team (CIRT).
- (b). The Director of Infrastructure Operations (DIO) is responsible for providing key support personnel and participation in the IHP and short-lived OCIO-ITS Incident Handling Team (IHT). The Security Incident Duty Officer (SIDO) may, at anytime, utilize these technical experts from the OCIO-ITS Infrastructure Operational Division (IOD). Other technical subject matter experts may be called upon, such as:
 1. USDA Human Resources (HR)/Employee Relations
 2. Office of Inspector General (OIG)
 3. Other OCIO-ITS and/or USDA management
- (c). FISMA requires that Government agencies have policies and procedures for detecting, reporting, and responding to Information Technology (IT) security incidents. This policy creates and establishes a Computer Incident Response Team (CIRT) with authority to declare, manage, handle, report and close out computer security incidents.
- (d). The CIRT shall be aware of the requirements to establish rigorous incident identification and declaration processes. The CIRT Security Incident Duty Officer shall have the authority to declare OCIO-ITS IT security incidents. The following events shall automatically meet the IT security incident threshold and be assigned an OCIO-ITS security incident number:
 1. Mandatory Incidents
 - a. All USDA incidents that are reported to the CIRT for handling.
 - b. OCIO-IDS reports that are re-identified and confirmed as being High-Internal or High-External exploits or compromises that can be confirmed by OCIO-ITS logs.
 - c. Incidents reported to the CIRT from the National Information Technology Center-Systems Network Control Center (NITC-SNCC) as unresolved events.
 - d. Direct contact or notification by the USDA-OIG for either criminal or civil prosecution.
 - e. Complaints from the public about OCIO-ITS employees, contractors, devices or IP addresses, in appropriate activities or attacks.

Chapter Ten: Incident Identification, Declaration, Reporting, and Handling Security Policy

- f. Law enforcement initiated by the Federal Trade Commission, Task Force, Federal Protective Service or by other law enforcement agencies.
 - g. US-CERT (Computer Emergency Response Team) makes direct contact via telephone or e-mail with the CIRT regarding personnel or an actual exploit, attack, or other anomaly.
 - h. Notification of real or suspected theft or trafficking in copyright protected materials, software, music, videos, movies, pictures or documents by the Industry Associations of America, the Software and Information Industry Association and/or the Business Software Alliance.
 - i. Whistleblower complaints.
 - j. Installation and use of peer-to-peer software.
 - k. Public complaints regarding theft of copyrights, Recording Industry Association of America (RIAA), ISP and/or spamming.
2. Discretionary Incidents
- a. Internal incidents
 - b. Inappropriate use, such as pornography, gambling and hate crimes
 - c. Unofficial use of chat rooms using the Internet
 - d. Help Desk initiated
 - e. Employee complaints
 - f. Vulnerability scans

(2). Reporting Process

- (a). All OCIO-ITS IT security incidents will be processed through the CIRT Duty Officers.
- (b). The CIRT may solicit subject expert assistance from:
 - 1. Infrastructure support personnel
 - 2. Telecom Operations personnel
 - 3. Security Operations personnel
 - 4. Infrastructure Deployment personnel
 - 5. Hosting Operation personnel
 - 6. Data Management personnel
 - 7. OCIO-ITS and Agency Information Systems Security Program Managers (ISSPMs)
 - 8. OCIO-ITS Human Resources/Employee Relations personnel
 - 9. Other subject matter experts as required
- (c). The CIRT will turnover all specific employee and contractor misconduct allegations to the appropriate ISSPM. After the misconduct is turned over to the appropriate ISSPM, the CIRT will close out any associated OCIO-ITS tracking numbers.
- (d). The CIRT will investigate all OCIO-ITS misconduct allegations and will notify OIG and/or OCIO Cyber Security as appropriate.
- (e). The CIRT will forward all virus incidents on OCIO-ITS equipment to the IO Lab, Telecom, Data Centers and/or Web Farms, as appropriate. The CIRT will coordinate all incident reporting back to OCIO Cyber Security.
- (f). When the OCIO-ITS closes out a misconduct offense, the agency or office that receives that event is responsible for completing all required USDA and US-CERT reports.

11. CHAPTER ELEVEN: INFORMATION CLASSIFICATION SECURITY POLICY

a. General Policy Statement

- (1). This policy establishes the requirement for the classification, protection, and management of sensitive data stored and processed on information systems supporting the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS).
- (2). Sensitive But Unclassified (SBU) information shall be properly handled, stored and protected from the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction. SBU information also includes Sensitive Security Information (SSI). However the SBU category contains information that is not security related but is still sensitive in terms of its risk of exposure.
- (3). For Official Use Only (FOUO) identifies information that is exempt from mandatory release under the provision of the Freedom of Information Act (FOIA). For Official Use Only (FOUO) is a document designation, not a classification. This designation is used to identify information or material which, although unclassified, may not be appropriate for public release.

b. Policy Detail

(1). Sensitive But Unclassified (SBU) Information Protection

- (a). All OCIO-ITS offices will analyze their information to determine appropriate levels of concern for their data in accordance with OMB A-130 and NIST Special Publication 800-37.
- (b). SBU/SSI information with a high level of concern should not be discussed or transmitted via telephones, pagers, cell phones, fax, or other wireless devices as these are not secure and the risk of interception of the transmission is great. The use of other than secure telephonic devices to discuss SBU/SSI information shall only be permitted where the degree of risk is understood and accepted.
- (c). Service Center Agencies shall analyze all information available or to be published on public Web pages to ensure that SBU/SSI information is not made available except on a need-to-know basis.
- (d). SBU/SSI shall be processed and stored only on systems that meet Cyber Security guidance requirements for controlled access protection.
- (e). Service Center Agencies shall shred SBU/SSI documents of high-level concern in lieu of disposal in trash to prevent unauthorized disclosure.
- (f). Government-owned mobile systems, laptops, and Personal Electronic Devices (PED) may be used to house SBU/SSI data only when required for official duties. This information shall be encrypted during storage to protect against unauthorized disclosure. When a mobile system or PED is no longer required for official business, the SBU/SSI data shall be removed with software to overwrite the sensitive information in accordance with USDA regulations.
- (g). Care shall be taken by Service Center Agencies to avoid leaving SBU/SSI information readily available at workstations or on personal computer screens. SBU/SSI data with a high level of concern will be stored on a floppy disk or zip drive in a locking desk drawer, file cabinet, or locked office. Care should also be taken when printing SBU/SSI information on inkjet printers as printer ink will smear if wet. SBU/SSI information should be printed on laserjet printers (if available).
- (h). Access to SBU/SSI will be provided to employees and contractors with a need-to-know basis. When SBU/SSI data must be shared with contractors and entities outside of the USDA, a Non-Disclosure Agreement form shall be executed by the system owner or

Chapter Eleven: Information Classification Security Policy

Information Systems Security Program Manager (ISSPM) prior to granting access to the data in order to preclude possible organizational or personal conflicts.

- (i). All Statements of Work (SOW) shall be marked in a conspicuous manner with the following notice: “Sensitive But Unclassified/Sensitive Security Information – Disseminate on a Need-To-Know Basis Only” in accordance with OCIO-ITS regulations. Electronic messages shall be marked with this notice as well.
- (j). All FOIA requests for SBU/SSI will be processed in accordance with OCIO-ITS regulations and the Attorney General’s memorandum.

(2). For Official Use Only (FOUO) Information Protection

- (a). For Official Use Only (FOUO) is a document designation that is used to identify information or material which, although unclassified, may not be appropriate for public release. There is no national policy governing use of the FOUO designation. FOUO information is unclassified sensitive information that is or may be exempt from public release under the FOIA.
- (b). The OCIO-ITS shall define what information shall be protected as FOUO and how this protected information shall be handled. FOUO information may be disseminated as necessary in the conduct of official business. FOUO information may also be released to officials in other departments and agencies in performance of a valid government function.
- (c). Unclassified documents and material containing FOUO information shall be marked as follows:
 - 1. Documents will be marked FOR OFFICIAL USE ONLY at the bottom of the front cover (if available), the title page (if available), the first page, and the outside of the back cover (if available).
 - 2. Pages of the document that contain FOUO information shall be marked FOR OFFICIAL USE ONLY at the bottom.
 - 3. Each paragraph containing FOUO information shall be marked with the abbreviation FOUO in parentheses at the beginning of the FOUO portion.
 - 4. Material other than paper documents (i.e., slides, computer media, films, etc.) shall bear markings which alert the holder or viewer that the material contains FOUO information.
- (d). FOUO information shall be safeguarded as follows:
 - 1. FOUO information should be handled in a manner that provides reasonable assurance that unauthorized persons do not gain access.
 - 2. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, FOUO may be stored as a minimum in a locked desk, file cabinet, bookcase, locked room, or similar place.
 - 3. FOUO documents and material may be transmitted via first class mail, parcel post, or, for bulk shipments, via fourth class mail.
 - 4. Fax or e-mail transmission of FOUO information (voice, data, or facsimile) should be made via encrypted communications systems whenever practical. FOUO information may be put on an Internet web site only if access to the site is limited to a specific target audience and the information is encrypted.
 - 5. FOUO documents may be destroyed by shredding or tearing into pieces and discarding the pieces in a regular trash container unless circumstances recommend a need for more careful protection.

(3). Encryption

Chapter Eleven: Information Classification Security Policy

(a). General

1. All OCIO-ITS offices, employees, and contractors will identify and provide adequate security protection for all SBU/SSI information. This information will be encrypted when electronically transmitted to prevent unauthorized disclosure of sensitive information to users.
2. Each Service Center Agency will provide a report to their ISSPM on an annual basis that identifies all SBU information.

(b). Encryption Plan

In accordance with the Office of Management and Budget Guidance on Data Availability and Encryption, each implementation shall include an encryption plan. Required components in the OCIO-ITS encryption plan include:

1. A configuration layout showing complete end-to-end details of the telecommunication or computer systems encryption points.
2. The type of encryption to be used.
3. The source of key generation and insertion for symmetrical encryption methods.
4. The cryptographic period required, that is, the amount of time before a session key should be updated. The maximum valid age of the cryptographic period is 60 days.
5. The system procedures for key loading, key generation, key protection and distribution, key recovery, and key destruction.
6. Each Service Center Agency shall have key recovery procedures to recover encrypted sensitive information when the data is stored electronically.

(c). Encryption Policy

1. OCIO-ITS offices shall implement encryption algorithms that are endorsed by NIST and the U.S. Department of Agriculture on those computing systems that process and store sensitive information. These requirements include internal and external information systems that process and store sensitive information within the USDA infrastructure and by other parties on behalf of Service Center Agencies.
2. Any Service Center Agency that cannot implement the requirements of the policy shall require a waiver approved by the OCIO-ITS ISSPM and Associate CIO for Cyber Security. Waivers will be considered for implementation timeframes only. However, all SBU/SSI information shall be encrypted – no exceptions will be considered for this requirement.
3. All OCIO-ITS telecommunication and network encryption systems shall have an encryption plan approved by the OCIO-ITS ISSPM.
4. Sufficient redundancy and capacity needs to be incorporated into departmental or OCIO-ITS mission critical and essential communication systems to prevent transmission of SBU/SSI information in clear text.
5. SBU/SSI will be processed and stored as per USDA Cyber Security guidance on C2-like Controlled Access Protection.
6. All Service Center Agencies and offices shall exercise control over all keys utilized in encrypted transmissions.
7. All encrypted protocols shall deploy either the Triple Data Encryption Standard (DES) or the Advanced Encryption Standard approved by NIST. Encryption products used to protect sensitive information shall conform to the NIST Cryptographic Module Validation Program validated listing. All encryption implementations will conform to the Level 2 Security requirements as specified in FIPS 140-2 unless otherwise identified in this policy.
8. Secure Shell (SSH) may be deployed solely for the remote administration of sensitive systems.

Chapter Eleven: Information Classification Security Policy

9. The Secure Sockets Layer (SSL) specification may be deployed to provide secured access to sensitive information on Web servers. When SSL is used to protect OCIO-ITS sensitive information, the latest version shall be used with 128-bit encryption.
10. Virtual Private Networks (VPN) shall be deployed in environments where data-link layer encryption would not be a practical solution to maintain and operate. VPN technology using IPSEC encryption allows it to be implemented independent from a particular link layer communications technology (i.e., HDLC, Frame Relay, FDDI, Ethernet, Gigabit Ethernet, ATM, etc.). As such, this policy strongly encourages the use of VPN technology to secure departmental and OCIO-ITS sensitive communications.
11. Data-Link (symmetrical) Encryption shall be used in environments where VPN management would not be a reasonable and/or warranted.
12. Pretty Good Privacy (PGP) may be used to protect sensitive information transmitted via e-mail using a minimum key size of 2048. Public key information may be maintained on public or internal PGP key servers.
13. Public Key Infrastructure (PKI) implementations are suitable for all environments and shall follow Cyber Security's Interim Guidance on the Use of Public Key Infrastructure (PKI) Technology in the USDA, CS-008.
14. Secure/Multipurpose Internet Mail Extension (S/MIME) is a standards-based security enhancement used to secure message attachments and provide strong authentication through digital signatures, message confidentiality, integrity, and non-repudiation.

12. CHAPTER TWELVE: INTRUSION DETECTION MANAGEMENT SECURITY POLICY

a. General Policy Statement

- (1). This policy establishes the requirement for the use of Intrusion Detection Systems (IDS) on information resource supporting the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS). The Change Control Board (CCB) shall give written approval to the configuration of the IDS prior to any activity. All sensor-to-console communications shall be encrypted to prevent interception or changes being made.
- (2). The OCIO-ITS shall use intrusion detection sensors to monitor all network traffic at major gateways. The scope of intrusion detection shall be expanded to include new equipment or subnets as they are added to the primary network. Electronic updates to intrusion detection signature files shall be received and applied in an automated fashion as to ensure the IDS system can be kept current with the latest attack signatures. All updates must be tested prior to updating the production system.
- (3). IDS Administrators and OCIO-ITS Information Systems Security Program Managers (ISSPMs) shall report any security breach, successful attack, or violation of this policy in accordance to the Chapter 10: Incident Identification, Declaration, Reporting, and Handling Security Policy, or its replacement.

b. Policy Detail

(1). IDS Access

- (a). Access to IDS management consoles, operating systems, sub-systems, and signature files shall be limited to IDS Administrator personnel. For security reasons, no exceptions to this rule shall be permitted. All IDS user credentials shall comply with Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (b). Administrator accounts are any accounts with read/write access to the IDS configuration. These accounts shall be user specific and access shall only be permitted from workstations intended for this function. This type of account shall only be issued to IDS Administrators.
- (c). The administrator account is the original administrative account of the IDS. This account shall be renamed where possible and will be used on a limited need-to-know basis. Only IDS administrative personnel are permitted to have knowledge of this type of password and shall comply with Chapter 3: Authorization and Access Control Security Policy or its replacement.

(2). IDS Configuration Standards

IDS documentation, specifically all configuration standards used to control usability, efficiency, and security of the overall IDS environment, shall be maintained and secured from non-secured resources. This documentation shall be strictly adhered to when designing, implementing, or managing IDS configurations.

(3). IDS Physical Security

All IDS systems and sensors shall be physically secured in accordance with Chapter 17: Physical Access Security Policy or its replacement.

(4). IDS Logs

Chapter Twelve: Intrusion Detection Management Security Policy

- (a). The IDS Administrator shall monitor and view IDS log files on a daily basis using the IDS central console. The IDS Administrator shall submit a monthly report to the Agency ISSPM detailing the month's activities.
- (b). All IDS logs are to be written to drives external to the IDS. IDS logs shall be managed in a manner that maintains their integrity and authenticity. These logs are to be stored or archived for a minimum of six (6) months. Request for access to IDS logs shall be made directly to the IDS Administrators with final approval to be determined by the security staff in the event that the Information Security Staff and the IDS Administrator are synonymous.
- (c). In the event of increased activity, monitoring and reporting activity shall be adjusted as needed.

(5). IDS Implementation

A request for implementation of new IDS system and sensor implementations shall be submitted to the CCB. This request shall include all configuration and policy settings along with other system information. After obtaining CCB and ISSPM approval, authorized personnel can proceed with the IDS implementation. Any changes from the original design made during the installation will need to be submitted via a change request.

(6). Change Request

Change requests for any modifications to the IDS system, configuration, sensors, or rules shall be submitted in writing to the CCB for review. All change requests shall include the reason and timeframe for the request as well as all risks, threats, and known issues associated with this change. Following approval by CCB, IDS Administrators may proceed with the IDS changes.

13. CHAPTER THIRTEEN: MEDIA SANITATION and DISPOSAL SECURITY POLICY

a. General Policy Statement

This policy establishes the requirement for the secure and appropriate disposal of Information Technology (IT) equipment, devices, network components, operating systems, application software, and storage media belonging to the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) to prevent unauthorized use or misuse of Federal Government information. All IT equipment shall be properly sanitized prior to disposal or release, and sanitization procedures shall be properly documented to prevent unauthorized release of sensitive and/or confidential information that may be stored on that equipment and other electronic media.

b. Policy Detail

(1). Sanitization of IT Equipment and Electronic Media

The sale, transfer, or disposal of computers, computer peripherals, and computer software or other OCIO-ITS devices may create information security risks including potential violations of software license agreements and the unauthorized release of sensitive information. Due to these risks, all OCIO-ITS computers containing sensitive data shall have their hard drives securely erased.

(2). Sanitization of Hard Drives

- (a). Sanitization must be performed on hard drives to ensure all information is removed in a manner that gives assurance that the information cannot be recovered. Three acceptable methods to be used for the sanitization of hard drives include:
 1. Overwriting
 2. Degaussing
 3. Physical Destruction
- (b). Sanitization methods shall depend upon the operability of the hard drive:
 1. Operable hard drives that will be reused must be overwritten prior to disposition. If operable hard drives are to be removed from service completely, they must be physically destroyed or degaussed.
 2. Hard drives that are inoperable or those that have reached the end of their useful life must be physically destroyed or degaussed.
- (c). Clearing data (deleting files) is not an acceptable method of sanitizing OCIO-ITS hard disk storage media as this process does not prevent data from being recovered by technical means.

(3). Overwriting Specifications

- (a). Overwriting is the approved sanitization method for OCIO-ITS hard disk drives as it effectively renders data unrecoverable. The entire hard disk shall be overwritten with a repetitive group of characters. Writing repetitive characters over the surface of the disk will destroy data previously left on the hard disk.
- (b). All software products and applications used for the overwriting process must be able to overwrite the entire hard drive, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data. When extremely sensitive information is present on a hard drive, the overwrite

Chapter Thirteen: Media Sanitation and Disposal Security Policy

procedure must be completed at a minimum of three times. After sanitizing a hard disk, the Agency will attach a statement to the unit certifying that it was sanitized.

(4). Degaussing Specifications

Degaussing is a process used to erase magnetic media on hard drives, rendering them useless. The degaussing method shall only be used when the hard drive is inoperable and will not be used for further service. However, as the use of a degausser does not guarantee that all data on the hard drive will be destroyed, degaussing efforts should be audited periodically to detect equipment or procedure failures.

(5). Physical Destruction

Hard drives must be destroyed when they are defective or cannot be repaired or sanitized for reuse. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive.

(6). Sanitization of Other Computer Media

- (a). Risks for the potential disclosure of sensitive data on media other than computer hard drives shall be sanitized accordingly. Particular attention shall be paid to floppy disks, tapes, CD-ROMs, DVD-ROMs, and optical disks. Unlike magnetic media sanitization, clearing is an acceptable method of sanitizing memory components before release.
- (b). Memory components are categorized as either volatile or nonvolatile. Volatile memory components do not retain data after removal of all electrical power sources, i.e. Static Random Access Memory (SRAM) and Dynamic Random Access Memory (DRAM). Nonvolatile memory components do retain data when all power sources are discontinued. These memory components include Read Only Memory (ROM), Programmable ROM (PROM), or Erasable PROM (EPROM) and their variants.
- (c). Memory components that have been programmed at the vendor's commercial manufacturing facility and are considered unalterable in the field may be released.

(7). Disposal of OCIO-ITS Equipment

Following the proper sanitization of OCIO-ITS computer equipment, these components may be disposed of in the appropriate format listed below:

- (a). Donation to educational institutions and educational nonprofit organizations under authority of Public Law (PL) 102-245 may be used with any quantity of units.
- (b). Regular excess procedures if the quantity of units is ten or less.
- (c). Exchange sale through GSA may be used for large accumulations of equipment.
- (d). If the location quantity is three or less units, donation to public bodies (i.e., Federal Agencies, public libraries, Indian Tribes) is authorized under PL 102-245.

14. CHAPTER FOURTEEN: NETWORK ACCESS SECURITY POLICY

a. General Policy Statement

This policy establishes requirements for the secure access and transmission of data on all USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) networks to prevent unauthorized use or misuse of Federal Government information. The following guidelines shall be followed:

- (1). All servers, network devices, or appliances hosting information or resources accessed from the Internet shall be placed in a De-Militarized Zone (DMZ) network segment which is separated from the Internet and separated from the OCIO-ITS network by a firewall.
- (2). All Internet Service Providers (ISP) shall be approved by the Change Control Board (CCB) prior to installation.
- (3). Firewalls and Intrusion Detection Systems (IDS) and router-based Access Control Lists (ACL) shall be used to control, restrict, and monitor all network traffic to and from the OCIO-ITS networks.
- (4). All network traffic between OCIO-ITS locations shall be transported on dedicated OCIO-ITS owned circuits or through a Virtual Private Network (VPN) connection meeting encryption levels set by OCIO-ITS Security Policies.
- (5). No OCIO-ITS office shall have Internet connectivity other than the connectivity provided by the OCIO-ITS.

b. Policy Detail

(1). Warning Banners

- (a). The following Warning Banner will appear prior to system/network logon in order to provide fair notice on proper use to those attempting to access USDA systems and networks, including routers, switches, and workstations. Waivers in language will be considered if the OCIO-ITS has a requirement to use stronger verbiage in this banner.

- (b). Warning Banner:

Unauthorized access to this United States Government Computer System and software is prohibited by Title 18, United States Code 1030. This statute states that: Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States shall be punished by a fine under this title or imprisonment for not more than 10 years, or both.

All activities on this system and network may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crime found on USDA computer systems. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING OR CAPTURING AND DISCLOSURE. **REPORT UNAUTHORIZED USE TO AN INFORMATION SYSTEMS SECURITY OFFICER.**

(2). Remote Access

- (a). General Access

Chapter Fourteen: Network Access Security Policy

1. Client side or personal firewalls shall be installed and configured on each computer used to remotely access OCIO-ITS networks or applications.
 2. Government-owned computer equipment, software, and communications are required for remote connection to an OCIO-ITS network or computer system.
 3. Remote access privileges to any OCIO-ITS modem pool shall follow existing USDA remote access and approval guidelines as described in CS-029 Cyber Security Guidance Regarding Telework and Remote Access, [Part 3, Telework and Remote Access Security](#) or its replacement.
 4. The OCIO-ITS Information Systems Security Program Manager (ISSPM) shall control and monitor remote access usage by individual users.
 5. Government-owned laptops must be adequately protected by current antivirus software and must be consistently configured to ensure security against known vulnerabilities in operating systems and application software. Refer to Chapter 16: Patch Management Security Policy, and Chapter 27: Virus Protection Security Policy, or their replacements, for additional information.
 6. All remote access connections shall comply with Chapter 3: Authorization and Access Control Security Policy or its replacement.
 7. All remote servers, workstations, laptops, and Portable Electronic Devices (PED) shall be equipped with antivirus software that is kept current with the latest virus signatures.
 8. Reconfiguration of equipment used for remote access into the OCIO-ITS network is not permitted for any reason or purpose.
 9. All security incidents or violation of this policy shall be reported in accordance with Chapter 10: Incident Identification, Declaration, Reporting, and Handling Security Policy or its replacement.
 10. All remote users shall be disconnected after 30 minutes of inactivity.
- (b). Dial-Up Access
1. Circuits used by OCIO-ITS telecommunications personnel for direct connectivity and/or emergency purposes are permitted. The telecommunications staff shall maintain a listing of telecommunication lines, their location, and purpose. Updated listings shall be provided to the Information Systems Security program Manager (ISSPM) as changes are made. Access to use these emergency lines shall be tightly controlled.
 2. Routers for dedicated ISDN lines configured for access to the OCIO-ITS network shall meet minimum authentication requirements of Challenge-Handshake Authentication Protocol (CHAP).
 3. All installations and use of modems or dial-up solutions shall first obtain written approval from the ISSPM.
 4. Passwords used for dial-up authentication shall be changed at a minimum of every 30 days.
- (c). Internet Access
1. All network connections established with OCIO-ITS networks from the Internet shall be protected by a Virtual Private Network (VPN).
 2. All VPN solutions shall use encryption and authentication schemes that comply with the OCIO-ITS Security Policy Manual or its replacement.
 3. A list of currently used ports shall be maintained and kept current by the network administrator.
 4. Only those protocols and ports required to perform remote functions are to be permitted by the firewall.

Chapter Fourteen: Network Access Security Policy

5. Distributed file sharing (i.e., Windows SMB file shares, SAMBA file shares, Network File Systems) shall only be used by remote users/sites when connected through secured access, i.e., VPN access, authenticated dial-up connection, dedicated secure line, etc.
 6. ISSPMs shall periodically scan remotely connected systems for security vulnerabilities.
- (d). Other OCIO-ITS or Partner Connections
1. Connections between third parties that require access to non-public OCIO-ITS resources fall under this policy section, regardless of whether a Telco circuit (such as frame relay or ISDN) or VPN technology is used for the connection.
 2. All new extranet connectivity shall go through a security review with the ISSPM. These reviews shall ensure that all access matches the business requirements in the best possible method, and that the principle of least access is followed.
 3. Sponsoring organizations that wish to establish connectivity to a third party shall file a new site request with the telecommunications group. The telecommunications group shall engage the security office to address security issues inherent in the project. The sponsoring organization shall provide full and complete information as to the nature of the proposed access to the telecommunications group and the security office, as requested.
 4. All connectivity established shall be based on the principle of least access in accordance with the approved business requirements and security review. In no case shall the OCIO-ITS rely upon the third party to protect networks or resources.
 5. All changes in access shall be accompanied by a valid business justification and are subject to a security review. The sponsoring organization is responsible for notifying the telecommunications group and/or the security office when there is a significant material change to their previously provided information so that security and connectivity evolve accordingly.
 6. When access is no longer required, the sponsoring organization shall notify the telecommunications group responsible for that connectivity, which shall then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate.
 7. The telecommunications group shall conduct an audit of the respective extranet connections on an annual basis to ensure that all existing connections are still needed and that the access provided meets the needs of the connection. Connections that are no longer being used to conduct business shall be terminated immediately.
- (e). Remote Control
- All remote control programs that permit a user to manage another computer over a network connection shall comply with the following principles:
1. The ISSPM shall provide guidance on the implementation the security features in your selected software package.
 2. All remote control hosts shall require a username and password to establish a connection. Anonymous access is prohibited.
 3. Remote control software shall retain log files and audit trails showing all access and failed access.

(3). Telework

- (a). General Requirements

Chapter Fourteen: Network Access Security Policy

1. Telework, also known as telecommuting, flexiwork, and flexiplace, is not considered an employee right. Supervisors and/or the applicable ISSPM can suspend or terminate an individual's privilege to participate in the Telework program at any time. Accordingly, the appropriate disciplinary actions shall be taken against the individual.
 2. An employee who participates in the Telework program on a regular and recurring basis shall certify in writing the security level of the official information used outside the primary work-site and the protection of Government-owned equipment and property.
 3. Only Government-owned equipment, software, and materials shall be used for Telework duties.
 4. Government-owned equipment shall only be used for official duties. Only Telework participants are authorized to use Government-furnished equipment.
 5. The employee shall return all Government-owned equipment, software, and materials at the conclusion of the Telework arrangement or at the request of OCIO-ITS.
 6. The Government retains the right to inspect the home or alternate work-site and the equipment used by an employee to ensure that proposed work-sites are safe and that all equipment is adequately installed, maintained, and secured.
- (b). Privacy Act, Sensitive or Classified Data
1. Decisions regarding the proper use and handling of sensitive data, as well as records subject to the Privacy Act, are delegated to individual supervisors who permit employees to work at home.
 2. Care shall be taken to ensure those records subject to the Privacy Act and sensitive data are not disclosed to anyone except to those who are authorized access to such information in order to perform their duties. Organizations allowing employees to access records subject to the Privacy Act from a remote work site shall maintain appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the records.
 3. Due to the sensitive nature of payroll and personnel databases, applications not normally accessible using public web browsers, shall not be accessible to Telework participants.
- (c). Data Access for Telework Participants
1. All sensitive data shall be encrypted when transmitted. Encryption software shall be loaded on Government-owned equipment for Telework participants accessing sensitive data.
 2. Participants shall be trained to use the software package provided.
 3. Where employees work on an ad hoc basis, personal computers can be used to work on limited amounts of sensitive unclassified material, on the basis that the employee shall delete the files as soon as they are no longer required and verify in writing that such action has been completed. Supervisors shall pre-approve such arrangements.
 4. Correspondence files and historical records are likely to be one-of-a-kind and may not be taken from the primary work-site. Since these records exist mainly in hard copy, they are inaccessible via electronic means. Scanners and imaging systems (copiers) may be used to reproduce records for use off-site if needed.
- (d). Computer Security Requirements
1. Only hardware/software configuration procured by the Federal Government and authorized by the OCIO-ITS shall be installed at the Telework location. Under no

Chapter Fourteen: Network Access Security Policy

circumstances shall users be allowed to add non-Government-owned or unauthorized hardware or software to the home workstation if Government-owned.

2. Government-owned computers utilized in support of the Telework program shall be loaded with the latest version of the common computing core load, applicable remote access software and a data encryption package, if required. Telework supervisors shall notify the information technology staff of any additional software requirements of the participant.
3. Remote telecommunication access to Government computers presents special security concerns. A combination of physical controls, unique user identifiers, passwords, terminal identifiers, access control software, and strict adherence to security procedures is required to protect the information from unauthorized access.
4. Telework participants shall comply with security procedures to protect Government information stored on magnetic media of workplace computers when the computers are repaired or serviced. Where the hard disk of a computer is inoperable, arrangements shall be made to remove sensitive information from the hard disk prior to having the computer serviced in accordance with Chapter 13: Media Sanitization and Disposal Security Policy or its replacement.

(e). Help Desk Support

1. Telework participants shall be provided the same type and availability of help desk service that would be available to them in the traditional work-site.
2. Due to the limited nature of face-to-face troubleshooting, employees must be prepared to assist the help desk staff remotely. For example, employees shall be willing and capable of following detailed systematic instructions over the telephone to assist the help desk staff in troubleshooting and resolving issues.
3. Situations that cannot be resolved remotely may require that the participant transport the equipment to the primary work-site for further evaluation.

(4). Wireless Technology

Wireless technology is a new telecommunications media that is being explored. However, due to inherent security risks associated with wireless technology, an approved waiver is required. The OCIO-ITS ISSPM will monitor the usage of wireless technology within the ITS and Service Center Agency (SCA) environments.

15. CHAPTER FIFTEEN: NON-GOVERNMENT OWNED LAPTOP COMPUTER AND PED SECURITY POLICY

a. General Policy Statement

- (1). All non-Government issued laptop computers shall be inspected by USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) Information Systems Security Program Manager (ISSPM) or designated representative prior to connecting to any OCIO-ITS network or computer resource. The inspection shall include scans and system checks to ensure all devices are safe and meet OCIO-ITS standards. If the device is found to be safe, an authorization shall be given for that device. Non-Government issued laptop authorizations for use must expire after five working days or after the laptop computer leaves the Government premises that issued the authorization.
- (2). Use of non-Government owned Portable Electronic Devices (PED) is prohibited in the OCIO-ITS information resource environment.
- (3). The ISSPM shall assist the laptop owner to mitigate any vulnerability found during the inspection. The ISSPM requests a 48-hour advance notice of inspections to ensure equipment and personnel are available. Long-term use non-Government issued laptops shall require the submission of a waiver to the ISSPM for approval.
- (4). Laptop computers and PEDs provided to employees as awards are not considered Government-owned devices and shall be deemed to be of non-Government issue.
- (5). For information on the use of Wireless Technology, refer to Chapter 14: Network Access Security Policy or its replacement.

b. Policy Detail

(1). Non-Government Owned Laptop Computers Security

(a). Inspections

1. File and printer sharing must be disabled or secure on all laptops.
2. Use of passwords is required to enter the system in accordance with Chapter 3: Authorization and Access Control Security Policy or its replacement.
3. Encryption must be available on tested laptop computer equipment and must meet or exceed levels set in the OCIO-ITS Security Policies.
4. All laptop computers must be compliant with Chapter 27: Virus Protection Security Policy or its replacement.
5. All laptops shall be scanned for vulnerabilities. All discovered vulnerabilities shall be corrected prior to authorization.
6. After a non-Government issued laptop computer has completed the inspection process and is found to be safe, the inspecting ISSPM shall issue an authorization form, specifically the Network Remote Access Authorization Form.
7. All non-Government owned laptop computers shall have an OCIO-ITS approved/current version of antivirus software (i.e., McAfee, Norton, etc.) installed prior to connecting to any OCIO-ITS network or computer source.

(b). Personal Usage

1. On-site laptop computer usage is restricted to business purposes only with exception to limited personal use.
2. While connected to Government networks, users are bound to adhere to the “Standards of Ethical Conduct for Employees of the Executive Branch.” Laptop computers shall not be used to generate, view, send, or store harassing e-mail, pornography, or similar text and sound files.

Chapter Fifteen: Non-Government Owned Laptop Computer and PED Security Policy

(c). Access Control

1. All sensitive information stored electronically shall be saved either as an encrypted file within an encrypted folder, or onto an encrypted drive. All sensitive data transmitted shall also be encrypted.
2. Users entering and exiting a Federal facility with laptop computers are expected to carry their access authorization form with the device.
3. Laptop computers shall use a password-enabled screen saver to further protect data integrity and confidentiality when working outside the office perimeter.
4. Before non-Government issued laptops are removed from Government premises, all sensitive data files shall be removed from them.
5. All laptop computers shall require a password on startup. All passwords are to comply with the current OCIO-ITS password policy in accordance with Chapter 3: Authorization and Access Control Security Policy or its replacement.

(2). Non-Government Owned Portable Electronic Devices (PED)

- (a). Non-Government owned PEDs are not permitted. PEDs include, but are not limited to, non-Government owned/issued cellular phones including picture and movie-enabled phones, pagers, text messaging devices, and wireless e-mail devices such as Blackberries, hand-held scanners, PDAs, voice recorders, and flash memory.
- (b). Users shall not attempt to connect non-Government owned PEDs to any OCIO-ITS network or computer resource.

16. CHAPTER SIXTEEN: PATCH MANAGEMENT SECURITY POLICY

a. General Policy Statement

This policy establishes requirements for a secure patch management program for all USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) networks to prevent unauthorized use or misuse of Federal Government information. The patch management program shall be used to create a consistently configured environment that ensures security against known vulnerabilities in operating systems and application software. A key component of patch management is the intake and selection of information regarding both security issues and patch release. OCIO-ITS must be aware of which security issues and software updates are relevant to the environment.

b. Policy Detail

(1). Patch Prioritization and Scheduling

(a). Normal Application of Patches and Updates to Systems

The patch cycle shall be used to facilitate the application of standard patch releases and updates. This cycle can be time or event based. For example, the schedule can mandate that system updates occur quarterly or a cycle may be driven by the release of service packs or maintenance releases. In either instance, modifications and customizations shall be made based on availability requirements, system criticality, and available resources.

(b). Critical Security and Functionality Patches and Updates

Criticality shall be the measure used by the OCIO-ITS to determine the priority of patch deployment. A number of factors shall be considered when determining patch priority and scheduling urgency:

1. Vendor-reported criticality (i.e., high, medium, low) is a key input for calculating a patch's significance and priority as is the existence of a known exploit or other malicious code that uses the vulnerability being patched as an attack vector.
2. System criticality (i.e., the relative importance of the applications and data the system supports to the overall business).
3. System exposure (i.e., DMZ systems vs. internal file servers vs. client workstations).

(2). Patch Testing

Verification of the patch's source and integrity is an important step that ensures the update is valid and has not been maliciously or accidentally altered. Once a patch has been determined valid, it shall be placed in a test environment that closely mirrors the production environment. Critical applications and supported operating platforms must be fully accounted for while testing the patch infrastructure. However, detailed patch testing will be dictated by system criticality and availability requirements, available resources, and patch severity.

(3). Change Management

Change management practices are required by OCIO-ITS to be applied to the patch management process. Once a configuration-managed item has been identified for change, a Request for Change (RFC) must be submitted and the configuration shall be modified according the procedures established by the change management process.

Chapter Sixteen: Patch Management Security Policy

(4). Audit and Assessment

The audit and assessment process is used to verify that the systems to be updated were actually patched. Reports shall be generated that will be used to drive the effort toward consistent installation of patches and updates across the organization. Finally, controls should be in place to ensure that newly deployed and rebuilt systems are up to desired specifications with regard to OCIO-ITS patch level requirements.

(5). Notification of Users

In the event that patches may be uploaded to workstations or servers in an automated fashion, no announcement will normally be made to the user community. Warnings or notices to users shall only occur in the event that significant news has been released to the public or if the update requires any special action on the part of the users or administrative personnel.

17. CHAPTER SEVENTEEN: PHYSICAL ACCESS SECURITY POLICY

a. General Policy Statement

This policy establishes physical security standards for Large Information Technology (IT) Facilities and Field Offices of the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS). This includes IT Restricted Space requirements for IT Centers, Web Farms, Sensitive Compartmented Information Facilities (SCIF), and De-Militarized Zone (DMZ) computer equipment to protect information resources from risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction. This protection shall be afforded through layered physical security, high data security, and effective security procedures. Successful IT security protection will dictate the physical control of restricted space that contains major OCIO-ITS computer and telecommunications resources.

b. Policy Detail

(1). Large IT Facility Security Requirements

OCIO-ITS buildings that house Web Farms, Sensitive Compartmented Information Facilities (SCIF), and De-Militarized Zone (DMZ) equipment shall be automatically considered Critical IT facilities and must provide a level of physical security commensurate with that designation. Physical security requirements of Large IT Facilities are:

- (a). Facility parking shall be controlled; signs will be posted, and arrangements shall be made for the immediate towing of unauthorized vehicles. Adequate lighting shall be provided for parking areas.
- (b). Closed Circuit Television (CCTV) surveillance cameras with time-lapse video recording shall be utilized.
- (c). Lighting with emergency power backup shall be utilized.
- (d). Facilities shall be controlled by armed security guards and intrusion detection systems with a central monitoring capability maintained to current life safety standards.
- (e). Electronic security locks shall be installed and used on all entrances and exits.
- (f). Photo IDs shall be required for all personnel and these IDs shall be displayed at all times; visitors shall be controlled and screened.
- (g). Utility access shall be restricted to authorized personnel; emergency power shall be provided to all critical systems (alarms, radio communications, computer facilities, etc.).
- (h). Specific security construction guidance can be found in the ISC Security Design Criteria for many of the above requirements.
- (i). Annual Security Awareness Training shall be conducted for all OCIO-ITS Federal employees and contractors that possess access to the facility information systems and networks.
- (j). Occupant Emergency Plans (OEP) shall be implemented in all Large IT Facilities and shall be updated and tested annually.

(2). IT Restricted Space within Large Office IT Facilities

(a). General Restrictions

1. IT Restricted Space shall only be managed by designated OCIO-ITS Federal employees. Although contractors may be permitted to control the operations within these controlled environments, they are not permitted to directly manage IT Restricted Space.”
2. New and/or planned specifications for IT restricted space shall contain a requirement that the issue of physical security will be coordinated with the

Chapter Seventeen: Physical Access Security Policy

Information Systems Security Program Manager (ISSPM) during the design phase to ensure compliance with this policy.

3. ISSPM deputies shall perform annual reviews to ensure IT restricted space complies with the policies set in this document and other OCIO-ITS Security Policies. Deficiencies shall be reported to the ISSPMs.
4. Each restricted area shall have an OCIO-ITS Federal employee designated to oversee physical security policies for that section. This individual is responsible for performing security evaluations including monthly access log reviews and periodic inspections.
5. A Physical Security Checklist shall be used. This checklist is used as part of the Certification and Accreditation (C&A) review process and on individual Service Center Agency location site reviews to determine compliance with USDA policy and federal directives concerning information security.

(b). Physical Restrictions

1. All computer rooms shall be located in the interior of the building away from exterior windows. Consideration shall be given to its proximity to public areas such as training rooms, cafeterias/vending areas, and rest rooms. Computer rooms shall not be located either above or below public areas in multi-story buildings.
2. A roving security guard will inspect entrances to IT restricted spaces for signs of forced entry on a daily basis.
3. Weapons are not allowed in IT restricted spaces with the exception of an armed security guard, police officer, or U.S. Armed Forces personnel.
4. All mail and/or packages being delivered to the computer room shall be physically examined and x-rayed (where available). All mail and/or packages shall be recorded in a logbook.
5. Periodic inspections of the door locking mechanism will be conducted to assure that hardware cannot be easily manipulated to gain unauthorized access.
6. Signage indicating IT Restricted Space locations is prohibited.
7. Critical or sensitive asset locations shall not be advertised or displayed to the public including floor plans, directories, or building maps.
8. Computer rooms shall be designed and built in accordance with the ISC Security Design Criteria for Federal Buildings (where possible).
9. The computer rooms shall be protected by a fire suppressant system in accordance with local building and fire codes, preferably dry-pipe.
10. The number of entrances to a computer room shall be kept to the minimum required by local building and fire codes.
11. Activities with visitor populations shall be located as far away from the computer room as practical.
12. Mailrooms shall not be located in close proximity to the computer room (where possible).
13. Storage areas and loading docks shall not be located in close proximity to the computer room (where possible).
14. Glass doors or large windows shall not be used in computer rooms.
15. Metal clad doors or solid wood doors with a 2-hour fire rating shall be used at all computer room entrances and exits.
16. Entrance to the computer room shall be electronically controlled with the capability of providing an audit trail.
17. Exterior computer room doors having key access hardware shall be removed from the master key system of the facility.
18. The issuance of non-master keys shall be strictly controlled and strictly limited.

Chapter Seventeen: Physical Access Security Policy

19. The use of intrusion detection system shall be used on all computer room entrances.
 20. The access control and intrusion detection systems shall have Uninterrupted Power Supply (UPS) backup.
 21. Exterior computer room doors shall have either interior hinges or exterior hinges with non-removable pins.
 22. The facility housing the computer room shall have an Occupant Emergency Plan.
 23. Periodic inspections of the door locking mechanism, intrusion detection, fire suppression, and access control systems shall be conducted to assure proper working order.
- (c). Personnel Security Restrictions
1. Only authorized Federal employees and contractors having an ongoing recurring business need shall be given unescorted access to the computer room. Review of this access shall be performed by management on a monthly basis to minimize the number of people granted access.
 2. Any employee or contractor that no longer has a business need to enter restricted space shall be immediately removed from the access control system.
 3. Approved USDA Federal identification cards (with photo) shall be required for all OCIO-ITS employees and authorized contractors (with an ongoing, recurring business need to enter the IT restricted area) and this ID shall be displayed at all times while in the building.
 4. Visitors shall be screened by armed security personnel to include the examination of photo identification and the physical examination and x-ray of all personal items to include, but not limited to, outerwear (coats, jackets), handbags, personal organizers, briefcases, computer laptops and other personal electronic devices. Metal detection equipment, including the use of metal detection wands, shall be used to examine each visitor prior to being permitted access to the facility.
 5. Visitors shall be kept to a minimum; tours by non-USDA personnel are prohibited.
 6. A sign in/sign out logbook shall be required for all escorted visitors; as a minimum requirement, the logbook shall contain the printed identity of each visitor to include the visitor's signature, USDA Agency/company represented, purpose of visit, date/time in and date/time out.
 7. Cleaning and maintenance personnel shall be escorted at all times by Federal employees or contractor personnel.
 8. A Federal employee or contractor who has knowledge of the system requiring maintenance shall escort non-permanent contractors needing access to equipment at all times.
 9. A quarterly access review shall be conducted by designated GSA employees or contractor personnel (i.e., maintenance) having an ongoing business need in all restricted space.
- (d). Web Farm Restrictive Requirements
1. Web Farms located in rooms other than a secure computing facility shall be subject to the same physical security requirements as if it was co-located. These rooms must have Web Farm computing equipment contained in secured cabinets.
 2. Cabinets housing network equipment shall not be visible to the public.
 3. Cabinets storing network equipment shall remain locked (if available) at all times. Keys for the cabinet shall have minimal distribution and shall be safeguarded. If available, keys shall be stored in the office safe.
 4. Access shall be restricted to key staff members only.

Chapter Seventeen: Physical Access Security Policy

5. A security log (in either paper or electronic form) shall be kept of all staff access. The log shall include date, name, organization, and purpose. Field Office management shall periodically review the log for unusual entries.

(3). Facility Security for Field Offices

- (a). OCIO-ITS Field Offices are not required to maintain Large IT Facility security standards, i.e., mandatory design criteria, ceiling fire suppressants, metal fire doors, electronic access with audit trail, IDS at entrances, IDS with UPS backup, etc. However the information processed within the Field Offices is sensitive in nature and shall be safeguarded. Facility security for Field Offices shall be maintained relative to office size and physical location issues, commensurate with the neighborhood environment. The following are the minimum facility requirements for Field Offices:
 1. Computer equipment shall be secured and logged off at the end of the workday. Mobile computer equipment such as computer laptops and/or Personal Electronic Devices (PEDs) shall be secured when they are not in use.
 2. Field Office employees shall be familiar with emergency and evacuation procedures. Periodic fire and emergency evacuation drills shall be conducted. Emergency computer equipment shutdown procedures shall be documented and periodically tested.
 3. Due to the remote locations of the Field Offices, the ISSPMs shall rely upon Field Office management to perform annual physical security reviews. These reviews shall be performed in conjunction with the annual security plan. Review reports shall be submitted with the security plan to the ISSPM.
 4. At a minimum, each Field Office shall have emergency lighting, fire and/or smoke detection, and suppression systems such as fire extinguishers or automated sprinkler systems (if available). Portable fire extinguishers shall be maintained and checked annually.
 5. Computer equipment shall be located in an area restricted to authorized Federal employees and contractors only. The area shall be free of obstruction and kept organized.
 6. Office door keys shall be controlled and the distribution of these keys shall be periodically verified by Field Office management.
 7. A security log for visitors and employees shall be maintained for all Field Office facility access outside of established business hours. All log files shall be periodically reviewed.
 8. Local police or security guards should regularly patrol and check the Field Office buildings during non-business hours.
 9. Access to the Field Office computer room shall be controlled by protection systems to include keyed entry locks, keycard systems, and guards (when possible).
 10. Computers that process sensitive data shall be protected from the intentional and/or unintentional viewing by unauthorized individuals. The public nature of the Field Offices requires employees to be conscientious in protecting sensitive data from access by visitors.
- (b). Field Office CCE Network Cabinet Security
 1. Cabinets housing network equipment shall not be visible to the public.
 2. Cabinets storing network equipment shall remain locked (if available) at all times. Keys for the cabinet shall have minimal distribution and shall be safeguarded. If available, keys shall be stored in the office safe.
 3. Access shall be restricted to key staff members only.

Chapter Seventeen: Physical Access Security Policy

4. A security log (in either paper or electronic form) shall be kept of all staff access. The log shall include date, name, organization, and purpose. Field Office management shall periodically review the log for unusual entries.

18. CHAPTER EIGHTEEN: PRINTER MANAGEMENT SECURITY POLICY

a. General Policy Statement

- (1). This policy establishes guidelines for the management and protection of network single-function printers and multipurpose printers (i.e., printer/facsimile/scanner/copier) used within the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS).
- (2). Improperly configured printers may permit the retrieval of sensitive information, thus impacting OCIO-ITS operating system settings or print data integrity. Should printer integrity be lost due to malicious software (malware), the printer has the potential to function as an agent for distributing viruses or initiate a Denial of Service (DoS) attack on every device present on the OCIO-ITS network.

b. Policy Detail

(1). Printer Management Access

- (a). All new variances of printer devices when procured under an enterprise purchase order must be scanned before connecting to the network in accordance with Chapter 28: Vulnerability Scan Security Policy or its replacement.
- (b). Printers made available through any other source must be scanned on an individual basis.
- (c). Access to printer configuration control settings shall be limited to authorized personnel only. All administrative accounts shall comply with the password requirements defined in Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (d). All non-essential services must be removed immediately from the network printer.
- (e). The printer's Administrator Account, i.e., the original administrative account of the printer, shall be renamed and used on a limited basis. Only select administrator personnel shall be permitted to have knowledge of this account's credentials.

(2). Waiver and Configuration Change Requests

- (a). Requests for Changes (RFC) to the standard printer configuration shall be submitted in writing to the Change Control Board (CCB) for review. In the event that a waiver to secured printing operation is necessary, waiver requests shall include the reason and timeframe for the requests as well as all known risks, threats, and issues associated with this change. Only after security office approval shall system administrator personnel proceed with processing the waiver.
- (b). Any waiver affecting the network environment shall require formal approval by the OCIO-ITS Information Systems Security Program Manager (ISSPM). All workstations connecting or joining to any enterprise domain shall comply with all security configurations and standards established by configuration management and shall be approved by the CCB before connecting or joining any enterprise domain.

(3). Network and Multipurpose Printer Services

OCIO-ITS network single-function and multipurpose printers shall not host any services to include, but not limited to DNS, DHCP, FTP, Site, and Telnet. All printer services not required for system functionality shall be disabled.

(4). Special Provisions for Large Scale Printer/Copy Stations

Chapter Eighteen: Printer Management Security Policy

- (a). Large scale printer and/or copier stations that may be used in Large Office environments (i.e., State Office level and above) are subject to special interface requirements.
- (b). Large scale printer/copier stations shall not contain Network Interface Cards (NIC) in the enterprise system if:
 - 1. These devices retain images in memory as a thief could violate Sensitive But Unclassified (SBU) customer and business information.
 - 2. IT System Administrators have no access or control, i.e., the management of that specific system.
 - 3. This hardware has unapproved drivers; currently none are specifically approved.
- (c). Where as a business need is evident for this resource, security is currently not comprehensive enough to sustain interaction to the network infrastructure.
- (d). Resources to bring these systems into security compliance are identified for the future.

(5). Incident Reporting and Response

In the event of a security vulnerability or breach, malicious activity, successful attack, or violation of this policy has been discovered or suspected, an incident shall be reported in accordance with Chapter 10: Incident Identification, Declaration, Reporting, and Handling Security Policy or its replacement.

19. CHAPTER NINETEEN: PRIVACY IMPACT ASSESSMENT SECURITY POLICY

a. General Policy Statement

This policy establishes requirements for the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) to ensure the privacy, confidentiality, integrity, and availability of customer and employee information. The OCIO-ITS shall recognize that privacy protection is both a personal and fundamental right of its customers, including Federal employees, contractors, and partners. Among the most basic of rights is an expectation that OCIO-ITS will protect the confidentiality of personal, financial, and employment information. Customer, Federal employee, and contractor information is protected by the Privacy Act of 1974, as Amended (5 USC 552a), the Computer Security Act of 1987 (Public Law 100-235), OMB Circular A-130 - Management of Federal Information Resources, and the Freedom of Information Act as Amended (5 USC 552).

b. Policy Detail

(1). Privacy Impact Assessment

- (a). The Privacy Impact Assessment (PIA) shall be initiated during the early stages of the development of a system and completed as part of the required Systems Development Life Cycle (SDLC) reviews. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design.
- (b). Both the system owner and system developers shall work together to complete the PIA. System owners must address what data is to be used, how the data is to be used, and who will use the data. The system developers must address whether the implementation of the owner's requirements presents any threats to privacy.
- (c). New systems, systems under development, or systems undergoing major modifications are required to complete a PIA. The Privacy Policy Analyst reserves the right to request that a PIA be completed on any system that may have privacy risks. More specifically:
 1. New systems and systems under development or undergoing major modifications are required to complete a PIA.
 2. Legacy systems, as they exist today, are not required to complete a PIA. However, if the automation or upgrading of these systems puts the data at risk, the Privacy Policy Analyst may request a PIA.
 3. Currently operational systems are not required to complete a PIA. However, if privacy is a concern for a system the Privacy Policy Analyst can request that a PIA be completed. If a potential problem is identified concerning a currently operational system, the OCIO-ITS will use best or all reasonable efforts to remedy the problem.

(2). SDLC Methodology

The PIA shall incorporate privacy into the development life cycle so that all system development initiatives can appropriately consider privacy issues from the earliest stages of design.

- (a). Training on the PIA will be available to both Federal employees and contractors upon request from the Office of the Chief Information Officer.
- (b). The PIA document will be initially completed by the system owner and system developer to answer privacy-related questions.

Chapter Nineteen: Privacy Impact Assessment Security Policy

- (c). During the development of the PIA document, the Office of the Chief Information Officer will be available to answer questions related to the PIA process and other concerns that may arise with respect to privacy.
- (d). The Privacy Policy Analyst will work with the system owner and system developer to develop design requirements to resolve the identified risks. If known system risks cannot be resolved with the Privacy Policy Analyst, the risks must be presented to the Chief Information Officer.
- (e). The SDLC review process will be used to validate the incorporation of the design requirements to resolve the privacy risks. Formal approval will be issued in accordance with the SDLC as defined in CS-009, Cyber Security Configuration Management Guidance, or its replacement.
- (f). The completed PIA document is to be submitted to the Office of the Chief Information Officer for review. The PIA is a requested deliverable required to attain formal Certification and Accreditation (C&A).

20. CHAPTER TWENTY: RISK MANAGEMENT SECURITY POLICY

a. General Policy Statement

Protection of information assets and maintaining the confidentiality, integrity, and availability of USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) information technology assets and telecommunications resources are vital in meeting the USDA's overall program delivery requirements. Implementation of security measures such as a risk management program, effective security controls, certification and accreditation of information systems, and updated security plans are vital components.

b. Policy Detail

The OCIO-ITS will perform formal Risk Assessments (RA) of all IT systems. RAs will be conducted using the same processes and procedures as defined in the [DM3540-000 Risk Management Program](#), dated August 19, 2004, inclusive of [Table 1: USDA Risk Assessment Methodology](#) dated, dated February 11, 2003, or their replacements. Risk assessments typically identify risks that a system could be affected by. Risk mitigation plans are required as a follow-up document to an RA.

A formal system risk analysis is required every three years or when a major change is made in a General Support System (GSS) or Major Application (MA). Major changes are defined as modifications to the system that affect the security controls and which render the system vulnerable to compromise or intrusion. Waiver requests will be considered for extensions in compliance time only; all IT systems will undergo regular risk assessments. The OCIO-ITS will include the cost for IT system mitigations in budgetary planning and prepare a business case to ensure that funding is available to implement protection against identified vulnerabilities.

21. CHAPTER TWENTY-ONE: ROUTER AND SWITCH MANAGEMENT SECURITY POLICY

a. General Policy Statement

This policy establishes requirements for access to USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) router and switch resources. These environments shall require authorization and access control through the use of individual credentials as outlined in Chapter 3: Authorization and Access Control Security Policy or its replacement. Where possible, the Terminal Access Controller Access System (TACAS+) is to be used for authentication. Additionally, the use of local system accounts shall be limited and used on an exception basis.

b. Policy Detail

(1). Router and Switch Configuration

- (a). Configuration standards and management procedures shall be used to control usability, efficiency, and security of the overall router and switch environment, and shall be kept in a Trusted Facility Manual (TFM) in accordance with Chapter 5: Certification and Accreditation Security Policy or its replacement. These standards and other procedures shall be followed when designing, implementing, or managing router and switch configurations. Written approval from the Change Control Board (CCB) is required to deviate from these standards.
- (b). The following shall be disallowed on all routers and switches:
 1. IP direct Broadcasts
 2. Incoming packets with invalid source address.
 3. TCP and UDP small servers
 4. Router web services
- (c). All routers and switches shall use Access Control Lists (ACL) to only permit traffic that has a recognizable business need.
- (d). Traffic shall be denied unless permitted.
- (e). All security related service packs, patches, and hot-fixes shall be tested and applied to all routers and switches in a timely manner.
- (f). All routers and switches must present and display a warning banner in accordance with Chapter 14: Network Access Security Policy or its replacement.
- (g). All back-up media shall be kept in a secured manner consistent with Chapter 17: Physical Access Security Policy, or its replacement, and be protected by a password.
- (h). A selected portion of backup media shall be kept in an alternate physical location and shall be secured in a manner consistent with Chapter 17: Physical Access Security Policy or its replacement.
- (i). The Administrator/Root Account is the original administrative account of the router and switch. This account shall be renamed and used only on a limited or emergency basis. Only select administrative personnel shall have knowledge of these account credentials, which must be stored in a locked environment.

(2). Router and Switch Management

- (a). All routers and switches shall be physically secured in accordance with Chapter 17: Physical Access Security Policy or its replacement.
- (b). All routers and switches shall be backed up in a manner that permits a complete recovery of routers and switches on a weekly basis. Archives of router and switch backups shall be maintained until no longer required by management.

Chapter Twenty-One: Router and Switch Management Security Policy

- (c). Any prolonged or delayed application of a security-related service pack, patch, or hot-fix shall be documented and an application for a wavier to this policy must be applied for.

(3). Router and Switch Management Access

- (a). Access to router and switch consoles and operating systems shall be limited to network administrator personnel only. All router and switch user accounts shall comply with password requirements in accordance with Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (b). Permitted access shall be limited to only essential users and service accounts.
- (c). Only one person shall have access to one user account - that is, more than one person shall not have access to the same account.
- (d). All network administrators shall receive the appropriate level of training to perform their duties in a competent manner.

(4). Router and Switch Information Access

Access to router and switch information shall be restricted to the network administrator, CCB, OCIO-ITS Information Systems Security Program Manager (ISSPM) or designated representative, and/or persons with written permission from the CCB or ISSPM. Restricted information shall minimally include documents, details, drawings, diagrams, or screen prints containing any information regarding router and switch configurations, installed applications, data storage, scripts, pass codes, or log files. Any account with administrative privileges shall be issued to network administrators only.

(5). Router and Switch Logs

- (a). All routers and switches shall maintain and record security auditing events to logs.
- (b). All routers and switches shall log security auditing events that display both successful and unsuccessful incidents.
- (c). All log files and events shall be managed in a manner that maintains their integrity and authenticity. These logs are to be stored or archived for a minimum of six (6) months.
- (d). Requests for access to router and switch logs shall be made to the appropriate network administrator and Agency ISSPM.
- (e). Event logs shall be reviewed by the network administrator and ISSPM or designated representative on a regular basis.

(6). Change Request

Change requests for any modifications to a router and switch system, configuration, or design shall be submitted in writing to as a Request for Change (RFC) following Change Management (CM) procedures. All change requests shall include the reason and timeframe for the request as well as all risks, threats, and known issues associated with this change. Only after CCB approval shall network administrator personnel proceed with the router and switch changes. Any changes from the original design once approved, and not yet implemented or in the process of implementation, will require a formal change request form.

(7). Router and Switch Implementation

A request for implementation of new routers and switches shall be submitted to the CM. This request shall include all configuration settings together with other pertinent system information. Only after obtaining approval from the CCB shall authorized personnel proceed with the router and switch implementation.

Chapter Twenty-One: Router and Switch Management Security Policy

(8). Implied Authority

- (a). All network administration personnel have the implied authority and responsibility to take action(s) to protect OCIO-ITS assets from loss without approval from the CCB in an emergency only to include modifying router and switch operating systems, hardware, or configurations. This authority is only justified if a direct threat or attack has been discovered and prompt action is required to reduce the risk and/or loss.
- (b). The OCIO-ITS ISSPM has the implied authority and responsibility to direct and authorize action(s) to protect OCIO-ITS information assets from loss without CCB approval in an emergency only.
- (c). If this authority is exercised, the administrator shall report it as an incident and follow Chapter 10: Incident Identification, Declaration, Reporting, and Handling Security Policy or its replacement.

(9). Incident Reporting and Response

In the event that a security vulnerability or breach, malicious activity, successful attack, or violation of this policy has been discovered or suspected, an incident shall be reported in accordance with Chapter 10: Incident Identification, Declaration, Reporting, and Handling Security Policy or its replacement.

22. CHAPTER TWENTY-TWO: SECURITY ARCHITECTURE FRAMEWORK MANAGEMENT SECURITY POLICY

a. General Policy Statement

This policy establishes requirements for the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) to evaluate their Information System Security (ISS) architecture framework to ensure adequate protection of all OCIO-ITS information resources. The OCIO-ITS will conduct an initial review to develop a security model of their information systems assets. The review will include a systematic approach of identifying and allocating all information systems assets to a security architecture baseline. The baseline will include assigning assets with their functional responsibilities (end user systems, relay systems, etc), identifying how these assets are used to meet OCIO-ITS business needs and requirements, in the form of security domains (Internal, External, Public Access, Remote Access), and finally identifying the general security control requirements for each asset.

b. Policy Detail

- (a). The OCIO-ITS will develop a Security Architecture Framework (SAF) baseline and security model within their respective IT structure in alignment with Cyber Security's Guidance Regarding Developing a Security Architecture Framework, CS-035, or its replacement, for additional information and guidelines. The steps in this process include:
 1. Identifying/storing information pertaining to local IT assets: The SAF process shall be used by the OCIO-ITS to identify how each IT asset contributes to the security architecture framework.
 2. Identifying how assets link to a generic security model: The Service Center Agencies supported by the OCIO-ITS shall determine how their assets link to a Basic Element category and assign it to a generic security model.
 3. Identifying security domains: After identifying the assets and assigning them to their basic elements within the security model, the OCIO-ITS must develop security domains. A security domain consists of a set of users, the data for a system, and a security policy that governs the use of the domain.
 4. Identifying security control requirements: Once OCIO-ITS assets have been categorized into basic elements in the security model and security domains have been created, security controls will be assigned based upon the level of security required for each domain level and element.
 5. Identifying security products to support security controls and security domains: Only those products approved by the USDA OCIO in the Security Product Database will be used for meeting security requirements unless otherwise agreed upon with the OCIO-ITS.
 6. Periodic Review of Security Architecture Framework: The OCIO-ITS will periodically evaluate their ISS architecture to ensure that changes are made accordingly to the SAF baseline to reflect changes in business and systems requirements.
 7. Process Scope: This process can be used by the OCIO-ITS for small and large IT architectures. The key is capturing all IT assets within the OCIO-ITS architecture.
- (2). Submission and review of the SAF shall follow the guidance in Cyber Security's Guidance Regarding Developing a Security Architecture Framework, CS-035, or its replacement.

23. CHAPTER TWENTY-THREE: SECURITY AWARENESS, TRAINING, and EDUCATION SECURITY POLICY

a. General Policy Statement

- (1). This policy establishes requirements for the Security Awareness, Training, and Education program for information resources supporting the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS).
- (2). Federal requirements justifying the OCIO-ITS Security Awareness, Training, and Education program are as follows:
 - (a). OPM Regulation 5 CFR 930, Employees Responsible for the Management of Use of Federal Computer Systems.
 - (b). National Institute of Standards and Technology (NIST) Special Publication 800-16, OCIO-ITS Security Training Requirements: A Role-and Performance-Based Model, dated April 1998.
 - (c). Executive Order 13103, Computer Software Piracy, dated September 30, 1998.
 - (d). NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998.
 - (e). Office of Management and Budget (OMB) Circular No. A-130, Appendix III, dated February 8, 1996, Security of Federal Automated Information Resources.
 - (f). Computer Security Act of 1987.
 - (g). Presidential Decision Directive 63 (PDD63), May 22, 1998.
 - (h). OPM Regulation Title 5, Volume2, Parts 930.301-305

b. Policy Detail

- (1). The OCIO-ITS will develop, organize, implement, and maintain an IT systems security awareness training program to ensure the security of OCIO-ITS information resources and to establish requirements for formal training to be conducted at least annually.
- (2). NIST Special Publication 800-16 is the source for guidance and direction in the design of the computer security awareness training program in the OCIO-ITS.
- (3). All OCIO-ITS employees, contractors, subcontractors, grantees and co-operators involved in the management, use, design, development, maintenance or operation of an application or automated information system shall be made aware of their security responsibilities based on their need-to-know and trained to fulfill them.
- (4). Training content shall assure that all groups specified above are versed in the rules and requirements pertaining to security of the respective Federal IT systems, which they access, operate, or manage.
- (5). Computer security awareness refresher training is required at least annually or whenever there is a significant change in IT direction, major system modifications, changes/upgrades in software utilized, or change of duties for continued access to OCIO-ITS information systems.
- (6). The OCIO-ITS will retain records documenting initial or annual computer security awareness training.
- (7). Training must include software piracy prevention and appropriate software use training in compliance with Executive Order 13103, "Computer Software Piracy."
- (8). The OCIO-ITS will distribute security alerts and advisories, as needed, through appropriate media to remind all groups of security practices or to inform them of new security issues.
- (9). New OCIO-ITS and Service Center Agency (SCA) employees and Government contractors shall receive Security Awareness Training within 30 days of being hired.

24. CHAPTER TWENTY-FOUR: SECURITY PLAN MANAGEMENT SECURITY POLICY

a. General Policy Statement

(1). Federal Requirements

The Computer Security Act of 1987 and OMB A-130, Appendix III, requires security plans for all USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) information technology systems. Each plan shall reflect accurate and comprehensive details required by NIST 800-18, Guide for Developing Security Plans for IT Systems. The generic term “systems” covers all General Support Systems (GSS) and Major Applications (MA).

(2). Security Plans

- (a). The OCIO-ITS shall develop and maintain individual security plans for all general support systems and major applications, and an Overall Program Security Plan. These three types of plans shall be prepared using the instructions and templates as defined in the following:
 1. Security Plan Development, section b., (1).
 2. General Support System (GSS) Security Plan Templates for Hardcopy Submission (refer to CS-021, 2003 Annual Security Plans for Information Technology Systems or its replacement for template)
 3. Major Application (MA) Security Plan Templates for Hardcopy Submission (refer to CS-021, 2003 Annual Security Plans for Information Technology Systems or its replacement for template)
 4. General Support System (GSS) Security Plan Templates for Electronic Submission (refer to CS-021, 2003 Annual Security Plans for Information Technology Systems or its replacement for template)
 5. Major Application (MA) Security Plan Templates for Electronic Submission (refer to CS-021, 2003 Annual Security Plans for Information Technology Systems or its replacement for template)
 6. Modification of these templates closely parallels NIST 800-18 but also contains information required by Federal Information Security Management Act (FISMA), and the Office of Inspector General audits.
- (b). The OCIO-ITS and Agency Information Systems Security Program Managers (ISSPMs) shall work with their respective system owners and developers to prepare and update security plans for all general support systems and/or major applications on a periodic basis or when a GSS or MA is implemented or significantly changed.
- (c). The OCIO-ITS ISSPM shall prepare a security plan for the Overall Security Program as outlined in Security Plan Development (Section b), and the Overall Program Security Plan Template.
- (d). The OCIO-ITS ISSPMs will submit all completed annual security plans to the OCIO-ITS CIO's office and shall submit a cover letter with all plans attesting to the completeness and accuracy of these security plans.
- (e). All OCIO-ITS shall submit security plans will be updated every three years or upon a major change.

b. Policy Detail

(1). Security Plan Development

Chapter Twenty-Four: Security Plan Management Security Policy

- (a). Security plans shall reflect input from individuals with responsibilities concerning the system and/or application including functional end users, system owners, the system administrator, and the system security manager.
- (b). For those contractors and/or partners operating an OCIO-ITS sponsored information system, the respective ISSPM will ensure that the necessary contract language is included in procurement requests to specify compliance with the security plan in the development, maintenance, and operation of all information systems and/or applications.
- (c). Any security plan developed by a contractor or outside entity shall always be reviewed by the sponsoring ISSPM and the application or system owners.

(2). Determining General Support Systems and Major Applications

- (a). All applications and systems shall be covered by system security plans if they are categorized as a major application or general support system. All other applications shall be accounted for in the Service Center Agencies' Overall Security Plan.
- (b). Applications that are categorized as non-major will require a statement regarding security and require software certification before inclusion in the enterprise system.
- (c). A system is identified by constructing logical boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a security plan. Each element of the system shall:
 - 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
 - 4. Reside in the same general operating environment
 - 5. A group of portable PCs provided to employees who require mobile computing capability for their jobs
 - 6. A system with multiple identical configurations that are installed in locations with the same IT environmental and physical safeguards.
- (d). All components of a system need not be physically connected, for example:
 - 1. A group of stand alone personal computers (PCs) in an office
 - 2. A group of PCs placed in an employees' homes under defined telecommunications program rules

25. CHAPTER TWENTY-FIVE: SERVER MANAGEMENT SECURITY POLICY

a. General Policy Statement

This policy establishes requirements for authorization and access to USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) server resources through the use of individual credentials. Group credentials are not permitted for access to any server. For the purpose of this policy, system level resources such as Domain Name Server (DNS) or Dynamic Host Configuration Protocol (DHCP) do not apply. The intent is to eliminate anonymous access to resources and establish a foundation for auditing. Additionally, OCIO-ITS servers containing sensitive information shall meet USDA C2-like Level of Trust.

b. Policy Detail

(1). Server Configuration

- (a). Configuration standards and management procedures shall be used to control usability, efficiency, and security of the overall server environment and shall be kept in a Trusted Facility Manual (TFM). These standards and other procedures shall be strictly followed when designing, implementing or managing server configurations. Written approval from the Change Control Board (CCB) is required prior to any deviation from these standards.
- (b). All security-related service packs, patches, and hot-fixes shall be tested and applied to all servers in a timely manner in accordance with Chapter 16: Patch Management Security Policy or its replacement.
- (c). All servers shall comply with the encryption of sensitive data in accordance with Chapter 11: Information Classification Security Policy or its replacement.
- (d). All servers shall be physically secured in accordance with Chapter 17: Physical Access Security Policy or its replacement.
- (e). All servers shall be protected by antivirus software in accordance with Chapter 27: Virus Protection Security Policy or its replacement.
- (f). All servers will display a warning banner in accordance with Chapter 14: Network Access Security Policy or its replacement.
- (g). All servers shall be backed up in a manner that allows for a complete server recovery, including operating system, applications, data and system state, on a daily basis. Archives of server backups shall be kept for a period of at least six weeks.
- (h). All back-up media shall be kept in a secured manner consistent with Chapter 17: Physical Access Security Policy, or its replacement, and be protected by controlled access.
- (i). A selected portion of backup media shall be kept in an alternate physical location secured in a manner consistent with Chapter 17: Physical Access Security Policy, or its replacement, and be protected by controlled access.
- (j). System owners shall be responsible for the documentation, validity, and availability of information regarding their full operations outside of the backup archive.

(2). Server Specification Settings

- (a). Maximum password age shall be no more than 90 days.
- (b). Maximum password length shall be set to 14 and the minimum length shall be set to 9.
- (c). Lock out duration is set to 0 (zero) to enable lockout forever, or until unlocked by an authorized administrator.
- (d). Lock out procedures shall be initiated after three failed attempts to login.
- (e). Password complexity shall be implemented on all servers.

Chapter Twenty-Five: Server Management Security Policy

- (f). Null login credentials shall be disabled on all servers.
- (g). All server configurations shall be set to prevent administrators from performing the following actions:
 - 1. Debugging programs
 - 2. Using logon as a service

(3). Server Management Access

- (a). Access to server consoles and operating systems shall be limited to system administrator personnel only. For security purposes, no exceptions to this rule shall be allowed. All server administrator accounts shall comply with the password requirements set by Chapter 3: Authorization and Access Control Security Policy or its replacement.
- (b). All non-essential user, group, and service accounts must be removed immediately.
- (c). All non-essential services must be removed immediately.
- (d). The administrator account is the original administrative account of the server and/or domain. This account shall be renamed and used on a limited basis. Only select system administrator personnel are to have knowledge of this account's credentials.
- (e). Administrators are not permitted to have access to more than one administrator account.
- (f). Administrators are not permitted to share their account information with anyone, including the help desk and management.
- (g). Any service account used by a service to access system resources is not to be used for any other purpose. Only system administrator personnel are permitted to have knowledge of service account credentials.
- (h). All system administrators shall receive the appropriate level of training to perform their duties in a competent manner.

(4). Server Classification

- (a). Each server hosting a mission critical application or service in a production environment shall be identified as a production server. All production servers must be logically separated and isolated from test and development environments.
- (b). Each server shall be clearly identified as to the classification of information stored or used by the server. These classifications shall follow information classification processes in accordance with Chapter 11: Information Classification Security Policy or its replacement.
- (c). Servers shall be managed and administered in accordance to their identified type and classification.

(5). Server Information Access

Access to server information is restricted to a system administrator and Information Systems Security Program Managers (ISSPM) or persons with written permission from the ISSPM. In the event that server access is created for security audit purposes, it shall be with read-only privileges.

(6). Server Logs

- (a). All servers shall maintain security audit logs that include (at a minimum) the UserID, date, time, and action performed.
- (b). All servers shall log security auditing events showing successful and unsuccessful events, including inappropriate access events.
- (c). All log files and events shall be managed in a manner that maintains their integrity and authenticity, and will be stored or archived for a minimum of six (6) months.

Chapter Twenty-Five: Server Management Security Policy

- (d). Request for access to server logs shall comply with the server information statement in this document.
- (e). Access to security auditing logs shall be limited to system administrators and ISSPM personnel.
- (f). Event logs should be reviewed by system administrators on a daily basis and reviewed randomly or on an as-needed basis by ISSPM personnel.

(7). Server Implementation

All new servers shall meet defined standards and configuration requirements as outlined in the appropriate configuration management document. A request for implementation of new or revised configuration servers shall be submitted to the CCB. Only after obtaining CCB approval shall system administrators proceed with the server implementation. Any changes from the original design plan approved by CCB shall need to be resubmitted via a Request for Change (RFC). Servers being added to the environment shall require additional approval by the CCB.

(8). Server Change Requests

Change requests for any changes to the enterprise server system components, configuration or active directory design shall be submitted in writing via an RFC to the CCB for review. All change requests shall include the reason and timeframe for the request as well as all risks, threats, and known issues associated with this change. Only after CCB approval shall system administrators proceed with the server changes.

(9). Server Services

Servers shall only host services for which they were designed and approved to host. Any additional services must be approved by the CCB. For the purpose of this policy, the term 'services' refers to specific services that a server was designed to host such as a web site, file and print, DNS, DHCP, Telnet, or FTP. All services not required for system functionality are to be disabled.

(10). Implied Authority

- (a). All system administrators have the implied authority and responsibility to take action(s) to protect OCIO-ITS information assets from loss without CCB approval in an emergency to include modifying or changing server operating systems, hardware, configurations, or accounts. This authority is only justified if a direct threat or attack has been discovered and prompt action is required to reduce the risk and/or loss.
- (b). The OCIO-ITS ISSPM has the implied authority and responsibility to direct and authorize action(s) to protect OCIO-ITS information assets from loss without CCB approval in an emergency only. This authority is only justified if a direct threat or attack has been discovered and prompt action is required to reduce the risk and/or loss.
- (c). If this authority is exercised, the administrator shall report it as an incident and follow Chapter 10: Incident Identification, Declaration, Reporting, and Handling Security Policy or its replacement.

(11). Incident Reporting and Response

In the event of a security vulnerability or breach, malicious activity, successful attack, or violation of this policy has been discovered or suspected, an incident shall be reported in accordance with Chapter 10: Incident Identification, Declaration, Reporting, and Handling Security Policy or its replacement.

26. CHAPTER TWENTY-SIX: SYSTEMS DEVELOPMENT LIFE CYCLE SECURITY POLICY

a. General Policy Statement

- (a). This policy establishes requirements for the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) to successfully implement security protocols and procedures into the Systems Development Life Cycle (SDLC) to ensure that a system is developed in accordance with the stated requirements, works effectively, is cost effective, is secure, and is maintainable. The inclusion of security controls and measures early in the SDLC will result in less expensive and more effective security than adding it after a system is operational.
- (b). The OCIO-ITS will implement baseline security controls during the developmental life cycle of all IT systems. The security controls selected for each baseline must be implemented at the recommended level of robustness in order to achieve the estimated threat coverage. In cases where security baselines do not provide sufficient coverage against certain types of threats, additional security controls must be provided upon discovery. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, provides additional information on appropriate security controls for each type of baseline.
- (c). OCIO-ITS information systems security controls shall be integrated into the SDLC from system inception. System owners will identify and contact the Information Systems Security Program Manager (ISSPM) when the system is in the Initiation Phase of the SDLC.
- (d). Legacy systems which do not have an existing SDLC plan, or equivalent, shall develop an SDLC Plan relative to the current phase of the system if it is not fully operational or identified for additional security controls. Corresponding documentation shall clearly reference its equivalence to SDLC information.
- (e). OCIO-ITS system security requirements documentation as identified in the SDLC shall be placed under configuration management control from the inception of the system and will be included as part of the total set of system documentation that evolves over the lifecycle.
- (f). All SDLC plans and SDLC related documents shall be kept current.

b. Policy Detail

The SDLC is separated into five phases during which information system products are developed. These phases include the Initiation Phase, the Development/Acquisition Phase, the Implementation Phase, the Operations/Maintenance Phase, and the Disposition Phase.

(1). Initiation Phase

This is the first phase in the SDLC. The following shall be included in this phase:

- (a). Preparation of the Interconnectivity Security Agreement (ISA)
The OCIO-ITS shall initiate an ISA during this phase of the SDLC. An ISA is part of the overall Certification and Accreditation process and must be completed for each new system that will be connected to an existing legacy system, unless those systems are under the same management.
- (b). Preliminary Risk Assessment
The OCIO-ITS shall conduct an assessment in examination of the basic security needs of the proposed system. A preliminary risk assessment shall define the threat environment in which the system will operate. This assessment should (1) result in a brief initial description of the basic security needs of the system, (2) define the threat environment in which the product or system will operate, and (3) define a potential set

Chapter Twenty-Six: Systems Development Life Cycle Security Policy

of countermeasures. This risk-based approach to information security is defined in NIST SP 800-30, Risk Management Guide for Information Technology Systems.

- (c). Security Categorization
The OCIO-ITS shall define and establish a level (i.e., low, moderate, or high) of potential impact(s) to prevent a potential breach of security. FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, shall be used in conjunction with available vulnerability and threat information in assessing all potential risk to an organization through operation of the proposed information system.
- (d). Privacy Impact Assessment
The OCIO-ITS is required to initiate a Privacy Impact Assessment (PIA) in this phase as part of the ongoing security effort. Refer to Chapter 19: Privacy Impact Assessment Security Policy, or its replacement, for additional information on this subject.

(2). Development Phase

This is the second phase in the SDLC. The following shall be included in this phase:

- (a). Risk Assessment
The OCIO-ITS is required to perform a Security Risk Assessment during this phase to identify protection requirements for the system through a formal risk assessment process. The selection of appropriate types of safeguards or countermeasures must take into consideration the results of the security assurance requirements analysis as defined in the previous phase.
- (b). Security Functional Requirements Analysis
The OCIO-ITS is required to perform an analysis of requirements that include the following components: (1) system security environment, and (2) security functional requirements. This process shall include an analysis of laws and regulations such as the Privacy Act, FISMA, OMB circulars, Agency enabling acts, NIST Special Publications and FIPS, and other legislation and federal regulations, which define baseline security requirements.
- (c). Security Assurance Requirements Analysis
The OCIO-ITS is required to conduct an analysis of requirements that address the developmental activities required and assurance evidence needed to produce the desired level of confidence that the information security will work correctly and effectively. A balance must exist between the benefits to mission performance from system security and the risks associated with operation of the system without security.
- (d). Cost Considerations and Reporting
The OCIO-ITS is required to determine what percentage of the development cost can be attributed to information security over the life cycle of the system. Security controls should be included at the beginning of the SDLC as it is the most cost effective approach for two reasons: (1) it is usually more difficult to add functionality into a system after it has been built; and (2) it is frequently less expensive to include the preventive measures to deal with the cost of a security incident.
- (e). Security Planning
The OCIO-ITS is required to ensure that agreed upon security controls, planned or in place, are fully documented in a system security plan. Refer to Chapter 24: Security

Chapter Twenty-Six: Systems Development Life Cycle Security Policy

Plan Management Security Policy, or its replacement, for additional information on this subject.

- (f). Security Control Development
Security controls described in the respective security plans shall be designed, developed, and implemented in this phase. Refer to Chapter 24: Security Plan Management Security Policy, or its replacement, for additional information on this subject.
- (g). Developmental Security Test and Evaluation
The OCIO-ITS is required to ensure that security controls developed for a new information system are working properly and are effective as evidence by the developer's test materials and test results.

(3). Implementation Phase

This is the third phase of the SDLC. The following shall be included in this phase:

- (a). Security Control Integration
The OCIO-ITS is required to make certain that security controls are integrated at the operational site where the information system is to be deployed into production. Security control settings and switches will be enabled in accordance with manufacturer instructions and available security implementation guidance such as the Trusted Facility Manual (TFM) for the system.
- (b). Security Certification
The OCIO-ITS is required to ensure that security controls are effectively implemented through established verification techniques and procedures within the system certification process. Refer to Chapter 5: Certification and Accreditation Security Policy, or its replacement, and in accordance with NIST SP 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004.
- (c). Security Accreditation
The OCIO-ITS is required to ensure that the necessary security authorization of an information system to process, store, or transmit information is obtained. OMB Circular A-130 requires the security authorization of an information system to process, store, or transmit information. Refer to Chapter 5: Certification and Accreditation Security Policy, or its replacement, and in accordance with NIST SP 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004.

(4). Operations and Maintenance Phase

This phase is the fourth phase of the SDLC. The following shall be included in this phase:

- (a). Configuration Management and Control
The OCIO-ITS is required to ensure adequate consideration of potential security impacts due to specific changes to an information system or its surrounding environment. Depending upon the extent of change to an operational system, additional Certification and Accreditation (C&A) measures may be required. Significant changes include operating system version and major applications that could impact the current operation.
- (b). Continuous Monitoring

Chapter Twenty-Six: Systems Development Life Cycle Security Policy

The OCIO-ITS is required to make certain that controls continue to be effective in their application through periodic testing and evaluation.

(5). Disposition Phase

Disposition is the final phase in the SDLC. The following shall be included in this phase:

(a). Media Sanitization

The OCIO-ITS is required to make certain that all data is deleted, erased, and/or written over as necessary to protect information system hardware. Refer to Chapter 13: Media Sanitation and Disposal Security Policy, or its replacement, for additional information on this subject.

(b). Hardware and Software Disposition

The OCIO-ITS is required to ensure that all hardware and software is disposed of in accordance with Chapter 13: Media Sanitation and Disposal Security Policy or its replacement.

27. CHAPTER TWENTY-SEVEN: VIRUS PROTECTION SECURITY POLICY

a. General Policy Statement

- (1). This policy establishes the guidelines for the management and protection of software used within the USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS). Instructions for installing and configuring the virus protection software on workstations and laptops shall be made available online at <http://www.sci.usda.gov/cce/guides.html>.
- (2). Virus definitions and updates shall be tested and certified prior to deployment.
- (3). All users are responsible for reporting suspected viruses to designated IT support staff immediately.

b. Policy Detail

(1). Virus Protected Systems

- (a). Virus-checking software must be installed and maintained to include the latest virus signature file applied on all servers, workstations, laptops, and personal electronic devices regardless of operating system, whether connected to the OCIO-ITS networks or not. This includes contractor-owned and/or contractor-operated systems, standalone computers and personal electronic devices, and computers of the OCIO-ITS and business partners connected to networks. Virus-checking software must meet the requirements outlined in this policy and in CCE Trusted Facilities Manuals (TFM) or standards.
- (b). E-mail servers must have an antivirus package installed and running with the latest virus signatures applied. E-mail servers shall have a content filtering package or additional device capable of blocking specified attachments, installed, and be running.

(2). Virus Software Configurations and Scanning Policy

- (a). All non-Government machine-readable produced computer media (for example, floppy diskettes, zip cartridges, CD-ROMs, tapes, etc.) and downloaded files must be scanned for viruses and other malicious software before initial use. This pertains to all OCIO-ITS equipment operated by employees, contractors, and partners.
- (b). Remote access users are required to bring in their Government-issued computer laptops and Portable Electronic Devices (PED) to their designated Service Center Agency work facility (minimum of once each month) so that OCIO-ITS approved virus scans can be run and/or antivirus software updates be installed on this equipment. However, this frequency may change in the event of a virus outbreak.
- (c). When feasible, standardized virus software configurations shall be used on non-enterprise systems.
- (d). Antivirus software shall be configured to scan all files and macros (not just program executables) for viruses. This does not apply to swap files.
- (e). Antivirus software shall be configured for both on-access and scheduled scanning.
- (f). Antivirus software shall be configured so that all inbound and outbound files are scanned along with the boot sector and floppy drive (during shutdown).
- (g). Antivirus software shall be configured to scan e-mail attachments prior to sending or opening.
- (h). Antivirus software shall be configured so that ActiveX and Java components in Web pages and HTML-based e-mail messages are scanned.
- (i). End users shall not have the ability to disable the antivirus software on their computer.

Chapter Twenty-Seven: Virus Protection Security Policy

- (j). All e-mail stored, inbound or outbound, with or without attachments, must be scanned for viruses regardless of the destination address.
- (k). E-mail scanning must include all attachments and macros. Attachments and macros that cannot be scanned must be deleted and replaced with a message detailing the action taken. Outgoing e-mail must be scanned at the network server to which the client is connected. If a virus is detected on outgoing e-mail, the server must run a virus scan immediately on the originating client.
- (l). Antivirus software shall be configured so that all activity of the antivirus software is logged. Ensure the logs are included in the daily backups. Logs must be maintained until no longer needed.
- (m). The date of the virus definitions shall be monitored to ensure the automatic update is functioning properly.
- (n). The directory that contains the “setup.exe” for the antivirus software shall be secured so that end users cannot delete, rename, or write files to this directory, and/or inhibit any file tampering.
- (o). Antivirus software shall be configured to block e-mail that it is unable to scan.
- (p). Antivirus updates shall be loaded at the time system instruction is received.
- (q). Antivirus software shall be configured to automatically pull and apply the latest virus definition updates from a central repository site daily.
- (r). All non-Government-owned laptops shall have an OCIO-ITS approved/current version of antivirus software installed prior to connecting to any OCIO-ITS network or computer source.

28. CHAPTER TWENTY-EIGHT: VULNERABILITY SCAN SECURITY POLICY

a. General Policy Statement

- (1). This policy establishes the guidelines for the protection of USDA Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) information systems. Vulnerability scans are required to be conducted on a monthly basis for all operational networks, systems, and servers, inclusive of routers and switches, that the OCIO-ITS are responsible for managing.
- (2). OCIO-ITS is the configuration authority for all vulnerability scans performed and requires that all scanning configurations established by the Service Center Agencies are required to be uniform in approach.
- (3). Each Information Systems Security Program Manager (ISSPM) is responsible for scanning all regional-based hardware, regardless of who owns the equipment.
 - (a). East Region: Natural Resources Conservation Service, ISSPM
 - (b). Central Region: Farm Service Agency, ISSPM
 - (c). West Region: Rural Development, ISSPM

b. Policy Detail

(1). New Equipment/Equipment Upgrade

- (a). Informational scans may be requested by the ISSPM and Change Control Board (CCB) prior to implementation of new or modified/upgraded equipment into the production environment. Scan results shall be provided to the ISSPM and CCB.
- (b). Scans will be conducted prior to new system installations and when any major modifications/upgrades are implemented on current operational systems regarding their connectivity, application functionality, and general security configurations. Service Center Agencies and staff shall only scan networks or servers for which they are responsible.
- (c). A series of scans shall be performed during the developmental cycle such as baseline server (if new hardware) with full applications loaded, then pre-pilot and pre-production. The systems administrator should contact the closest regional Field Office to coordinate the scanning request. Only pre-pilot and pre-production scans are required for configuration management approval prior to further action.
- (d). New systems and equipment or major modifications to existing systems/equipment must be scanned in their development and/or test environment prior to deployment into a production environment. System representatives must contact the ISSPM and CCB to initiate a scan 10 working days prior to scheduling a special or pre-production scan. The system/equipment will not be deployed until vulnerabilities identified have been adequately addressed or a waiver has been approved. Equipment not scanned prior to production will be removed immediately from the network.

(2). Routine Scans

- (a). The ISSPM shall coordinate all scans performed at the Agency level and provide the OCIO Office of Cyber Security with the names and contact information for a primary and secondary contact person relative to performing scans.
- (b). Scan results from production sources shall be forwarded to the responsible ISSPM and CCB for corrective action depending upon hardware ownership. It is the responsibility of the applicable ISSPM and/or the CCB to ensure that all vulnerabilities are addressed within the appropriate timeframes or when waivers are requested.

Chapter Twenty-Eight: Vulnerability Scan Security Policy

- (c). All scans should be completed no later than the 15th calendar day of each month, unless they are considered a special scan, i.e., following major modifications/upgrades. ISSPMs must notify the Department and all relative Service Center Agencies prior to performing a scan.
- (d). Scan results will be provided to the responsible system owners/administrators so that identified vulnerabilities can be addressed. High and medium risk vulnerabilities require a formal response from the appropriate system representatives.
- (e). Responsible parties will reply back to the respective Agency ISSPM within seven calendar days after receiving the scan results for a medium risk vulnerability, and within one workday for a high-risk vulnerability. An action plan must be included for vulnerabilities not mitigated within the required timeframes. The originating ISSPM must receive the results no later than the 23rd calendar day of each month.
- (f). Computer network staff shall address vulnerabilities in the order of their associated risk as a means to mitigate the most serious vulnerabilities immediately (High →Medium→Low). All vulnerabilities on OCIO-ITS networks, systems, and servers identified as 'high' and 'medium' must be formally addressed in a timely fashion. A reasonable effort shall be made to address and correct vulnerabilities rated "low."
- (g). Scan responses provided to the Agency ISSPM and CCB for all high and medium vulnerabilities should fall into one of five categories:
 - 1. Vulnerability has been corrected.
The response shall indicate what corrective action has been taken and the date of correction. The system owner/administrator must sign the response to certify that these actions have been taken. The ISSPM and CCB must initiate a rescan to ensure that corrective actions mitigated the vulnerability.
 - 2. Vulnerability is a false-positive.
System owners/administrators must explain why they believe an identified vulnerability is a false-positive. Once the system owner/administrator has provided the ISSPM and CCB an explanation and the ISSPM and CCB have concurred, the system representatives will no longer have to address the vulnerability on subsequent monthly reports.
 - 3. Corrective action is planned, but has not been completed.
The response must include an explanation outlining steps planned and the timeframe for expected completion.
 - 4. Vulnerability cannot be mitigated for business reasons.
The responsible system owner/administrator shall provide strong justification for vulnerabilities for which there is not a plan to correct. The ISSPM will request a waiver from the OCIO for vulnerabilities that cannot be mitigated for business reasons.
 - 5. Vulnerability cannot be mitigated for vendor reasons.
The system owner/administrator shall provide information on what is needed from the vendor to correct the vulnerability and the timeframe. If no fix is available or will not be available for one month or longer, then the owner/administrator should work with the ISSPM to find a workable alternative to mitigate the vulnerability.

Appendices

APPENDICES

Appendix A: Acronyms

ACRONYM	DEFINITION
ACL	Access Control List
AD	Active Directory
ADPO	Application Development Program Office
AIM	AOL Instant Messenger
C&A	Certification and Accreditation
C2	Command and Control
CCB	Change Control Board
CCE	Common Computing Environment (enterprise system)
CCTV	Closed Circuit Television
CHAP	Challenge-Handshake Authentication Protocol
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CM	Configuration Management
CO	Certifying Officer
COTR	Contracting Officers Technical Representative
COTS	Commercial-Off-The-Shelf (Software)
CPIC	Capital Planning and Investment Control
CS	Cyber Security (USDA)
CT	Certification Team
DAA	Designated Accrediting Authority
DAM	Deputy Administrators for Management
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIG	Director of Infrastructure Governance
DIO	Director of Infrastructure Operations
DMZ	De-Militarized Zone
DNS	Domain Name Server
DoS	Denial of Service
DRAM	Dynamic Random Access Memory

ACRONYM	DEFINITION
EPROM	Erasable Programmable ROM
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FMFIA	Federal Managers Financial Integrity Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FPS	Federal Protective Service
FSA	Farm Service Agency
FSC	Field Service Center
FTP	File Transfer Protocol
FTPS	Secure File Transfer Protocol
GISRA	Government Information Security Reform Act
GMSP	Group Manager of Security Policy
GOTS	Government-Off-The-Shelf (Software)
GPEA	Government Paperwork Elimination Act
GPRA	Government Performance and Results Act
GSA	General Services Agency
GSS	General Support System
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
I-TIPS	Information Technology Investment Portfolio System
IA	IDS Administrator
IAP	Internet Access Provider
IDS	Intrusion Detection System
IHP	Incident Handling Program
IHT	Incident Handling Team
IMAP	Internet Message Access Protocol
IMAPS	Internet Message Access Protocol, Secure
IO Lab	Interoperability Lab
IRC	Internet Relay Chat
ISA	Interconnectivity Security Agreement
ISP	Internet Service Provider

ACRONYM	DEFINITION
ISS	Information System Security
ISSPM	Information Systems Security Program Manager
IT	Information Technology
ITS	Information Technology Services
ITWG	Information Technology Working Group
LAN	Local Area Network
MA	Major Application
MAC	Media Access Control
Malware	Malicious Software
MP3	MPEG Audio Layer 3
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIACAP	National Information Assurance Certification & Accreditation Process
NIST	National Institute of Standards and Technology
NITC- SNCC	National information Technology Center – Systems Network Control Center
NRCS	Natural Resources Conservation Services
NSA	National Security Agency
NTP	Network Time Protocol
OCIO	Office of the Chief Information Officer
OEP	Occupant Emergency Plan
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PC	Personal Computer
PDA	Personal Digital Assistant
PDD	Presidential Decision Directive
PDSO	Personnel and Document Security Division
PED	Portable Electronic Device
PGP	Pretty Good Privacy
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
PL	Public Law

ACRONYM	DEFINITION
PM	Program Manager
POP3	Post Office Protocol, version 3
POP3S	Post Office Protocol, version 3, Secure
PROM	Programmable ROM
RA	Risk Assessment
RCF	Remote Call Forwarding
RD	Rural Development
RIP	Routing Information Protocol
RFC	Request for Change
RLOGIN	Remote Login
ROM	Read Only Memory
RPC	Remote Procedure Call
RS	Relay System
S/MIME	Secure/Multipurpose Internet Mail Extension
SAF	Security Architecture Framework
SBU	Sensitive But Unclassified
SCA	Service Center Agency
SCIF	Secure Compartmented Information Facility
SCMI	Service Center Modernization Initiative
SDLC	Systems Development Life Cycle
SF	Standard Form
SIDO	Security Incident Duty Officer
SM	Strategic Manager
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOW	Statement of Work
SP	Security Plan
SSP	System Security Plan
SRAM	Static Random Access Memory
SSH	Secure Shell
SSI	Sensitive Security Information
SSID	Service Set ID

ACRONYM	DEFINITION
SSL	Secure Socket Layer
TACAS	Terminal Access Controller Access System
TCP	Transmission Control Protocol
TFM	Trusted Facilities Manual
TFTP	Trivial File Transfer Protocol
TS	Transfer System
UDP	User Datagram Protocol
UPS	Uninterrupted Power Supply
US-CERT	United States - Computer Emergency Response Team
USDA	United States Department of Agriculture
UUCP	Unix-to-Unix Copy Program
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
VPN	Virtual Private Network

Appendix B: Definitions

TERM	DEFINITION
Access	The ability to log on to an information resource through the use of an identifier, such as a UserID, to associate a person/user with a set of access authorizations and privileges on a particular information system (i.e., an account). Generally, an individual must have an account and/or a password in order to use a system.
Access Control	The security service that ensures LAN resources are being utilized in an authorized manner.
Accreditation	The formal declaration by the Designated Accrediting Authority (DAA) that the system is approved to operate using a prescribed set of safeguards and should be strongly based on the risks identified during certification.
Active Directory	The directory service for Microsoft Windows 2000 Domain Controllers.
Adequate Security	Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, information. This includes assuring that systems and applications used by the Agency operate effectively and provides appropriate confidentiality, integrity, and availability, using cost-effective management, personnel, operational, and technical controls.
Alphanumeric	A contraction of the words alphabetic and numeric, which indicates a combination of any letters, numbers, and special characters.
Alternative Worksite	A place away from the traditional worksite that has been approved for the performance of officially assigned duties. It may be an employee's home, a Telework Center, or other approved worksite.
Application	A program or system that permits a user to process certain types of data.
Application Development Program Office (ADPO)	Centralized office within the Application Development division of OCIO-ITS which is established for each IT project and its associated SDLC processing. The mission of the Program Office is to ensure that the appropriate administrative, physical, and technical safeguards are incorporated into all applications, whether new or modified existing programs. Additionally, it is responsible for generating a strategic plan for each application or system.
Asset	Information system resources that support an OCIO-ITS organizational mission. This includes, but is not limited to, property, software, data, public image, and intellectual property.
Audit Trail	An audit trail is a series of records of computer events, about an operating system, application or user activities. An information resource may have several audit trails, each devoted to a particular type of activity.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

TERM	DEFINITION
Authenticity	The property of being genuine and able to be verified and be trusted; assurance of the validity of a transmission, message, or originator within an information system.
Authorization	The act of empowering and individual with the ability to perform a specific action with regards to an information system. This action or actions may include the ability to access and/or modify system software, hardware, networks, etc.
Automated Information System	An AIS is any assembly of electronic equipment, hardware, software, and firmware configured to collect, create, communicate, disseminate, process, store, and control data or information.
Availability	That aspect of security that deals with the timely delivery of information and services to the user.
Basic Input/Output System (BIOS)	A set of instructions stored in Erasable Programmable Read-Only Memory (EPROM) chip on the computer system.
Biometric Authentication	This method of authentication using fingerprint scan, voice recognition, retina scan, or signature recognition. This may be used as an alternative to dynamic passwords or smart cards only if it can be proved to provide a level of reliability.
Boot	To start the computer by loading the computer's operating system into the computer's main memory.
Breach	Any illegal penetration or unauthorized access to an information resource.
Capital Planning and Investment Control (CPIC)	A systematic approach to selecting, managing, and evaluating information technology investments.
Certification	The comprehensive assessment of technical and non-technical security features and other safeguards associated with the use and environment of a system to establish whether the system meets a set of specified security requirements.
Certification and Accreditation (C&A)	A formal evaluation and approval process with regard to technical and non-technical security controls of an Information Technology (IT) system that establishes the extent to which a particular design and implementation meets a set of specified security requirements based on an assessment of management, operational, and technical controls within the IT system.
Certifying Officer (CO)	The Certifying Officer assumes the role of an independent technical liaison for all stakeholders involved in the Certification and Accreditation process and is an objective third party, independent of the system developers. The Certifying Officer provides a comprehensive evaluation of the system, including technical and non-technical controls, to determine if the system is configured with the proper security controls in place.

TERM	DEFINITION
Clear Text	Unencrypted information or data.
Commercial-Off-The-Shelf (COTS)	Software acquired by Government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular Government project.
Common Computing Environment (CCE)	The Common Computing Environment was established as an enterprise system to provide a single, common computing environment for the Farm Service Agency (FSA), Natural Resources Conservation Service (NRCS), and Rural Development (RD) agencies of USDA.
Compromise	The unauthorized disclosure, modification, substitution, or use of sensitive information (includes plaintext cryptographic keys and other critical security components).
Computer Room	The physical space that houses any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information.
Computer Security Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, standard security practices, or an exploited system weakness or vulnerability.
Computer Virus Definition Files	Files provided by manufacturers of computer virus detection software to identify all known current viruses. As new computer viruses are identified, virus definition files are updated and released by vendors to eliminate, prevent, or destroy computer viruses.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Management	A family of security controls on the management class dealing with the control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the lifecycle of an information system.
Configuration Management Plan	A plan that describes the management controls involved in all changes and updates made to a system that affects security. The plan includes all documentation supporting these changes and updates. This plan is maintained throughout the Certification and Accreditation process and updated according to system development lifecycle (SDLC) activities.
Contingency Plan	An action plan for ensuring Information Technology processing continuity despite catastrophic events. Contingency Plans cover three types of actions: 1) Emergency procedures for initially responding to disruptions at primary locations; 2) Backup procedures for conducting operations at alternate locations, when necessary; 3) Recovery procedures for restoring normal operations back at the primary IT facility.
Contractors	Non-Government employee under contract and who use OCIO-ITS information systems or computer resources.

TERM	DEFINITION
Countermeasure	Any action, device, procedure, technique or measure that reduces a system's vulnerability to a threat.
Cracker	An intruder who breaks into an information resource or network using a variety of unauthorized access methods, exploiting resources either maliciously or for personal gain.
Credentials	Identification consists of a unique UserID and password for each user.
Critical Information	Critical information is that information which is used to support customer service functions and other ongoing business requirements.
Cryptography	The science and practice that embodies principles, means and methods for the transformation of information to hide its content, prevent its undetected modification, and prevent its unauthorized use.
Damage	The unauthorized accidental or deliberate modification, destruction or removal of information or data from an information resource.
Data Encryption Standard (DES)	A DES key consist of 64 binary digits of which 567 are randomly generated and used directly by the algorithm per FIPS Publication 46-3
Data Integrity	The state that exists when computerized data or information is the same as that in the source documents or code and has not been exposed to accidental or malicious alteration or destruction.
Data Key	A cryptographic key, which is used to transform data (i.e., encrypt, decrypt, authenticate).
Decryption	The process of transforming encrypted data into plain or readable information.
Decryption Software	Decryption takes encrypted information and makes it comprehensible again.
De-Militarized Zone (DMZ)	A De-Militarized Zone is logically and physically restricted space that may contain sensitive equipment such as firewalls, Intrusion Detection Systems (IDS), or network nodes.
Denial of Service (DoS)	The intentional degradation or blocking of computer or network resources. Action(s) which prevent any part of a computer system or network from functioning in accordance with its intended purpose.
Designated Accrediting Authority (DAA)	The DAA determines accreditation based on security risks of the system, business case, and budget.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines.
Disaster Recovery Plan	A plan that identifies recovery procedures in the event of natural or man-made disasters or catastrophes affecting the availability of the system. This plan is tested annually to ensure the continued effectiveness and adequacy of the plan.
Encryption	The process of transforming readable information into cipher text through a sophisticated mathematical conversion process.

TERM	DEFINITION
Encryption Software	A computer program that allows data to be encrypted during transmission (useful for transmitting data across unsecured communications links) or in storage of the data (i.e., saving to a PDA, computer hard disk, floppy disk, or CD).
Encryption Standards	There are a wide variety of different encryption products available. The National Institute of Standards and Technology maintains a list of cryptographic modules that have been validated against Federal Information Processing Standard (FIPS) 140-2.
Exposure	The process of transforming encrypted data into plain or readable information.
Facility	This term includes, but is not limited to, personal and mainframe computers (networked or stand-alone), software; systems, networks, network ports for access, email servers, intranet web servers, and gateways used to access external networks such as the Internet and World Wide Web.
Firewall	A combination of hardware and software that controls network traffic using stateful inspection of all traffic and monitors and controls sessions between internal and external users and internal networks, computers, and resources.
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line.
Freedom of Information Act (FOIA)	The Freedom of Information Act, enacted in 1966, provides that any person has a right, enforceable in court, of access to Federal Agency records, except to the extent that such records are protected from disclosure by one of nine exemptions or by one of three special law enforcement record exclusions.
General Support Systems (GSS)	Interconnected information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.
Hacker	An individual who attempts to unauthorized access information systems and network resources primarily to create havoc, produce disruptions, and/or bring the system down altogether.
Harm	To damage, injure, or impair information systems using electronic methods.
High-risk	Potential for exceptionally serious impact on an Agency or program mission or the overall efficiency of the service.
Identification	The use of an identifier, such as a UserID, to allow an information system to associate a person/user with a set of access authorizations and privileges on a particular information system.

TERM	DEFINITION
Individual Accountability	Requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.
Impact Analysis	Analysis is performed during the initial life cycle phases to determine the overall effect of proposed changes on existing security controls.
Incident	Any adverse event, real or suspected, involving the security of OCIO-ITS information resources is to be considered a security incident. Any violation of law, regulation or security policy, real or suspected, is to be considered a security incident.
Incident Handling and Response	Policies, procedures and practices used to report, contain, investigate and preserve evidence and respond to security incidents. Used synonymously with incident response.
Information Resources	Any OCIO-ITS Information Technology Resource consisting of personnel, equipment, funds, and information technology.
Information Security	The protection of data and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Sensitivity	The formal process of identifying each system in terms of its confidentiality, integrity, and availability.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information Systems Security Program Manager (ISSPM)	The primary role of the ISSPM is to provide security engineering and security architecture support to the OCIO-ITS. This is performed in formal establishment of realizable security solutions that is consistently applied within OCIO-ITS in compliance with the application development community.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
Information Technology Restricted Space	An area of special-use space in OCIO-ITS locations that houses web farms, computer or telecommunications equipment/devices and the general space surrounding those areas.
Office of the Chief Information Officer (OCIO), Information Technology Services (ITS)	USDA IT component that specializes in providing information technology support to the Service Center Agencies including Large Offices, Field Offices, and their partners.
Integrity	Guarding against improper information modification or destruction, and

TERM	DEFINITION
	includes ensuring information non-repudiation and authenticity.
Internet	A set of networks and machines that use the TCP/IP protocol suite connected through gateways, and share a common name and address spaces.
Interoperability Lab (IO LAB)	The Lab's primary focus is the testing and approval/disapproval of legacy and COTS software and hardware products on the CCE platform. Other functions are system and security configuration management of PC and server rollouts, software repackaging, SNA gateway configuration, and virus protection administration throughout the CCE Enterprise Domain.
Intruder	An intruder is a person who is the perpetrator of a security incident.
Intrusion	Intrusion is an unauthorized, inappropriate or illegal activity by insiders or outsiders that can be considered a penetration or breach of an IT resource.
Intrusion Detection System (IDS)	Intrusion Detection Systems can include the following four types: 1) Anomaly Detection - this type picks out traffic, protocols, or packets that appear out of the ordinary, 2) Misuse Detection - these identify threats based on signatures and are similar to antivirus programs, 3) Passive Systems - these identify and log security compromises, and 4) Reactive Systems - these block apparent malicious activity.
IT Contingency Planning	Represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. IT contingency planning fits into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning. Ultimately an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and the facility.
IT Investment	An expenditure of money and/or resources for IT and IT-related products or services involving managerial, technical, or organizational risks for which there are expected benefits to the organization's performance.
IT Related Risk	The net mission impact considering 1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and 2) the resulting impact if this should occur.
IT Restricted Space	Computer rooms used for housing Web Farms, DMZ equipment, mission critical systems, systems containing sensitive information and critical infrastructure resources.
IT System	Defining boundaries around a set of processes, communications, storage, and related resources (an architecture) identifies a system.
LAN Room	A room that contains equipment used to support Local Area Networks (LAN). Most LANs connect workstations and personal computers that

TERM	DEFINITION
	span a relatively small area such as a single building or complex.
Level of Consequence	The impact an incident has on an organization. Impact includes: loss of data; the cost to a OCIO-ITS Agency or mission area, negative consequences to the organization (i.e., damage to reputation); and the magnitude of damage that must be corrected.
Levels of Concern	An expression of the criticality/sensitivity of an information system in the areas of confidentiality, integrity, availability, and exposure as expressed qualitatively as high, moderate, or low.
Local Area Network (LAN)	A LAN connects workstations and personal computers that span a relatively small area, such as a single building or complex.
Login Script	A command procedure stored on the laptop with a set of commands for logging into another computer or computer network.
Low Risk	Potential for limited impact on an Agency or program mission or efficiency of the service.
Major Application (MA)	An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.
Medium Access Control (MAC) Address	At the lowest level, computers communicate with each other using this hardware address.
Mission Critical	An operation system and its resource components that are required for an OCIO-ITS site to successfully function
Misuse	Unauthorized use of any OCIO-ITS Asset by any individual.
Moderate-Risk	Potential for moderate to serious impact on an OCIO-ITS or program mission or efficiency of the service.
National Institute of Standards and Technology (NIST)	A part of the U.S. Department of Commerce, formerly called the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.
National Security Information	Information that has been determined pursuant to Executive Order 12958 or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
National Security Position	Those positions involving activities of the Government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities

TERM	DEFINITION
	concerned with the preservation of the military strength of the United States; positions that require regular use of, or access to, classified information.
National Security System	Any information system (including any telecommunications system) used or operated by the OCIO-ITS or by a contractor of the OCIO-ITS, or other organization on behalf of the OCIO-ITS - 1) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, excluding a system that is to be used for routine administrative and business applications, for format, payroll, finance, logistics, and personnel management applications; or, 2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Need-to-Know	The necessity for access to, knowledge of, or possession of classified or other sensitive information in order to carry out officially sanctioned duties. Responsibility for determining whether a person's duties require possession or access to this information rests upon the individual having current possession (or ownership) of the information involved, and not on the prospective recipient. This principle is applicable whether the prospective recipient is an individual, a contractor, another Federal Agency or a foreign Government. (Source: USDA DM 3440-1).
Network	A group of computers and associated peripheral devices connected by a communications channel capable of sharing files and other resources among several users.
Network-Based IDS	Network-based systems examine the individual packets flowing through a network. Unlike firewalls, which typically look primarily at IP addresses and ports, network-based intrusion detection systems are able to understand all the different flags and options that can exist with a network packet.
Non-Repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later legitimately deny having processed, stored, or transmitted the information.
Non-Sensitive	Potential for limited damage to the national security (Damage to national security defines National Defense Confidential information).
Occupant Emergency Plan (OEP)	The OEP provides the response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property. Such events would include a fire, hurricane, criminal attack or medical emergency. General Services Administration (GSA) owned facilities maintain plans based on the GSA OEP template.

TERM	DEFINITION
Office of Chief Information Officer (OCIO)	The USDA's OCIO supervises and coordinates the design, acquisition, maintenance, use, and disposition of information and information technology (IT) by the OCIO-ITS.
Office of Inspector General (OIG)	The mission of the Office of Inspector General is to investigate allegations of crime against the department's programs, and to promote the economy and efficiency of its operations, with the object of helping to protect its programs and to ensure integrity.
Operational Controls	Security methods that focus on mechanisms that primarily are implemented and executed by people as opposed to systems.
Password	A unique, secret, string of alphanumeric characters selected by each user that is associated with a particular UserID. The password's primary function is to protect the UserID from unauthorized use. A non-display mode is used when the password is entered to prevent disclosure to others.
Personal Digital Assistant (PDA)	A small mobile hand-held device that provides computing and information storage and retrieval capabilities. PDA devices offer applications such as office productivity, database applications, address books, schedulers, and to-do lists.
Physical Security	Physical security refers to the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes and accidental damage.
Portable Electronic Device (PED)	Any electronic device that is capable of receiving, storing, or transmitting information using any format (i.e., radio, infrared, network or similar connections) without permanent connections to Federal networks.
Primary Worksite	The location where an employee would work absent a Telework arrangement. Also known as a traditional worksite or official duty station.
Privacy Information	Any item, collection, or grouping of information about an individual that is maintained by an Agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.
Public Data	Data which is accessible to all identified and authenticated public users of OCIO-ITS information resources, i.e., customers that use or store information on OCIO-ITS data resources.
Remote Access	The ability to access OCIO-ITS information and systems from a remote location, across an external telecommunications service.
Risk	A combination of: 1) the likelihood that a particular vulnerability in an information system will be either intentionally or unintentionally exploited by a particular threat resulting in a loss of confidentiality,

TERM	DEFINITION
	integrity, or availability; and 2) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability will have on operations (including mission, functions, image, or reputation), assets, or individuals (including privacy) should the exploitation occur.
Risk Assessment	A process that includes defining and valuing the assets, defining the threats to those assets, determining the system's vulnerabilities, and recommending reasonable safeguards to reduce risks to acceptable levels.
Risk Management	The ongoing process of identifying, controlling, and mitigating risks to OCIO-ITS operations (including mission, functions, image, or reputation), assets, or individuals resulting from the operation of an information system or multiple information systems. It includes: risk assessment, cost benefit analysis, and the selection, implementation, testing and evaluation of security controls.
Rules of Behavior	Rules that have been established and implemented concerning the use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of system privileges, and individual accountability.
Safeguards	Synonymous with security controls and countermeasures.
Screen Saver	A screen engaged by an operating system to prevent screen burns or discoloring. Screen savers can be configured to start after a specific period of time and to also be password protected.
Secure Compartmented Information Facility (SCIF)	A facility where Sensitive Compartmented Information (SCI) may be stored, used, discussed, and/or processed is called a Sensitive Compartmented Information Facility or SCIF.
Security Accreditation	The official management decision to authorize operation of an information system. This authorization, given by a senior OCIO-ITS official, is applicable to a particular environment of operation, and explicitly accepts the level of risk to operations (including mission, functions, image, or reputation), assets, or individuals, remaining after the implementation of an agreed upon set of security controls.
Security Analysis	A formal analysis conducted by the Agency Information Systems Security Program Manager in conjunction with the business owner or developer, for the purpose of determining the importance of information, assessing risks, formulating mitigation strategies, and other measures needed to safeguard the IT investment.
Security Audit Logs	The automatic logging of successful and unsuccessful access events including login/logoff, resource access, execution of security commands, and changes to security tables.
Security Certification	A comprehensive evaluation of the management, operational, and

TERM	DEFINITION
	technical security controls in an information system. This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the remaining vulnerabilities in the information system after the implementation of such controls.
Security Controls	The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information.
Security Plan	The Security Plan documents all security-related activities. In the pre-operation phases of the SDLC, the Security Plan needs to list actions to ensure that the system is developed in a reasonably secure environment and that it contains sufficient and appropriate security features. It defines the security requirements and provides the systematic management plans to meet those requirements. During the system's operation phase, the Security Plan becomes the document for responding to new vulnerabilities and threats as well as serving as the primary basis for management reports. It must be updated as least annually, but may be updated more often prior to the system's operational phase.
Security Policy	A document outlining acceptable and unacceptable requirement and practices directed and with the intent to provide IT security.
Sensitive But Unclassified (SBU)	Information that is not as critical as Classified Information, the need to protect this data has been recognized by the administration, law and the Institute of Standards and Technology .
Sensitive Security Information (SSI)	Information for which unauthorized access to, or the loss or misuse of, which would adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-235). Some specific categories of sensitive information are protected by statute, regulation or contract, (i.e., privacy information, proprietary information, export control information, pre-publication academic information).
Sensors/Taps	A class of modules that provide automated detection and response to threats. These modules are installed at strategic locations throughout the enterprise network and include network sensors, server sensors and operating system sensors.
Server	A computer or device on a network that manages and hosts network resources.

TERM	DEFINITION
Service Center Agency (SCA)	These Agencies, which include FSA, NRCS, and RD, are currently operating in partnership to accomplish a USDA modernization initiative that establishes a common information technology infrastructure.
Smart Cards	Handheld smart cards with embedded microprocessor chips containing authentication data and verified by a corresponding card reader (i.e., PCMCIA slot in a notebook computer) may be used for remote user authentication, only if used with a secondary (two factor) authentication mechanism. Acceptable secondary authentication mechanisms include: remembered PIN code or Biometric (i.e., signature verification, fingerprint reader) authentication. PIN codes must not be stored in close proximity to the smart card and must not be marked on the token.
Split Tunneling	Simultaneous direct access to a non-USDA network (such as the Internet or a home network) from a remote device while connected into the OCIO-ITS network via a VPN tunnel.
Sponsoring Organization	The OCIO-ITS organization that requested that the third party have access into the OCIO-ITS network.
Subsystem	A major subdivision or component of an information system consisting of hardware, software, or firmware that performs a specific function.
System	A collection of hardware, software, major application, operating system, and firmware integrated together to perform one or more functions.
System Development	The process for creating and implementing information technology-based system software and hardware inclusive of application code, middleware, operating systems, networks, firewalls, routers, switches, personal computers, servers, mainframe computers, etc., within the OCIO-ITS.
System Development Life Cycle (SDLC)	A contingency planning guide for Information Technology systems. It is the scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. The phases through which software evolves from an idea to implementation include the Initiation Phase, Development Phase, Certification and Accreditation Phase, Implementation Phase, Operation and Maintenance Phase, and the Disposal Phase. These phases may vary depending on the complexity of the system being developed.
System Owner	The primary liaison for a designated information system within the IT community. This person is responsible for all information technology-related activities including security. Additionally, this official represents the interests of the user community throughout the life cycle of the information system.
Security Plan (SP)	A set of requirements that are used to delegate how system security will be managed. This plan includes system identification, management controls, operational controls, and technical controls. The Security Plan outlines responsibilities for all system users and describes the rules of

TERM	DEFINITION
	behavior for those users.
Technical Controls	Hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.
Telework	A customized arrangement that allows an employee to work away from the traditional worksite or official duty station in either 1) his/her home, 2) a Telework center, such as those established by the General Services Administration (GSA) or, 3) a virtual or mobile office setting. The work site is not to be considered a barrier to an employee's ability to perform such obligations as official travel, attending face-to-face meetings and communication with colleagues and customers. Telework addresses the location of the work site as opposed to the work schedule.
Telework Agreement	A written agreement completed and signed by an employee and appropriate official(s), that outlines the terms and conditions of the Telework arrangement.
Telework Participant	An employee who, with the approval of his/her supervisor, works full, part-time at locations, or work sites other than the primary worksite. This does not include employees who only work remotely while in official travel status.
Threat	Any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability.
Triple DES	A key that consist of three DES keys, also referred to as a key bundle.
Trojan Horse	A Trojan horse is a command procedure containing hidden code that, when invoked, performs some unwanted function. A virus can infect a legitimate program and transform it into a Trojan horse.
Trusted Facilities Manual (TFM)	A document listing required security standards and settings, including implemented setting and standards. The TFM cautions about the functions and privileges that should be controlled when running a secure facility and procedures for examining and maintaining audit trails including the audit trail record structure.
Trusted Network Gateway	In networking, a gateway is a combination of hardware and software that links two different types of networks. A secure gateway or firewall blocks or filters access between two networks, often between an internal trusted network and an external un-trusted (public) network such as the Internet.
User	All Federal Employees, Contractors, and volunteers, Permanent or Temporary, which access OCIO-ITS information resources and network resources.
UserID	The authorization code used to identify OCIO-ITS users who are entitled to access OCIO-ITS computer resources.
Validation	The process of evaluating software at the end of the software development process to ensure compliance with software requirements.

TERM	DEFINITION
Verification	The process used by an independent certification agent to confirm or establish by testing, evaluation, examination, investigation or competent evidence.
Virtual Private Network (VPN)	A technology by which authorized individuals (such as remote employees) can gain secure access to an organization's intranet via the Internet. VPN technology provides secure data transmission across public network infrastructures. VPNs employ cryptographic techniques to protect information as it passes from one network to the next or from one location to the next. Data that is inside the VPN tunnel, the encapsulation of one protocol packet inside another, is encrypted and isolated from other network traffic.
Virus	A program that searches out other programs and infects them by embedding a copy of itself within the other programs. When the other programs are executed, the embedded virus is executed, thus spreading the infection.
Vulnerability	A condition or weakness in security procedures, technical, management or physical controls that could be exploited by a threat.
Vulnerability Scan	A test of the network's or system's vulnerability to known exploits and attack methods, by either passive (non-intrusive) or active (intrusive) scanning of network points of access.
Waiver	A formal approval to not comply with a security policy or exemption from a security policy.
Web Farm	A web farm is an integrated collection of firewalls, switches, servers, back-up libraries and other components that are precisely focused to develop and maintain a secure, scalable and redundant web delivery infrastructure.
Wireless Access	Any digital communication protocol or process that does not require a physical connection media. This includes but not limited to all 802.11 a/b/g or infer-red access devices or point-to-point devices.
Wireless Technology	A transport mechanism that supports communication between mobile, portable, or fixed facilities using the electromagnetic spectrum without a physical connection.
Worm	A self-replicating program that is self-contained and does not require a host program. It is designed to propagate through a network rather than just a single computer. A worm exploits flaws in operating systems or inadequate system configurations. Release of a worm usually results in brief, but spectacular, outbreaks that can shut down entire networks.

OCIO-ITS Security Waiver Form

Requests for exceptions to these waiver requirements will include a persuasive and cogent justification. The waiver package will include the following:

1. An explanation of exception requested.
 - Identify which policy and item(s) the exception covers and provide information detailing the exemption requested. Explain why the policy cannot be implemented.
2. Business case necessitating the service.
 - How will the lack of this exemption impact program delivery?
3. Is sensitive (SBU) information involved?
 - Details explaining how the confidentiality, integrity and availability of the sensitive information will be preserved.
 - Since this exemption may increase the vulnerabilities to the system/application, how will the information be safeguarded?
4. Technical details of the proposed alternative approach.
 - Explain the technical solution. Include diagrams that show the current condition and what the proposed alternative approach will look like (before and after). If this is provided electronically, use Visio or a similar type of software.
5. Associated security costs for the Agency requested solution funded by the proposing Agency (Include a copy of any IT Moratorium Waiver Request and associated hardware and software costs not covered in waiver)
 - How much is this going to cost? How does this compare to the cost of implementing the policy?
6. Risk analysis of the proposed alternative approach.
 - Since this exemption may increase the vulnerabilities to the system/application, a risk assessment needs to accompany this request. What are some of the current exploits of these vulnerabilities identified in risk analysis and how are these addressed by the proposed solution?
7. Assurances that any alternatives implemented will not adversely affect the costs, security, maintenance or operations of existing solutions implemented by other Departmental entities.
 - Who else is potentially at risk and are they aware of the risk?
8. A schedule and tasks to be undertaken to become compliant.
 - When do you plan to become compliant with OCIO-ITS policy? Provide an action plan and appropriate milestones. Typically the plan should run no more than a year. Waivers for longer than 12 months will be re-evaluated periodically.

NOTE: Any alternatives implemented will be subject to periodic reviews and must be adjusted, as necessary, to conform to the USDA Enterprise Architecture and Security standards. Waiver packages will be forwarded to the ITS Information Systems Security Program Manager (ISSPM) in accordance with normal procedures. These packages will be forwarded to OCIO Cyber Security for review and further action. Additionally, all waiver packages are subject to review by the OIG and other audit bodies.

Policy Manual Approval Signature Page

OCIO-ITS SECURITY POLICY MANUAL

Version 1.0, Dated November 29, 2004

The OCIO-ITS Security Policy Manual establishes policy for the management and administration of information technologies for the United States Department of Agriculture (USDA) Office of the Chief Information Officer (OCIO), Information Technology Services (ITS) that supports the Farm Service Agency (FSA), Natural Resources Conservation Service (NRCS), and Rural Development (RD) including Large Offices and Service Centers (including State, District, Area, County, and Local Field Service Offices), and their partners.

This policy manual is directed to and applies to all Federal employees, partners, Government contractors, and all others responsible for managing, administering, supporting, or accessing information technology for the OCIO-ITS, which supports the Service Center Agencies (SCA).

In conformance with the IT policy-making process developed by the United States Department of Agriculture Office of the Chief Information Officer (OCIO), Information Technology Services (ITS), we shall forward this guidance to the Service Center Agency Chief Information Officers and Deputy Administrators for Management for their information.

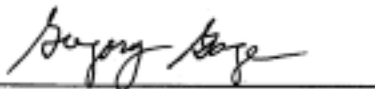
Our signatures below recognize our commitment to incorporate the policy within this document into the official policy of OCIO-ITS. We shall review our existing policy and/or operating procedures related to this policy and revise or develop new guidance accordingly.

Approved by:



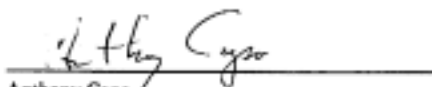
Richard Roberts
Associate CIO, Acting
OCIO-Information Technology Services

1/7/05
Date



Greg Gage
Deputy Associate CIO, Acting
OCIO-Information Technology Services

1/7/05
Date



Anthony Capo
Chief, Acting
Security Policy Branch
OCIO-Information Technology Services

12/2/04
Date

OCIO-ITS Security Policy Manual - FINAL - Version 1.0