CHAPTER 9, PART 2
USDA INFORMATION SYSTEMS SECURITY PROGRAM

1 BACKGROUND

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

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

2 POLICY

All USDA agencies and staff offices will organize, implement and maintain an ISSP that ensures security of all information technology assets. Security must be adequately addressed in all phases of the System Development Life Cycle (SDLC), normally

commencing in the IT System Initiation Phase. Each agency ISSP will include the following responsibilities:

- Categorize sensitivity of information and information systems in accordance with FIPS 199;
- Conduct regular risk assessments for IT systems and computing devices;
- Implement effective risk mitigation strategies;
- Conduct formal Certification and Accreditation (C&A) of all agency IT systems;
- Implement security controls throughout the System Life Cycle;
- Use the Capital Planning and Investment Controls (CPIC) process to formulate and plan security costs for all systems;
- Monitor the system Configuration Management (CM) process of all systems;
- Prepare agency annual Program and System Specific Security Plans;
- Manage an effective Security Awareness and Training Program;
- Manage the agency Security Incident Response Program;
- Conduct annual self-assessment of the ISSP using NIST 800-26 and NIST 800-53;
- Monitor IT systems using audit trails, controls logs and other mechanisms;
- Establish an electronic inventory of all IT systems and computing devices;
- Maintain agency IT inventory in the Enterprise Architecture Repository (EAR);
- Disseminate department policy and procedures to all agency personnel;
- Respond to regular and ad hoc reporting requirements and audits by internal or external agencies; and
- Monitor agency compliance to USDA, OMB, NIST and other governing bodies' policy for security.

Agencies may elect either a traditional ISSP structure with the responsibilities delineated in Responsibilities, Section 4, of this policy or use the alternative structure defined in Procedures, Section 3 below. An alternative structure is useful in agencies of greater than 1,000 IT users (employees, contractors, volunteers, partners, or customers), as it outlines the tactical security

responsibilities below the ISSPM level. The duties of the ISSPM/ISSM can be designated as the agency sees fit, as long as all responsibilities are designated in writing and effectively executed. Associate CIO for Cyber Security (ACIO CS) must be advised that the alternative structure is being implemented and each agency must comply with the duties defined for this structure.

Each Agency Head or CIO will formally designate at least one Information Systems Security Program Manager (ISSPM) using the Designation of ISSPM and Deputy ISSPM form contained in Appendix A to serve in these positions. These forms will be sent to the ACIO CS when individuals are assigned to these positions. The duties and responsibilities of an ISSPM are diverse, comprehensive and complex. This position is one of high sensitivity and level of trust and therefore will be filled only by full time government personnel. In addition, this position has a requirement for high confidentiality due to the critical nature of the investigatory and compliance work. Therefore space should be assigned to the ISSPM and Deputy ISSPM that affords locking files and the ability to conduct meetings of a highly sensitive nature in private. In no case, are ISSPMs and Deputy ISSPMs to be assigned to a work/office area with individuals not associated with information security. To successfully establish, manage and improve an agency/staff office/program area ISSP, the ISSPM shall receive comprehensive annual security training. Agencies/staff offices/program areas shall appoint a Deputy ISSPM and as many Information Systems Security Officers (ISSOs) as necessary to comply with this policy. The agency ISSPM shall be recognized as the organization's CS expert, leader and point of contact. The agency ISSPM, Deputy ISSPM and ISSM/ISSO positions are considered to be High Risk Public Trust positions as defined by 5 CFR 731. Each agency will ensure that the individuals in these positions have the appropriate level of background investigation completed. Additionally, each agency is responsible for determining the National Defense sensitivity level of these positions as defined in 5 CFR 732 and obtaining the appropriate level of security clearance. Individuals in these positions will have a direct reporting relationship with the agency CIO.

Policy Exception Requirements – Agencies/Staff Offices and program areas that cannot comply with this policy will submit all policy exception requests directly to the ACIO CS. Temporary exceptions to policy will be considered only in terms of implementation timeframes and progress toward meeting the standards will be monitored by OCIO CS. Exceptions that are approved will require that each agency report this Granted Policy Exception (GPE) as a Plan of Action & Milestone (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be considered for renewal on an annual basis with an updated timeline for completion. OCIO CS will monitor all approved exceptions.

3 PROCEDURES

Agencies and staff offices electing to adopt a three-tier ISSP management approach will have a structure comprised of:

- Information Systems Security Program Manager (ISSPM): This person and the deputy ISSPM are responsible for managing the ISS efforts for an entire agency or staff office. This person is a program manager responsible for the strategic security requirements of the program to include planning, budget review, consolidation of agency security reports, and coordination of the ISSP into the culture of the entire organization. ISSPMs will act as consultants for ISSM/ISSOs and work with them to resolve highly technical matters, when necessary. Ultimately, the ISSPM is still responsible for efficient operation of the overall ISSP.
- Information Systems Security Manager (ISSM): This individual(s), including deputy(ies), is responsible for managing the tactical efforts of a business, functional, or operational entity within an agency. Their responsibilities include the daily operational security issues of the unit and overall management of the "front line" security requirements for the unit. This individual may often be

called upon to assist in the resolution of certain system security issues.

- Information Systems Security Officer (ISSO): This person(s), including deputy(ies), is responsible for the day-to-day security administration for one or more information systems. Theirs is an operational security effort regarding the system(s) for which they are responsible.

a RESPONSIBILITIES (Alternate)

(1) The Agency Chief Information Officer (CIO) will:

(a) Act as the agency Senior Security Officer (SSO) who is responsible for supporting the strategic requirements of the ISSP;
(b) Ensure that adequate funding, training and resources are provided to the ISSP to support the agency mission;
(c) Facilitate the resolution of high-level security matters within the agency by acting as a champion for the ISSPM;
(d) Ensure that ISSM/ISSOs are designated to provide adequate security to business, functional or operational entities;
(e) Serve as the certification official for agency security requirements (i.e., Annual Security Plans, FISMA and other formal reporting requirements, Waiver Requests and Certification of agency IT Systems);
(f) Formally designate in writing to ACIO CS the ISSPM(s) and Deputy(ies) for each agency; ensure that these individuals are permanent members of all system development, telecommunications planning and System Development Life Cycle planning teams; and
(g) Provide role-based and specialized security-based training to the ISSPM(s) and Deputy ISSPM(s) from USDA enterprise training vehicles.

(2) The Agency Information Systems Security Program

Manager (ISSPM) will:

(a) Manage the agency ISSP including the activities and training from USDA Enterprise training vehicles of the ISSM/ISSOs;

(b) Support the strategic security program requirements to include: planning, budget analysis, department policy review and internal policy formulation, agency FISMA, POA&M, and audit reporting requirements, agency Security Architecture and agency IT CPIC;

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

(d) Monitor the progress of the ISSM/ISSOs to ensure that they meet the necessary program security requirements of NIST 800-26 and departmental policy directives;

(e) Serves as the principle consultant to the agency CIO and senior management, including ACIO CS;

(f) Coordinate agency Incident Response with the agency ISSM/ISSOs to include all associated actions necessary to mitigate the risk to unit systems; and

(g) Oversee the implementation of agency security policies, procedures and guidelines.

(3) The Agency Information Systems Security Manager (ISSM) will:

(a) Serve as the Point of Contact (POC) for all unit CS matters; provide subject matter guidance to agency personnel;

(b) Participate in the process and monitor to ensure that all agency systems are C&A'd prior to actual operation and that they are reaccredited every three years or when significant system change occurs;

(c) Disseminate departmental security policy and procedures; formulate internal agency security procedures and support implementation, testing, and integration into the agency culture (mission and business operation);

(d) Participate as a permanent member of unit system development teams, telecommunications planning, and System Development Life Cycle (SDLC) processes;

(e) Conduct internal audits of all agency IT systems to ensure compliance with federal and departmental policy and procedures;

(f) Participate in general and role-based security training to enhance knowledge and skill level; recommend appropriate training for staff to ISSPM;

(g) Proactively coordinate the establishment of system security controls to protect agency information using authentication techniques, encryption, firewalls, access controls, and comprehensive departmental Incident Response Procedures with all System Administrators (SA) and business owners;

(h) Coordinate with business owners to categorize information systems and determine sensitivity levels;

(i) Establish Disaster Recovery/Business Resumption (DR/BR) and other emergency plans for all IT systems; ensure compliance with backup and storage procedures;

(j) Monitor physical spaces to ensure that the security requirements of IT Restricted Space are followed in maintaining, updating or planning new space, and advise the CIO if space does not meet security requirements;

(k) Develop and manage a Security Awareness Program including arranging or conducting security awareness briefings; recommend to the agency ISSPM security training for all agency personnel, including contractors,

based on their role in the organization; ensure that all personnel are appropriately trained in the security Rules of Behavior prior to being granted access to unit systems;

(l) Arrange for background screening of unit employees based on the level of trust and sensitivity of the position they occupy in the organization;

(m) Participate in the development of an agency security architecture for all IT systems;

(n) Monitor and coordinate patch management and scanning techniques for all unit systems; participate in identification and mitigation of all system vulnerabilities,

(o) Coordinate the provision of security controls for Portable Electronic Devices (PEDS) and other wireless technology;

(p) Participate in the Overall Agency Security Plan for the program and coordinate with Information Systems Security Officers (ISSO) to ensure that current system specific plans are in place for all IT systems; coordinate or participate in risk assessments of all unit systems and mitigate vulnerabilities;

(q) Monitor CM practices to ensure that security controls are maintained over the life of the IT systems, and formulate and prepare an electronic agency inventory for unit computing devices;

(r) Monitor and participate in assessments to ensure that Privacy requirements are met;

(s) Plan and document security costs for unit IT investments and systems;

(t) Prepare and update reports to ensure that the unit complies with mandated internal and external security reporting requirements, including FISMA and CPIC;

(u) Proactively participate in new CS initiatives including, but not limited to, computer investigations and forensics; and

(v) Prepare and coordinate unit Incident Responses with the agency ISSPM to include all associated actions necessary to mitigate the risk to unit systems.

4 Agency Information Systems Security Officers (ISSO) will:

(a) Be knowledgeable of Federal, Departmental, and agency security regulations when developing functional and technical requirements; serve as a POC for system users with security issues;
(b) Coordinate security program and system elements with the agency IT Program Managers by evaluating system environments for security requirements and controls including: IT Security Architecture, hardware, software, telecommunications, security trends, and associated threats and vulnerabilities;
(c) Manage security controls to ensure confidentiality, integrity and availability of information; build security into the system development process and define security specifications to support the acquisition of new systems; review and sign off on system procurement requests to ensure that security has been considered and included;
(d) Assist with security controls and associated costs in the CPIC Process;
(e) Assist the ISSM in the C&A process, including updates to the overall Agency and System Security Plans (SSP) for the program; serve as a key advisor in risk assessments of all systems and mitigate vulnerabilities; adhere to CM practices to ensure that security controls are maintained over the life of IT systems; update the electronic agency inventory for all agency computing devices;

(f) Adhere to and implement system security controls that ensure the protection of Sensitive But Unclassified (SBU) information using authentication techniques, encryption, firewalls, and access controls;
(g) Assist the ISSPM in following Department Incident Response Procedures;
(h) Assist the system owner and ISSM in the development, testing and maintenance of agency and system contingency plans, backup and storage procedures; document all procedures according to departmental and agency standards;
(i) Audit and monitor application, system and security logs for security threats, vulnerabilities and suspicious activities; report suspicious activities to the agency ISSPM;
(j) Support and facilitate the security awareness, training and education program; and
(k) Assist the ISSM in any other security related duties, as required.

4 RESPONSIBILITIES

a The Associate CIO for Cyber Security (ACIO CS) will:

(1) Act as the recognized Senior Security Officer (SSO) for the department and the central point of contact for CS management within USDA;

(2) Formulate and issue departmental CS policies and procedures for all USDA agencies and staff offices;

(3) Promote and monitor C&A of all USDA IT Systems;

(4) Provide enterprise-wide contractual vehicles and tools for security products and services;

(5) Monitor agencies to ensure that all Security Plans are current for programs and agency IT systems;

(6) Ensure that agencies comply with CS policy and procedures;

(7) Collaborate in identification of material weaknesses and assist in formulating mitigation strategies, if required;

(8) Centralize the department's Computer Incident Response with US-CERT and other computer emergency response teams;

(9) Assist agencies in responding to computer fraud and with the handling of forensic evidence and investigations;

(10) Ensure that agencies implement and maintain managerial, technical, and operational security controls;

(11) Support and promote IT Contingency Planning efforts;

(12) Monitor and evaluate physical security within IT Restricted space;

(13) Ensure agencies meet Privacy Act requirements;

(14) Review and make recommendations to the CIO for all IT Investments and Waiver requests;

(15) Establish and support a Departmental security awareness and training program;

(16) Review requests for exceptions to CS Policy and Procedures in a timely manner; and

(17) Act as the central point for preparing regulatory reports required by FISMA and other legislation.

b Agency Chief Information Officer (CIO) will:

(1) Establish, implement and provide adequate resources for an agency ISSP that provides a comprehensive and proactive security process to protect agency assets;

(2) Be knowledgeable in legal and liability issues surrounding computing devices, the consequences of security breaches and requirements of executive accountability for IT systems;

(3) Ensure that all agency systems are C&A'd prior to operation and that they are reaccredited every three years or when significant system change occurs;

(4) Ensure that Departmental security policy and procedures are disseminated; ensure that internal agency security procedures are implemented, tested, and integrated into the agency culture;

(5) Designate in writing, using the form in Appendix A, an agency ISSPM who is a direct report; ensure that the ISSPM is a permanent member of all agency system development initiatives, telecommunications planning, and SDLC processes;

(6) Provide general and role-based security training to the ISSPM and security staff to include field personnel from USDA enterprise training vehicles;

(7) Establish and monitor an agency Personal Use Policy for all computing devices;

(8) Proactively support the establishment of system security controls at the USDA's C2 Level of Trust and provide protection of SBU information using authentication techniques, encryption, firewalls, access controls, and comprehensive Departmental Incident Response Procedures;

(9) Support agency contingency planning efforts by establishing DR/BR and other emergency plans for all IT systems;

(10) Ensure that the security requirements of IT Restricted Space are followed in maintaining, updating or planning new space;

(11) Ensure that all agency personnel, including contractors, receive security awareness briefings and training based on their role in the organization; conduct background screening of all employees based on the level of trust and sensitivity of the position they occupy in the organization;

(12) Support the development of an agency security architecture for all IT systems;

(13) Ensure patch management and scanning techniques are employed to protect, identify and mitigate system vulnerabilities;

(14) Provide security controls for Portable Electronic Devices (PEDS) and other wireless technology;

(15) Ensure that an overall agency security plan is prepared for the program and current system specific plans are in place for all IT systems;

(16) Conduct risk assessments of all systems and mitigate vulnerabilities wherever feasible;

(17) Establish CM practices to ensure that security controls are maintained over the life of the IT systems;

(18) Ensure that all computing devices are captured in an electronic agency inventory and included in the Department's Enterprise Architecture Repository (EAR);

(19) Ensure that agency and Federal Privacy Act requirements are met;

(20) Ensure that security costs are planned and entered in to agency's annual budget submission for all IT investments and systems;

(21) Ensure that the agency complies with mandated internal and external security reporting requirements, including FISMA and CPIC;

(22) Ensure that support is provided for computer investigations and forensics; and

(23) Proactively support CS initiatives.

c <u>The Agency Information Systems Security Program Managers (ISSPM) will:</u>

(1) Serve as the POC for all agency CS matters; provide subject matter guidance to agency personnel;

(2) Manage the agency ISSP, including field activities;

(3) Participate in the process and monitor the program to ensure that all agency systems are C&A'd prior to operation and that they are reaccredited every three years or when significant system change occurs;

(4) Disseminate Departmental security policy and procedures; formulate internal agency security policies, procedures and support implementation, testing, and integration into the agency culture (mission and business operation);

(5) Participate, as a permanent member, on all agency system development teams, telecommunications planning, and SDLC processes;

(6) Conduct internal audits of all agency IT systems to

ensure compliance with federal and departmental policy and procedures;

(7) Participate in general and role-based security training to enhance knowledge and skill level from USDA Enterprise training vehicles; recommend appropriate training for staff and field personnel from USDA Enterprise training vehicles and other sources to CIO;

(8) Proactively coordinate the establishment of system security controls at the USDA's C2 Level of Trust; the protection of SBU information using authentication techniques, encryption, firewalls, access controls, and comprehensive departmental Incident Response Procedures with all SAs and business owners, and develop security baselines, where applicable;

(9) Coordinate with business owners to categorize information systems and determine sensitivity levels;

(10) Establish DR/BR and other emergency plans for all IT systems; ensure compliance with backup and storage procedures;

(11) Monitor to ensure that the security requirements of IT Restricted Space are followed in maintaining, updating or planning new space, and advise the CIO if space does not meet security requirements;

(12) Develop and manage a Security Awareness Program including arranging or conducting security awareness briefings; recommend to the agency CIO security training for all agency personnel, including contractors, based on their role in the organization; ensure that all personnel are appropriately trained in the Security Rules of Behavior prior to being granted access to agency systems;

(13) Coordinate with local Human Resources Offices to arrange for background screening of all IT employees based on the level of trust and sensitivity of the position they occupy in the organization;

(14) Participate in the development of an agency security architecture for all IT systems;

(15) Monitor and coordinate patch management and scanning programs for all agency systems; participate in identification and mitigation of all system vulnerabilities;

(16) Coordinate the provision of security controls for PEDS and other wireless technology;

(17) Formulate and prepare the overall Agency Security Plan for the program and coordinate with ISSOs to ensure that current system specific plans are in place for all IT systems;

(18) Coordinate or participate in risk assessments of all systems and mitigate vulnerabilities;

(19) Monitor CM practices to ensure that security controls are maintained over the life of the IT systems;

(20) Develop and prepare an electronic agency inventory for all agency computing devices;

(21) Monitor and participate in assessments to ensure that agency Privacy requirements are met;

(22) Plan and document security costs for all IT investments and systems;

(23) Prepare and update agency reports to ensure that the agency complies with mandated internal and external security reporting requirements, including FISMA and CPIC; and

(24) Proactively participate in CS initiatives including, but not limited to, computer investigations and forensics.

d The Agency IRM, Automation Information System Management, Operations and Programming Staff will:

(1) Be knowledgeable of Federal and agency security regulations when developing functional and technical requirements;

(2) Coordinate security program and system elements with the agency IT Program Managers and ISSPM (ISSM or ISSO as appropriate) by evaluating system environments for security requirements and controls including: IT Security Architecture, hardware, software, telecommunications, security trends, and associated threats and vulnerabilities;

(3) Manage security controls to ensure confidentiality, integrity and availability of information; build security into the system development process and define security specifications to support the acquisition of new systems;

(4) Assist with defining security controls and associated costs in the CPIC process;

(5) Assist the system owner and ISSPM in the C&A process, including updates to the overall Agency and System Security Plans (SSP);

(6) Participate in risk assessments of all systems and mitigate vulnerabilities;

(7) Adhere to CM practices to ensure that security controls are maintained over the life of IT systems;

(8) Update the electronic agency inventory for all agency computing devices;

(9) Adhere to and implement system security controls at the USDA C2 Level of Trust and ensure the protection of SBU information using authentication techniques, encryption, firewalls, and access controls;

(10) Assist the ISSPM in following department Incident Response Procedures;

(11) Assist the system owner and ISSPM in the development, testing and maintenance of Agency and System Contingency Plans, backup and storage procedures; document all procedures according to departmental and agency standards;

(12) Audit and monitor application, system and security logs for security threats, vulnerabilities and suspicious activities; report suspicious activities to the agency ISSP Office; and

(13) Assist the ISSPM in any other security related duties, as required.

-END-

APPENDIX A
DESIGNATION OF ISSPM AND DEPUTY ISSPM

Name:_____

Agency: _____

GS Series/Title:_____

Level of Background
Investigation:_____

Location: _____

_____

Phone Number: _____ Cell Number: _____

Fax Number: _____ E-mail:_____

Agency CIO Name :_____

Agency CIO Signature: _____

Date: _____