United States Department of Agriculture
Marketing and Regulatory Programs
Animal and Plant Health Inspection Service

Directive **APHIS 3140.5** **3/17/09**

APHIS INFORMATION SYSTEMS SECURITY (ISS) ROLES AND RESPONSIBILITIES

1. PURPOSE

This Directive establishes policy and sets forth the responsibilities of the Animal and Plant Health Inspection Service (APHIS) employees whose positions support the Information Systems Security Program (ISSP).

2. REPLACEMENT HIGHLIGHTS

This Directive replaces APHIS Directive 3140.5, dated 5/26/00.

3. AUTHORITIES/REFERENCES

a. Computer Security Act of 1987. In this Act (Public Law 100-235), Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and creates a means for establishing minimum acceptable security practices for Federal information systems.
http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf

b. Clinger-Cohen Act. This Act (Public law 104-106, Division E) defines reforms in information technology acquisition management within the Federal Government.
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ106.104

c. Federal Information Security Management Act (FISMA). This Act (Title III of the E-Government Act of 2002) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.
http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

d. Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources. This Appendix establishes a minimum set of controls to be included in Federal automated information security programs. It also assigns Federal agency responsibilities for the security of automated information.
http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

e. United States Department of Agriculture (USDA) Department Manual (DM) 3555-01, Certification and Accreditation (C&A) Methodology. This DM provides a high-level overview of the roles related to the certification and accreditation life cycle.
http://www.ocio.usda.gov/directives/index.html

f. USDA APHIS Strategic Plan 2007-2012. The APHIS Strategic Plan defines the strategic direction as it relates to the Agency mission.
http://www.aphis.usda.gov/about_aphis/strategic_plan.shtml

g. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. The FIPS 200 provides security requirements for applications.
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

h. National Institute of Standards and Technology (NIST) Special Publication 800-61, Computer Security Incident Handling Guide. This Guide provides incident handling capability models.
http://csrc.nist.gov/publications/PubsSPs.html

i. NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, Test Procedures. This Guide provides guidance in executing the Security Test and Evaluation (ST&E) process.
http://csrc.nist.gov/publications/PubsSPs.html

j. Computer Fraud and Abuse Act. This Act holds employees individually and personally responsible for their computers.
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+18USC1030

4. SCOPE

a. This Directive applies to all APHIS employees as well as other Federal agencies, State and local governments, and private organizations or individuals who use APHIS information systems to accomplish APHIS business functions. All of the aforementioned are considered users and are included wherever the words “user” or “users” are referenced within this Directive.

b. APHIS information systems covered by this Directive include all information systems that process, store, or transmit data in support of APHIS’ mission. This includes all computer hardware, software, telecommunications equipment, or other information resources that comprise the APHIS network of general support systems or applications and services they support.

5. IMPLEMENTATION

This Directive must be implemented within 90 days of issuance. Programs must provide an implementation plan that details actions that will be taken to achieve full compliance with this Directive.

6. POLICY

a. All APHIS users have a responsibility to participate in the ISSP and must perform their duties in ways that support ISSP goals. In keeping with the philosophy of "least privilege", users will be provided access to and use of only those information resources needed to accomplish their official business duties. Systems will be installed, operated, and maintained with only those features or services required to satisfy official business requirements in support of APHIS' mission.

b. APHIS has a specific responsibility to protect information resources and will comply with all Federal and Departmental policies, regulations, and requirements.

c. APHIS security roles are described below:

(1) Administrator.

(2) Program Deputy Administrator.

(3) APHIS Chief Information Officer (CIO) / Certification Agent.

(4) APHIS ISSP Manager (ISSPM).

(5) Program CIO / Certification Agent.

(6) System Owner.

(7) Program ISS Manager (ISSM).

(8) Program ISS Officer (ISSO).

(9) IT Incident Response Personnel.

(10) Project Manager.

(11) System/Network Administrator.

(12) Application Developer.

(13) Procurement Professionals.

(14) Security Test and Evaluation Team.

7. RESPONSIBILITIES

a. The Administrator, in accordance with FISMA, will ensure that APHIS has an established ISSP that:

(1) Provides information security protections commensurate with the risk in consideration of the magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.

(2) Ensures that information security management processes are integrated with Agency strategic and operational planning processes.

(3) Delegates to the APHIS CIO the authority to ensure compliance with the requirements imposed by FISMA.

(4) Ensures the Agency has trained personnel to assist in FISMA compliance.

(5) Ensures that the APHIS CIO, in coordination with program unit senior program officials, reports annually on the effectiveness of the APHIS ISSP to USDA.

b. Program Deputy Administrators' heads of program units are responsible for their program unit's Information Technology (IT) security, and must:

(1) Serve as the Authorizing Official (AO) for systems in their programs. The AO is a USDA program executive with the authority to evaluate the mission, business case, and budgetary needs for the system in view of the security risks present in the system's operating environment.

Note: APHIS uses the AO title instead of Designated Authorizing Agent (DAA) to be compliant with NIST and Federal requirements.

(2) Concur with the recommendation of the Associate CIO for Cyber Security (ACIO-CS). In accordance with USDA DM 3555-001, the AO will:

(a) Be the business owner of the general support system or system being certified and accredited.

(b) Assume responsibility for the residual risks of operation of the system in a stated environment.

(c) Formally approve the operation of an IT system at an acceptable level of risk within its environment by issuing an accreditation decision. Accreditation decisions include the issuance of:

1 Authorization to Operate (ATO). If, after assessing the results of the security certification, the AO deems that the risk to Agency operations, Agency assets, or individuals is acceptable, an ATO is issued for the information system.

2 Interim Authorization to Operate (IATO). If, after assessing the results of the security certification, the AO deems that the risk to Agency operations, Agency assets, or individuals is unacceptable, but there is an overarching mission necessity to place the information system into operation or continue its operation, an IATO may be issued.

Note: It is USDA policy not to recognize IATO; however, the risk may be assessed and accepted internally to allow a system to operate under an IATO for the timeframe specified below:

a High and moderate impact systems – 90 business days.

b Low impact systems – 180 business days.

3 Denial of Operation to Operate (DTO). If, after assessing the results of the security certification, the AO deems that the risk to Agency operations, Agency assets, or individuals is unacceptable, the authorization to operate the information system will be denied.

4 Previous Authorization. In the event that a new AO is assigned responsibility for the information system, the newly assigned AO should review the current security accreditation package (i.e., accreditation decision, decision rationale, and terms and conditions) and the current system status reports to determine if a reaccreditation action is warranted. If the new AO is willing to accept the currently documented risk, then reaccreditation occurs only when there is a significant change to the information system or when a specified time period has elapsed in accordance with Federal or Agency policies.

5 Approved security requirements documents to include: Memoranda of Agreement (MOA), Memoranda of Understanding (MOU), and any deviations from security policies.

(d) Communicate to all APHIS employees that information systems security is important to APHIS' mission.

(e) Assign security management and daily system operations to program officials and system owners.

c. The APHIS CIO, in accordance with FISMA, will:

(1) Approve and issue APHIS ISSP directives and standards that establish a framework for an ISSP to be implemented by APHIS and its program units.

(2) Monitor, evaluate, and report to the Administrator on the status of information systems security within APHIS.

(3) In accordance with DM 3555-001, serve as the certification agent for:

(a) Low impact Marketing and Regulatory Programs Business Services (MRPBS) systems.

(b) Moderate and high impact applications/systems for all APHIS systems.

(4) Designate, in writing, an ISSPM to execute the APHIS ISSP, which will:

(a) Develop and maintain an APHIS ISSP.

(b) Develop and maintain ISS policies, procedures, and control techniques.

(c) Train and provide guidance to personnel with significant IT ISS responsibilities.

(d) Assist Agency officials in carrying out their FISMA responsibilities.

(5) Act as the certification agent for all systems within his/her programs. The certification agent will:

(a) Conduct a security certification which includes a comprehensive assessment of the management and operational and technical security controls of an information system.

(b) Determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome in meeting the security requirements for the system.

(c) Provide the recommended corrective actions to reduce or eliminate vulnerabilities in the information system.

(d) Provide independent assessments of the system security plan to ensure the plan adequately describes the security controls for the information system. The certification agent should be in a position that is independent of individuals who are responsible for the:

<u>1</u> Development of the information system.

<u>2</u> Day-to-day operation of the system.

<u>3</u> Correction of security deficiencies identified during the security certification.

Note: The independence of the certification agent is an important factor lending credibility to the security assessment results and ensuring the AO receives the most objective information possible in order to make an informed, risk-based, accreditation decision.

d. The <u>APHIS ISSPM</u> will:

(1) Be a full-time Federal employee appointed by the APHIS CIO.

(2) Develop, document, and implement an Agency-wide ISSP.

(3) Ensure information systems security is included in all initiatives to include strategic planning, security enterprise architecture, etc.

(4) Monitor and evaluate the status of the APHIS information systems security by performing annual compliance reviews of program and system controls.

(5) Advise the APHIS CIO and program unit CIOs of technological advances in information security that can be used on an Agency-wide basis to provide reduced costs for information systems security efforts.

(6) Report, as appropriate, to the APHIS CIO and external entities, such as OMB, the Government Accountability Office, and Congress, on APHIS ISSP.

(7) Provide information system security guidance and technical assistance to all program units.

(8) Monitor APHIS level weaknesses and monitor program level weaknesses reported as a result of self-assessments and external reviews using the FIMSA security management tool.

(9) Identify resource requirements, including the funding and personnel needed to efficiently manage the APHIS ISSP.

(10) Plan and chair regular meetings of the IT Leadership Advisory Council (IT-LAC) sub-committee, and the APHIS ISSM Council.

(11) Lead APHIS certification teams in support of the APHIS CIO certification duties.

e. The Program CIO, in accordance with FISMA, will:

(1) Provide an information systems security program management infrastructure that supports APHIS ISSP requirements.

(2) Appoint, in writing, an ISSM and ISSO and alternates to implement the APHIS ISSP requirements. Copies of the assignment letters must be maintained on file for the duration of the employees' appointments.

(3) Ensure that individuals working on ISS are properly trained and supported.

(4) Provide feedback to the APHIS ISSPM on the status of the program's security posture as required by FISMA.

(5) Serve as the certification agent for:

a Low impact program systems.

b Moderate and high impact applications/systems for other programs.

Note: The Program CIO may not certify moderate or high applications/systems for which he/she has direct operational control within his/her program.

f. APHIS System Owners are responsible for the day-to-day management and operations of applications and systems under their purview. In accordance with DM 3555-001, system owners will:

(1) Ensure certification and accreditation is maintained for all current and new systems under their purview.

(2) Ensure the system is deployed and operated according to the security controls.

(3) Conduct annual self-assessments of system safeguards on all operational systems and applications under their purview.

(4) Establish system-level plans of action and milestones (POA&Ms) and implement corrective actions in accordance with the APHIS standard for POA&Ms.

(5) Grant individuals the fewest possible privileges necessary for job performance (any privileges not specifically granted are denied access) so that privileges are based on a legitimate need to have system access. APHIS will re-evaluate system owners' access privileges annually and revoke access in a timely manner upon personnel transfer or termination.

(6) Implement rules of behavior for all systems that apply to all personnel managing, administering, or having access to the APHIS IT system.

(7) Notify the ISSM/ISSO of any suspected incidents in a timely manner, and assist in the investigation of incidents, if necessary.

(8) Ensure IT system service contracts include ISS provisions.

(9) Ensure systems' personnel are properly designated, monitored, and trained, including the appointment, in writing, of an individual to serve as the ISSO.

(10) Ensure system data is kept up-to-date using the FISMA security management toolset.

g. The APHIS Program ISSM will:

(1) Be a full-time Federal employee appointed by the Program CIO.

(2) Serve as the central point of contact for the program's overall ISSP.

(3) Ensure that the appropriate operational security posture is maintained for applications/information systems in his/her program.

(4) Serve as the principal advisor to the program's AO and system owners on all matters involving the security of the program's applications and systems.

(5) Maintain copies of all current program C&A packages for use in performing required security monitoring activities and reporting.

(6) Perform certification duties in support of the program CIO and ensure annual compliance reviews are conducted to verify that all systems have in place effective, quality security documentation.

(7) Conduct self-assessments of the program's ISSP annually to ensure effective implementation of, and compliance with, established policies, directives, and procedures.

(8) Establish an internal standard process to monitor, track, and close remedial actions required to mitigate risks in accordance with the APHIS standard for POA&Ms and the FISMA security management toolset.

(9) Assist the system owner in establishing a standard internal process to ensure that all users receive periodic security awareness briefings, copies of rules of behavior, and are trained to fulfill his/her ISS responsibilities.

(10) Assist the system owner in ensuring access privileges are revoked in a timely manner (e.g., transfer, resignation, retirement, change of job description, etc.) -- immediately for an individual being separated for adverse reasons or just prior to notifying him/her of the pending action.

(11) Notify system owners of user infractions identified during routine compliance assessments.

(12) Maintain the IT system inventory in accordance with the FISMA management toolset.

(13) Act as the program unit's central point of contact for all information security incidents and report incidents to the APHIS ISSPM.

(14) Distribute, as necessary, information to systems administrators and others concerning risks and potential risks to systems.

(15) Participate as a voting member of the APHIS ISSM Council, participate in special committees under the ISSM Council, and provide other support for the ISSM Council, as appropriate.

(16) Serve as the Contracting Officer Technical Representative (COTR) on IT security related contracts (e.g., C&A, etc.) within his/her program.

(17) Ensure that all deliverables are in compliance with all NIST, Departmental, and APHIS guidelines.

h. The Program ISSO is the individual responsible for working with the system owner and ISSM for ensuring the appropriate operational security posture is maintained for an information system. Multiple information systems may be assigned to a single ISSO.

i. The APHIS ISSO must:

(1) Have a working knowledge of system functions, security policies, and technical security protection measures.

(2) Have the detailed knowledge and expertise required to manage the security aspects of the information system. He/she is generally assigned responsibility for the day-to-day security operations of the system.

(3) Be appointed, in writing, by the system owner.

(4) Ensure the implementation of security protection controls and procedures that are documented in, or referenced by, the System Security Plan for each information system for which he/she is responsible.

(5) Assist the system owner and ISSM in ensuring that all users have the requisite security clearances, authorization, need-to-know, and are aware of their security responsibilities before being granted access to the information system.

(6) Assist the system owner and ISSM in ensuring that each information system user acknowledges his/her responsibility for the security of information systems and information.

(7) Maintain, and update annually, a copy of the C&A package for each information system for which he/she is the ISSO.

(8) Ensure that the ISSM is notified when an information system is no longer needed or when changes are planned that might affect the accreditation of the information system.

(9) Participate in the ISSM’s self-assessment and training programs.

(10) Communicate individual incident(s) and potential incident reports to the ISSM and initiate protective or corrective actions.

(11) Ensure that unauthorized personnel are not granted use of, or access to, the information system.

j. IT Incident Response Personnel will implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. The incident response capability *may* adopt one of several models described in NIST Special Publication 800-61, Computer Security Incident Handling Guide, and:

(1) Ensure that each system or program unit's respective IT incident response personnel have been trained in their incident response roles and responsibilities and provided refresher training annually.

(2) Test the incident response capability annually using tests and conduct exercises as defined by the system owner to determine the incident response effectiveness.

(3) Manage, monitor, and document all ISS incidents on an ongoing basis.

k. The IT Project Manager will work with the system owner to coordinate all activities that comprise a system's life cycle from design through implementation. The IT Project Manager reports to the system owner.

l. The System/Network Administrator's role may include security of local area network or application administration. As directed by the system owner, the system/network administrator will:

(1) Assist in the development and maintenance of system security plans and contingency plans for all systems under his/her responsibility.

(2) Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies.

(3) Participate in self-assessments of system safeguards, program elements, and in C&A of the system.

(4) Evaluate proposed technical security controls to ensure proper integration with other system operations.

(5) Identify requirements for resources needed to effectively implement technical security controls.

(6) Ensure the integrity of the implementation and operation of technical security controls by conducting control security tests and evaluations.

(7) Develop system administration and standard operating procedures and manuals as directed by the system owner.

(8) Evaluate and develop procedures to ensure proper integration of service continuity with other system operations.

(9) Notify the responsible system owner or ISSM/ISSO of any suspected incidents in a timely manner, and assist in the investigation of incidents, if necessary.

(10) Read and understand all applicable training and awareness materials.

(11) Read and understand all applicable use policies or other rules of behavior regarding use or abuse of program unit IT resources.

(12) Know which systems or parts of systems for which he/she is directly responsible (e.g., network equipment, servers, LAN, etc.), the sensitivity of the data he/she handles and take appropriate measures to protect it.

(13) Know and abide by all applicable APHIS and program directives and procedures.

m. Application Developers are responsible for developing applications. All applications must be developed in accordance with FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.

n. IT Procurement Professionals will ensure all IT contracts have specifically and adequately addressed the Federal Acquisitions Process, APHIS ISSP, USDA Departmental Regulations, and the NIST guidelines in their language and implementation.

o. The APHIS ST&E Team consists of personnel independent of the IT infrastructure and program systems/applications. The independent ST&E team is NOT required for “low” systems, and is responsible for executing the ST&E process in accordance with NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, Test Procedures.

8. EXCEPTIONS

a. Exceptions that reduce the requirements of this Directive may be approved only in writing by Unit Heads, the CIO, or the APHIS Administrator.

b. Each Program/Business Unit is authorized to develop and implement policies and procedures, which may (based on risk assessment, mission, legislative mandate, or information sensitivity) be more stringent or specific than those documented in this Directive.

9. COMPLIANCE AND SANCTIONS

All employees who work with APHIS resources are individually and personally responsible for applying the appropriate security measures and for complying with Federal, USDA, and APHIS policies and procedures on the subject. Willful failure to comply may result in punishment, including dismissal, under the Computer Fraud and Abuse Act and other appropriate Federal statutes.

10. INQUIRIES

a. Direct inquiries or requests for changes to this Directive to the APHIS ISSPM, 4700 River Road, Unit 103, Riverdale, MD 20737 or call 301-851-2483.

b. Copies of current APHIS Directives can be accessed on the Internet at http://www.aphis.usda.gov/library/directives/

/s/
Marilyn Holland
APHIS Chief Information Officer