APHIS INFORMATION SYSTEMS SECURITY (ISS) ROLES AND RESPONSIBILITIES

1. PURPOSE

a. This Directive establishes policy and sets forth specific responsibilities for APHIS employees in support of Information Systems Security (ISS).

b. The fundamental purpose of any security measure is to prevent losses. The APHIS ISS program exists to prevent or mitigate loss, damage, or disruption of information resources. which have become essential to the delivery of services and the operation of the Agency.

2. AUTHORITY AND REFERENCES

Basic APHIS ISS policy is contained in Directive 3140.1. Applicable national policy requirements regarding ISS are stated primarily in Presidential Decision Directive 63, Critical Infrastructure Protection-, the Computer Security Act of 1987 (Public Law (P.L.) 100-235), Office of Management and Budget (OMB) Bulletin 90-08, Appendix III of OMB Circular A- 1 30, Security of Federal Automated Information Systems; OMB Circular 1- 123, Management Accountability and Control; and the Computer Fraud and Abuse Act (18 U.S.C. Sec. 1030 [1993]). Taken together, these documents and others not cited prescribe establishing and maintaining a comprehensive ISS program that addresses managerial, technical, and continuity of operation issues inherent in Federal organizations. Additionally, United States Department of Agriculture (USDA), Office of Information Resources Management (OIRM), Department Regulation 3140-1, USDA IRM Security Policy, applies, as do policies and requirements related to protecting sensitive information, such as the Privacy Act of 1974 (P.L. 93579, 5 U.S.C. 552a).

3. SCOPE

a. This Directive applies to:

(1) All APHIS employees and contractors.

(2) Other Federal agencies, State and local governments, and private organizations or individuals who use APHIS information systems to accomplish an APHIS business function. 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 (IS) covered by this Directive include all computer hardware, software, and telecommunications that support APHIS business functions. This includes networks, program unit and administrative databases, office automation products (Smartsuite, Word Pro, Freelance Graphics, etc.), Lotus Notes and other electronic mail, and connections to the Internet.

4. POLICY

(1) All APHIS users have a responsibility to assist with ISS efforts and must perform their duties in ways that support ISS goals. In keeping with the philosophy of "least privilege" established in APHIS Directive 3140.1, users will be provided access to and use of only those nonpublic information resources needed to accomplish their jobs. Systems will be installed, operated, and maintained with only those features or services actually needed to accomplish APHIS missions.

(2) APHIS has specific responsibilities to protect information resources and will comply with Federal and Departmental policies, regulations, and requirements on ISS.

5. RESPONSIBILITIES

a. The Chief Information Officer (CIO), will:

(1) Provide general oversight for the APHIS ISS program, ensuring that goals are set and adequately supported to maintain credible and effective protection for the Agency's information assets.

(2) Appoint an Information Systems Security Program Manager (ISSPM) to manage the ISS program on behalf of the Administrator and provide the ISSPM with the resources necessary to ensure implementation of established ISS requirements.

(3) Empower the ISSPM to lead and assist APHIS Program/Business Units in Information Systems Security Program development. He/she will ensure thorough reviews of Units for compliance with Federal, Departmental, and Agency policies and procedures.

(4) Establish an appropriate body of senior IT personnel to review proposed ISS-related policies, directives, regulations, and guidelines.

(5) Be responsible for ensuring effective ISS measures for General Support Systems (GSS) that serve APHISwide missions and functions or application systems that transcend Unit boundaries and thereby affect the

entire Agency. The CIO will accredit (formally approve operation of) such systems, balancing operational requirements with prudent security measures. This includes ensuring that technical safeguards are established and maintained to:

(1) Protect GSS with a predetermined minimum set of safeguards.

(2) Prevent (to the extent possible) successful attacks on APHIS GSS or use of those systems by unauthorized personnel.

(3) Ensure compliance with APHIS ISS policies and procedures regarding GSS. This includes such actions as periodically running special software routines to ensure that passwords are robust and changed frequently and that known technical operating system vulnerabilities are corrected in a timely manner.

(4) Periodically review the status of GSS to ensure that changes have not occurred that negatively affect security. This will be done both manually (peer/management reviews of proposed changes) and by using specialized software tools.

(5) Enable monitoring of IS resources, with appropriate endorsement from the Internal Audit office (Resource Management Systems and Evaluation Staff (RMSES)) who will ensure compliance with the Electronic Communications Privacy Act, when there is credible evidence that specific personnel are misusing those resources.

(6) Ensure viable contingency plans for APHIS GSS.

(6) Ensure that Information Systems Security Managers (ISSM's) are appointed within lTc to implement the Agency's ISS program for GSS and submit the ISSM names to the APHIS ISSPM. The CIO will ensure those ISSM's are trained in ISS matters and formally evaluated on the performance of security-related duties. In accordance with USDA policy, ISSM’s and system administrators must successfully complete a background investigation to ensure their trustworthiness; successful completion of periodic re-investigations also is required.

(7) Promote general ISS awareness and training.

(8) Monitor overall compliance with Federal and Agency ISS policies.

a. Deputy Administrators/Directors of Program Units and Heads of Major Business Offices will:

(1) Be responsible for ensuring an effective ISS program in their organization. They will provide for the integrity, availability, and confidentiality of information that is critical to APHIS to meet its missions.

(2) Accredit (formally approve operation of) each major application system in use in their area of operation, balancing operational requirements with prudent security measures. This constitutes the decision authority (DAA - Designated Approving Authority) for establishing what controls and safeguards are reasonable and appropriate for their business data. This authority may not be redelegated. Accreditation applies to:

(a) New systems, incorporating security from initial concept and design through the life cycle of the system through disposal.

(b) Existing systems to ensure they are used, maintained, modified, and disposed of with attention to reasonable and prudent security requirements.

(3) Appoint, in writing, an ISSM to represent them on ISS matters and to implement the APHIS ISS-program within their organization. He/she will ensure their ISSM (and Information Systems Security Officer's (ISSO's), if appointed) are trained in ISS matters and formally evaluated on the performance of security-related duties. They will submit the ISSM name and contact information to the APHIS ISSPM, both when initially appointed and when changed.

(4) Ensure that responsibility for each major application is assigned to a management official knowledgeable in the nature of the information and process supported by the application including management, personnel, operational, and technical controls used to protect it. These "system owners" will work closely with ISSM's and ISSO's to ensure an effective ISS program.

(5) Provide the necessary resources to ensure implementation of APHIS ISS policy and to ensure that security is included in all stages of each application system's life cycle.

(6) Ensure that procedures are established to maintain individual accountability for information resources to which individuals have access. They will ensure individuals have only the access necessary to accomplish authorized

activities, in keeping with the APHIS policy of "least privilege" operations.

(7) Promote ISS awareness and training.

(8) Ensure that controls are established and maintained to modify/revoke information access privileges for employees transferring to a new position or leaving the Agency entirely. They will ensure that departing employees are debriefed on their access to APHIS systems and sensitive information, and turn-in of IS materials.

(9) Oversee and approve development of supplemental ISS standards and procedures -- beyond those established by the CIO for APHIS GSS and Agencywide applications -- as needed for Unit application systems.

(10) Establish and maintain viable IS contingency plans for appropriate application systems.

(11) Monitor Unit compliance with this Directive.

c. The ISSPM will:

(1) Be the lead ISS specialist for APHIS, managing the Agency's ISS program in a manner consistent with USDA and Federal policies, and serving as the Agency's authority on these issues.

(2) Establish an APHIS ISS structure that is logical, structured, and modular to allow:

(a) Maximum flow of ISS-relevant information.

(b) Problems to be resolved at the lowest practicable level.

(c) Ensured knowledge and skill at many levels to deal with questions or problems, even when key personnel may be absent.

(3) Advise management on standards and procedures to ensure data and system confidentiality, integrity, and availability. He/she will monitor and report on Agency compliance with Federal laws, requirements, and standards and USDA policies.

(4) Represent APHIS to the USDA ISSPM and ISS specialists in other Federal organizations. The ISSPM will establish and maintain working relationships with APHIS ISSM's, ISSO's, and APHIS employees to

exchange information and ideas about ISS.

(5) Ensure that ISSM's are appointed for Program and Business Units, in technical areas, and other areas as needed. The ISSPM will provide leadership to and coordinate the activities of ISSM's and others assigned security responsibilities in Program/Business Units.

(6) Coordinate development of ISS plans with system owners. Ensure development of a "Security Features Users Guide" or similar document for systems that process "high" or moderate" value information. This document will describe the sensitivity of the data, explain the need for protection, and establish specific safeguards for protecting data.

(7) Test (or monitor tests) for vulnerability of security safeguards.

(8) Provide guidance on risk assessment methodology and review assessments of systems.

(9) Guide development of security requirements for the acquisition of hardware/software/services, throughout the system life cycle.

(10) Monitor remedial measures, technical and otherwise, to correct deficiencies identified in audits or inspections or from security incidents.

(11) Coordinate or conduct ISS awareness and education, including training of deputy ISSPM's and ISSM's. He/she will answer questions regarding ISS policies and procedures.

(12) Act as the focal point for handling ISS-related incidents or violations, performing or directing investigations, and reporting as required.

(13) Be permitted to attend, at APHIS expense, at least two ISS-related conferences, training seminars, or other professional development events during each calendar year, in order to maintain proficiency and stay abreast of changes in the ISS arena.

(14) Submit to and successfully complete a background investigation to ensure their trustworthiness. Successful completion of periodic re-investigation also is required.

d. ISSM's for Program/Business Units will:

(1) Be the lead ISS specialists for their Unit, managing ISS efforts and serving as the Unit's authority on these issues. They will represent and report directly to (for ISS matters) Program/Business Unit heads. This appointment must be made in writing and ISSM's must be evaluated formally on performance of their ISS responsibilities.

(2) Advise management on policies, standards, procedures, and specific safeguards to ensure data and application system confidentiality, integrity, and availability. They will provide advice regarding Unit compliance with Federal laws, requirements, and standards as well as USDA/APHIS policies.

(3) Establish and maintain a positive working relationship with the ISSPM to collaborate and cooperate in maintaining and improving the APHIS ISS program.

(4) Ensure that ISSO's are appointed, in writing, for major sites or systems, as needed, to establish and maintain an effective ISS program in the Unit. ISSM's will coordinate the activities of ISSO's, providing guidance and oversight as necessary. (Actual appointment of ISSO's depends on factors that are unique to each Program/Business Unit. If ISSO's are not appointed, the ISSM is responsible for performing those duties.

(5) Help establish controls to ensure that employee access to sensitive data is appropriately limited, to provide proper operational control of the flow of sensitive data through the organization.

(6) Coordinate development of the ISS plans with each system "owner" and ISSO. ISSM's will assist in developing security requirements for the acquisition of hardware/software/services throughout each system's life cycle. They will ensure that sensitive applications are operated and maintained according to USDA/APHIS ISS policies and the approved level of risk.

(7) Test (or monitor tests of) application systems for security vulnerabilities at irregular intervals (a minimum of once a year).

(8) Participate in risk analyses for sensitive application systems, assisting Deputy Administrators/Directors in determining needed safeguards and acceptable levels of risk.

(9) Ensure that each sensitive application system is property accredited for operation. They will provide a copy of the security plan and accreditation

approval to the Agency ISSPM at least annually, for inclusion in the report to USDA. They will provide a list of sensitive application systems and the ISSO responsible for each to the APHIS ISSPM as needed.

(10) Administer/monitor remedial measures to correct deficiencies identified in audits or inspections or from security incidents.

(11) Coordinate or conduct ISS awareness, training, and education activities for all employees in their organization, including ISSO's, functional managers, and users. They will answer questions regarding ISS policies and procedures.

(12) Investigate ISS-related incidents or violations. They will make initial, interim (if needed), and final reports of incidents and violations to the ISSPM.

(13) Be permitted to attend classroom training on ISS issues and safeguards. This training must be attended, at APHIS expense, as soon as possible after being appointed. Unit ISSM's also should be permitted to attend, at APHIS expense, at least one ISS-related conference, training seminar, or other professional development event during each calendar year, in order to maintain proficiency and stay abreast of changes in the ISS arena.

e. ISSM's for GSS will:

(1) Be the lead ISS specialist for their assigned specialty area (either IT unit of technical area), managing ISS efforts and serving as a technical authority for protection of assigned GSS. They will represent and report directly to their Information Technology community (ITc) coach (for ISS matters). This appointment must be made in writing and ISSM's must be evaluated formally on performance of their ISS responsibilities.

(2) Help identify technical security risks applicable to assigned GSS. They will help identify and apply needed technical security controls for GSS and help the CIO/lTc coaches/ISSPM weigh technical security costs/benefits.

(3) Establish and maintain a positive working relationship with the ISSPM to collaborate and cooperate in maintaining and improving the APHIS ISS program.

(4) Ensure that ISSO's are appointed, in writing, for major sites or GSS(particularly at geographically remote locations) as needed to establish and maintain effective protection for systems that support the entire Agency. They will coordinate the activities of ISSO's, providing guidance and oversight as necessary. If ISSO's are not appointed, the ISSM is responsible for performing those duties.

(5) Coordinate development of ISS plans for GSS with each system ISSO'S. They will assist in developing security requirements for the acquisition of hardware/software/services throughout each GSS life cycle. They will ensure that assigned GSS are operated and maintained according to USDA/APHIS ISS policies and the approved level of risk.

(6) Test (or monitor tests of) application systems for vulnerability of security safeguards at irregular intervals (a minimum of twice per year).

(7) Assist with risk assessments and security certification and accreditation of each GSS, assisting the CIO/lTc coaches/ISSPM in determining needed safeguards and acceptable levels of risk.

(8) Ensure that each GSS is properly accredited for operation. They will provide a copy of the security plan and accreditation approval to the Agency ISSPM at least annually, for inclusion in the report to USDA. They will provide a list of GSS and the ISSO's responsible for each to the APHIS ISSPM as needed.

(9) Administer/monitor remedial measures to correct deficiencies identified in audits or inspections or from security incidents.

(10) Coordinate or conduct ISS awareness, training, and education activities for all employees in their assigned area, including ISSO's, system administrators, analysts, programmers, and technical assistants. They will answer questions regarding ISS policies, standards, and procedures.

(11) Investigate ISS-related incidents or violations. They will make initial, interim (if needed), and final reports of incidents and violations to the ISSPM.

(12) Be permitted to attend classroom training on ISS issues and safeguards. This training must be attended, at APHIS expense, as soon as possible after being appointed. GSS ISSM's also should be permitted to attend, at APHIS expense, at least one ISS-related conference, training seminar, or other professional development event during each calendar year, in order to maintain proficiency and stay abreast of changes in the ISS arena.

f. Customer Service ISSM's will:

(1) Assist Program/Business Unit ISSM's in implementing security measures across their assigned Program/Business Unit. They will represent and report directly to the Customer Service (CS) coach (for ISS matters). This

appointment must be made in writing and CS ISSM's must be evaluated formally on the performance of their ISS responsibilities.

(2) Help identify operational and technical security risks applicable to systems, both application and GSS. They will help ISSM's for GSS implement technical security measures.

(3) Establish and maintain a positive working relationship with the ISSPM to collaborate and cooperate in maintaining and improving the APHIS ISS program.

(4) Help ensure that employee access to sensitive data is appropriately limited to provide proper operational control of the flow of sensitive data through the organization.

(5) Assist with risk assessments for sensitive application systems, assisting ISSM's and Deputy Administrators/Directors in determining needed safeguards and acceptable levels of risk.

(6) Advise on and administer remedial measures to correct deficiencies identified in audits or inspections or from security incidents.

(7) Coordinate or conduct ISS awareness, training, and education activities for all employees in their assigned area. They will answer questions regarding ISS policies, standards, and procedures.

(8) Help prevent serious security problems through user education, advice to application developers, and by assisting with installation/use of security tools such as antivirus software.

(9) Help investigate ISS-related incidents or violations.

(10) Be permitted to attend classroom training on ISS issues and safeguards. This training must be attended, at APHIS expense, as soon as possible after being appointed. CS ISSM’s also should be permitted to attend, at APHIS expense, at least one ISS-related conference, training seminar, or other professional development event during each calendar year, in order to maintain proficiency and stay abreast of changes in the ISS arena.

g. ISSO’s for Specific Sites or Systems will:

(1) Administer ISS efforts within their assigned area, identifying and working to correct weaknesses and noncompliance with established safeguards.

(2) Help identify, develop, and implement needed security controls throughout the life cycle of the system(s) for which they have ISS responsibilities. They will review and sign off on procurement requests that affect the system(s) (additions or changes to hardware, software, telecommunications, etc.), verifying that security has been considered and included in the procurement request.

(3) Help administer the ISS awareness/education program. They will serve as primary point of contact for users who have questions about ISS policies, standards, and procedures.

(4) Advise functional managers about ISS issues, policies, requirements, and recommended safeguards. They also will document specific security procedures for the system(s) for which they have responsibility.

(5) Recommend and administer effective physical security measures to protect information resources and the specific system(s) for which they have responsibility.

(6) Serve as primary point of contact for completing risk assessments (but not as a replacement for involvement of functional managers).

(7) Develop ISS plans, including accreditation documentation, for the system(s) for which they have responsibility. They will provide copies of these documents to the Program ISSM as needed.

(8) Develop a Security Features Users Guide or similar document for any system assigned to them that processes "high" or “moderate" value information. This document will describe the sensitivity of the data, explain the need for protection, and establish specific safeguards for protecting data.

(9) Serve as primary point of contact for ensuring that users have appropriate access authorizations, including access to remote systems such as those operated by the National Finance Center. They will ensure that established safeguards are in place and used to protect user passwords. They will ensure that passwords of departing employees are canceled.

(10) Ensure that contingency and disaster recovery plans are developed for sensitive systems.

(11) Implement remedial measures to correct deficiencies identified in audits or inspections.

(12) Investigate ISS-related incidents or violations. They will make initial, interim (if needed), and final reports of incidents and violations to their ISSM.

(13) Become knowledgeable of USDA/APHIS ISS issues, policies, and recommended safeguards. Knowledge may be gained by reading or briefings from their Unit ISSM or by attending formal classroom training available after being appointed. ISSO's also should be permitted to attend, at APHIS expense, at least one ISS-related conference, training seminar, of other professional development event during each calendar year, in order to maintain proficiency and stay abreast of changes in the ISS arena. Classroom training and attendance at periodic conferences/seminars are a "must" (not should) for ISSO's of systems designated high value, according to the information valuation criteria established within APHIS.

(14) Be adequately trained in ISS.

(a) GSS ISSO's must be permitted classroom training on ISS issues. This training must be attended, at APHIS expense, as soon as possible after being appointed. ISSO's also should attend, at APHIS expense, at least one ISS-related conference, technical seminar, or other professional development event during each calendar year, in order to maintain proficiency and stay abreast of changes in the ISS arena.

(b) Program/Business Unit ISSO's assigned responsibility for application systems with a "high" value must attend classroom training on ISS issues and safeguards. This training must be attended, at APHIS expense, as soon as possible after being appointed.

(c) Program/Business Unit ISSO's assigned responsibility for application systems with a "moderate" or "low" value should attend classroom training on ISS issues and safeguards. At a minimum, these ISSO's must receive a thorough ISS orientation from their Unit ISSM.

(15) If responsible for a GSS or application system designated as "high" value, must submit to and successfully complete a background investigation to ensure their trustworthiness. Success ful completion of periodic re-investigations also is required.

h. Users of Information Resources will:

(1) Comply with this Directive and other ISS policies.

(2) Make every effort to avoid action/inaction that could jeopardize mission success, cooperator/customer rights, individual privacy, or APHIS reputation.

(3) Be responsible for IS resources they use. Each user will employ available and approved safeguards to protect those resources.

(4) Not attempt to break into any computer whether USDA, Federal. or private.

(5) Access or attempt to access only the data or resources specifically authorized and protect all data from unauthorized disclosure, alteration, or loss. Except for explicitly authorized cooperators and contractor personnel, only current APHIS employees are authorized access to sensitive (nonpublic) APHIS data. Cooperators and contractor personnel will be given access only to that nonpublic data needed to perform their approved duties.

(6) Protect computer equipment, media, and telecommunications from theft, fraud. misuse, loss, unauthorized modification, and unauthorized denial of use.

(7) Protect login ID and password(s) and use effective passwords that are not trivial, or easily guessed or deduced, or the same as their user identification. Users must not share, post, or otherwise jeopardize passwords, such as placing them in logon script files or programming them a function key. Each user is accountable for actions taken using their user identification.

(8) Change passwords frequently; at least every 45 days for network access and quarterly for e-mail and specific application systems. Users also must change passwords that validate their access to specific application systems as directed by the application owner.

(9) Use effective measures to guard against computer viruses and other malicious software in e-mail messages, downloaded software, etc.

(10) Log completely off workstations (or reset them to a screen that requires a password to reactive the workstation) any time they leave the workstation unattended (excepting genuine emergencies, such as fire).

(11) Protect dial-up telephone numbers and other telecommunications access keys against unauthorized disclosure.

(12) Protect sensitive (e.g., Privacy Act, etc.) input/output data from casual inspection or unauthorized retrieval.

(13) If using APHIS computer systems and networks for nonofficial purposes (when permitted by supervisors). will do so only on their own time and without interfering with official business.

(14) Refrain from using IS resources, including electronic mail and Internet/World Wide Web access for purposes that violate ethical standards, including harassment, threats, sending or accessing sexually explicit material, racially or ethnically demeaning material, gambling, chain letters, for-profit activities, political activities, promotion or solicitation of activities prohibited by law, etc.

(15) Understand and comply with license agreements for all software used. Except for IT employees, users must not install software on APHIS systems unless doing so is in support of an APHIS mission and is explicitly approved (in writing) by their supervisor.

(16) Practice good housekeeping with all electronic equipment, including keeping food, beverages, or other contaminants away from computers and data storage media.

(17) Report promptly to their supervisor and ISSO's/ISSM any actual or suspected violation of security.

(18) Stay abreast of ISS issues via education and awareness products distributed throughout APHIS.

(19) Sign a statement at the time of their initial computer user account issue and at least annually thereafter (at the time of their performance appraisal) acknowledging their ISS responsibilities and indicating their agreement to follow ISS policies and procedures.

(20) When transferring to a different position with APHIS or leaving the Agency altogether, remind their supervisor (prior to departure) of the impending event. Users must participate in a debriefing regarding their responsibilities to protect sensitive information, modification/revocation of system access privileges, requirement to turn in IS materials, etc.

i. USDA Contracting Officers and Procurement Officials will:

(1) Ensure that procurement and contract documents clearly state appropriate ISS terms and conditions.

(2) Assist Deputy Directors of Program Units and heads of major business units in ensuring that the provisions of this Directive are adhered to by contractor personnel.

(3) Assist the ISSPM in the investigation of alleged ISS violations by contractor personnel.

6. 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.

7. COMPLIANCE AND SANCTIONS

All employees who work with APHIS IS 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.

8. INQUIRIES

a. Direct inquiries or requests for changes to this Directive to the APHIS Information Systems Security Program Manager, 555 Howes Street, Fort Collins, CO 80521 or call 970-490-7814.

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

Chief Information Officer