

APHIS INFORMATION SYSTEMS SECURITY (ISS) PROGRAM

1. PURPOSE

- a. This Directive establishes the Information Systems Security (ISS) policy within APHIS. Management and coordination of security-related resources, assignment of collateral duty security personnel, and user responsibilities also are set forth.
- 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. REPLACEMENT HIGHLIGHTS

This Directive replaces APHIS Directive 3140.1, APHIS Security of Automatic Data Processing (ADP) Resources, dated 7/8/92.

3. AUTHORITY AND REFERENCES

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 100-235); Office of Management and Budget (OMB) Bulletin 90-08; Appendix III of OMB Circular A-130, 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, the United States Department of Agriculture (USDA) Office of Information Resources Management, 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 (PL 93579, 5 U.S.C. 552a).

4. SCOPE

- a. This Directive applies to all APHIS employees and contractors. It also applies to other Federal agencies, State and local governments, and authorized private organizations or individuals who use APHIS information systems to accomplish an APHIS business function. It includes anyone involved in the design, development, acquisition, installation, operation, maintenance, use, transfer, and disposal of APHIS information processing and telecommunications hardware and software.
- b. APHIS information systems (IS) covered by this policy include all computer hardware, software, and telecommunications that support APHIS business functions. This includes networks, program Unit and administrative data bases, office automation products (Smartsuite, Word Pro, Freelance Graphics, etc.), Lotus Notes and other electronic mail, and connections to the Internet.

5. POLICY

- a. Information is the lifeblood of APHIS operations and must be protected according to its value. The APHIS ISS program exists to help prevent damage to APHIS operations in much the same way that APHIS exists to prevent damage to American agriculture. Adherence to effective ISS practices is essential to our ability to continue our mission.
- b. APHIS has specific responsibilities to protect information resources and will comply with Federal and Departmental policies, regulations, and requirements on ISS as noted in Section 3. above.
- c. APHIS IS must be operated with a degree of control -- and a degree of risk -- consistent with the value of the information resources involved, including the value of the system infrastructure, the value of the data, and the value of the service provided. APHIS information resources must be protected against fraud, waste, unauthorized disclosure or use, theft, or abuse. Systems must not be installed or operated without a formal security review and official authorization from the Chief Information Officer (CIO), Deputy Administrator/Director, or head of major business offices, as appropriate. Using a risk-based approach, data must be given appropriate protection for confidentiality, accuracy and completeness, and timely availability. When feasible and cost effective, technological safeguards should be used to protect information resources instead of using labor intensive measures.
- d. To protect data and other information resources against unauthorized use, "least privilege" will be our mode of operation. This means that employees, cooperators, and contractor personnel will be provided access to and use of only those nonpublic information resources needed to accomplish their jobs. It also means

that systems will be installed, operated, and maintained with only those features or services actually needed to accomplish APHIS missions. The reason for this approach is simple: privileges and functions that do not exist in the first place cannot become points of security failure.

6. RESPONSIBILITIES

- a. The Chief Information Officer (CIO), Information Technology community (ITc), will:
- (1) Be the authorizing official for further ISS-related policies, directives, regulations, and guidelines. The CIO will issue the above as needed to address specific ISS issues and institute an effective ISS program consistent with the APHIS mission. The CIO derives his/her authority from the APHIS Administrator. Policies, directives, regulations, and guidelines issued by the CIO carry the same weight as if signed by the Administrator.
 - (2) Establish an appropriate body of senior ITc members to review and approve proposed ISS-related policies, directives, regulations, and guidelines.
 - (3) Appoint an Information Systems Security Program Manager (ISSPM) to manage the ISS program on behalf of the Administrator and provide the ISSPM with reasonable resources to create and maintain an effective program.
 - (4) Be personally responsible for ensuring an effective ISS program for General Support Systems (GSS) that serve APHISwide missions and functions and for those 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:
 - (a) Protect GSS with a predetermined minimum set of safeguards.
 - (b) Prevent successful attacks on APHIS IT resources or use of those resources by unauthorized personnel.

- (c) Ensure compliance with APHIS ISS policies and procedures regarding GSS and APHISwide applications. This includes such actions as periodically running special software routines to ensure that passwords are robust and changed frequently.
 - (d) 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.
 - (e) Enable monitoring of IS resources, with appropriate endorsement from the Internal Audit office (who will ensure compliance with the Electronic Communications Privacy Act), when there is credible evidence that specific personnel are misusing those resources.
 - (f) Ensure viable contingency plans for GSS and APHISwide application systems.
- (5) Ensure that ISSM's are appointed within ITc to implement the Agency's ISS program for GSS and submit the ISSM names to the APHIS ISSPM. He/she also will ensure those ISSM's are trained in ISS matters and formally evaluated on the performance of security-related duties.
 - (6) Promote general ISS awareness and training.
 - (7) Monitor overall compliance with Federal and Agency ISS policies.
- b. Deputy Administrators/Directors and heads of major business offices will:
- (1) Be personally responsible for ensuring an effective ISS program in their organization.
 - (2) Accredited (formally approve operation of) each major application system, unique to their area of operation, balancing operational requirements with prudent security measures. Doing so constitutes the decision authority for deciding what controls and safeguards are reasonable and appropriate for their business data. This authority may not be delegated.
 - (3) Appoint an Information Systems Security Manager (ISSM) to implement the APHIS ISS program within their organization and submit the ISSM's name to the APHIS ISSPM. ISSM's will work in close coordination with the APHIS ISSPM. ISSM's will further appoint (or obtain appointment

of) IS security officers (ISSO's) as needed to effectively manage and administer ISS endeavors.

- (4) Ensure their ISSM and ISSO's are evaluated formally on the performance of security-related duties.
- (5) Provide the necessary resources to ensure implementation of Agency security policy.
- (6) Promote ISS awareness and training.
- (7) Participate in processes to establish relative values for Unit data and to analyze risks for their business applications.
- (8) Develop supplemental ISS standards and policies -- beyond those established by the CIO for APHIS GSS and Agencywide applications -- as needed for their organization or unique application systems.
- (9) Establish and maintain viable IS contingency plans for their applications.
- (10) Monitor Unit compliance with APHIS ISS policy.

c. Employees, contractors, authorized cooperators, and other approved users of APHIS IS resources will:

- (1) Be individually and personally responsible for IS resources they use, and employ available and approved safeguards to protect those resources. Each user will be held personally accountable for actions taken using his/her user identification.
- (2) Access or attempt to access, only the data or resources specifically authorized and protect all data from unauthorized disclosure, alteration, or loss. Except for authorized cooperators and contractor personnel, only current APHIS employees will have 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.
- (3) Protect computer equipment, media, and telecommunications from theft, fraud, misuse, loss, unauthorized modification, and unauthorized denial of use.

- (4) Comply with this policy and other APHIS policies, directives, regulations, and guidelines developed in support of this policy.
- (5) 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.

7. EXCEPTIONS

There are no exceptions to this policy.

8. COMPLIANCE AND SANCTIONS

All personnel 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.

9. INQUIRIES

Direct inquiries or requests for changes to this policy to the APHIS ISSPM, 555 Howes Street, Fort Collins, CO 80521 or call 970-490-7814.

This Directive is available at www.aphis.usda.gov/library.

Bobby Acord
Acting Administrator