GIPSA INFORMATION SYSTEMS SECURITY (ISS) PROGRAM

1. PURPOSE

a. This Directive establishes the Information Systems Security (ISS) policy within GIPSA. 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 GIPSA 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

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).

3. SCOPE

a. This Directive applies to all GIPSA employees. It also applies to other Federal agencies, State and local governments, and authorized private organizations or individuals who use GIPSA information systems to

accomplish a GIPSA business function. It includes anyone involved in the design, development, acquisition, installation, operation, maintenance, use, transfer, and disposal of GIPSA information processing and telecommunications hardware and software.

b. GIPSA information systems (IS) covered by this policy include all government owned computer hardware, software, and telecommunications that support GIPSA business functions. This includes networks, program Unit and administrative data bases, office automation products (Microsoft Office, WordPerfect Suite) GroupWise and other electronic mail, and connections to the Internet.

4. POLICY

a. Information is the lifeblood of GIPSA operations and must be protected according to its value. The GIPSA ISS program exists to help protect GIPSA operations in much the same way that GIPSA exists to protect American agriculture. Adherence to effective ISS practices is essential to our ability to continue our mission.

b. GIPSA has specific responsibilities to protect information resources and will comply with Federal and Departmental policies, regulations, and requirements on ISS as noted in Section 2. above.

c. GIPSA 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. GIPSA 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 Branch/Field offices, as appropriate. CIO approval is needed at the planning stage of all new systems. Using a risk-based approach, data must be given appropriate protection for confidentiality, accuracy 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 GIPSA 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.

5. RESPONSIBILITIES

a. The Chief Information Officer (CIO) 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 GIPSA mission. The CIO derives his/her authority from the GIPSA 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 IT 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.

(4) Be responsible for ensuring an effective ISS program for General Support Systems (GSS) that serve GIPSA-wide 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 attacks on GIPSA IT resources or use of those resources by unauthorized personnel.

(c) Ensure compliance with GIPSA ISS policies and procedures regarding GSS and GIPSA wide applications. This includes promoting such actions as the periodic running of special software routines to ensure that passwords are robust and changed frequently.

(d) Periodically oversee the review of the status of GSS to ensure that changes have not occurred that negatively affect

security. This will be accomplished both manually (peer/management reviews of proposed changes) and by using specialized software tools.

(e) Approve the monitoring of IS resources, with appropriate endorsement from APHIS Human Resources Representative (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 GIPSA-wide application systems.

(5) Ensure that Security Representatives are appointed within GIPSA field locations to implement the Agency's ISS program for GSS and submit the Security Representative names to the GIPSA ISSPM. He/she also will ensure those Security Representatives are trained in ISS matters.

(6) Promote general ISS awareness and training.

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

b. <u>Deputy Administrators/Directors and heads of branch/field offices will:</u>

(1) Be responsible for ensuring an effective ISS program in their organization.

(2) Accredit (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.

(3) Notify System Administrators (through the ISSPM) of all new and departing employees. Procedures for accomplishing this task can be found on “InGIPSA” under the Information Systems Security section.

(4) Appoint a Security Representative to implement the GIPSA ISS program within their organization (Field locations).

(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) Identify to the Agency ISSPM any unique additional standards and policies that may need to be incorporated.

(9) Establish and maintain documented viable IS contingency plans for their applications.

(10) Monitor Unit compliance with GIPSA ISS policy.

c. The ISSPM will:

(1) Be the lead ISS specialist for GIPSA, 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 a GIPSA 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) 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 GIPSA to the USDA ISSPM and ISS specialists in other Federal organizations. The ISSPM will establish and maintain working relationships with GIPSA Security Representatives, and GIPSA employees to exchange information and ideas about ISS.

(5) Ensure that Security Representatives 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 Security Representatives 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 Security Representatives. 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. All security related issues will be tracked and reported monthly to the CIO.

(13) Attend 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) Successfully complete a background investigation to ensure trustworthiness. Successful completion of periodic re-investigation also is required.

d. <u>Security Representatives will:</u>

(1) Be the lead ISS specialists for their Field Offices, 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.

(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/GIPSA policies.

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

(4) 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.

(5) Participate in risk analyses and disaster preparedness planning for field applications, assisting ISSPM in determining needed safeguards and acceptable levels of risk.

(6) Administer/monitor 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 organization, including functional managers, and users. They will answer questions regarding ISS policies and procedures.

(8) Attend classroom training on ISS issues and safeguards. This training is required to start as soon as possible after being appointed. Field Office Security Representatives should attend 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.

(9) Are required to report to the ISSPM, in writing, all security incidences in their area of responsibility within 24 hours of the occurrence.

e. <u>Employees, authorized cooperators, and other approved users of GIPSA IS resources will:</u>

(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 GIPSA employees will have access to

sensitive (nonpublic) GIPSA 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.

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

(5) Users will be issued a copy of ISS policies and will be required to sign a statement at the time of their initial computer user account issue and at least annually thereafter (at the time of annual security training) acknowledging their ISS responsibilities and indicating their agreement to follow ISS policies and procedures.

6. EXCEPTIONS

There are no exceptions to this policy.

7. COMPLIANCE AND SANCTIONS

All federal personnel who work with GIPSA IS resources are individually and personally responsible for applying the appropriate security measures and for complying with Federal, USDA, and GIPSA 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

Direct inquiries or requests for changes to this policy to the GIPSA ISSPM at (202) 690-0044.

Copies of current GISPA directives can be accessed on the Intranet site, "InGIPSA" and on the Internet at **www.aphis.usda.gov/library**.

/s/ David R. Shipman
Acting Administrator
GIPSA