

GIPSA INTERNET USE AND SECURITY POLICY

1. PURPOSE

This Directive establishes:

- a. The policy, foundation, rules, and guidelines for the use, security, and privacy of Internet access, including the World Wide Web (WWW).
- b. The requirement for adequate protection to protect GIPSA data and systems accessible via the Internet from intrusion, tampering, unauthorized modification, and service disruption.

2. AUTHORITIES/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 (PL) 100-235); the Computer Fraud and Abuse Act (18 U.S.C. Sec. 1030 [1993]); Office of Management and Budget (OMB) Circular No. A-123, Management Accountability and Control; Appendix III of OMB Circular No. A-130, Management of Federal Information Resources; FED-STD-1037A, "An Electronic Means for Communicating Information;" and the Electronic Communications Privacy Act (18 U.S.C. 2701). Taken together, these documents and others not cited prescribe establishing and maintaining a comprehensive Information Systems Security (ISS) program and set standards for using information systems, including electronic mail. Additionally, the United States Department of Agriculture (USDA) Office of Information Resources Management, Department Regulation 3140-1, USDA IRM Security Policy, applies, as do other USDA policies and requirements specifically related to e-mail Federal requirements related to protecting sensitive information, such as the Privacy Act of 1974 (PL 93-579, 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 and

electronic messaging capabilities to accomplish an GIPSA business function. All of the aforementioned are considered users and are included wherever the words “user” or “users” are referenced within this Directive.

- b. GIPSA information systems (IS) covered by this Directive include all computer hardware software, and telecommunications that support GIPSA connections to the Internet. This includes those systems owned, operated, or funded by GIPSA or those supplied for GIPSA use by contractors.

4. POLICY

- a. GIPSA provides links to the Internet to enhance business capabilities. Users are encouraged to use the Internet as a valuable source of information in their work and as a tool to disseminate information about GIPSA programs and activities. As with other GIPSA assets, however, Internet access and use must be protected against waste, fraud, unauthorized use, and/or abuse. Use of the Internet requires responsible judgment, supervisory discretion, and compliance with applicable laws. Use of GIPSA access to the Internet and other information technology in ways that violate ethical standards, deprive Americans of rightful value for their tax dollars, or embarrass this Agency will not be tolerated.
- b. Confidentiality must be assured for sensitive data. Information exempted from disclosure under the Freedom of Information Act (Public Law 93-502), prohibited from disclosure by the Privacy Act (Public Law 93-579), or that is proprietary to a customer or cooperator will not be placed on publicly-accessible Internet sites. Sensitive information must not be transmitted over the Internet network without confidentiality controls (e.g., encryption).
- c. GIPSA reserves the right to either randomly or systematically monitor use of Agency Internet connections and traffic. GIPSA users have no right to expect privacy in their use of GIPSA access to the Internet.
- d. Users are permitted limited personal use of Internet access on an occasional basis, provided that such use involves minimal expense to the government, doesn't interfere with official business, and take place during the user's personal time. Users who have doubts about the meaning of “limited” or “occasional” should consult their supervisor. Official government business always takes precedence over personal use. Authorized purposes may include limited personal use, with Supervisor approval, and it is determined that such communications:
 - (1) Do not adversely affect the performance of official duties by the GIPSA employee or the GIPSA employees organization;

- (2) Are of reasonable duration and frequency, and made during the GIPSA employee's personal time such as after duty hours or lunch periods;
- (3) Serve a legitimate public interest (such as educating the USDA employee on the use of the telecommunications system; enhancing the professional skills of the USDA employee; job searching in response to Federal Government downsizing);
- (4) Do not put Federal Government telecommunications systems to uses that would reflect adversely on USDA or the Agency (such as uses involving pornography; playing on-line games; for purposes of private business; chain letters; unofficial advertising, soliciting or selling, violations of statute or regulation; inappropriately handled sensitive information; and other uses that are incompatible with public service);
- (5) Do not overburden the telecommunications system (such as chat programs and group mailings), and create no significant additional cost to USDA or to the Agency; and
- (6) Follow the policy of the Internet Activities Board (IAB) as stated in RFC 1087.
- (7) Must not be harassing, libelous, or disruptive to others while connected to the Internet.
- (8) Must not transmit personal data or unauthorized government-owned data across the Internet.
- (9) Must obey all copyright laws.
- (10) Must not access from government computers via the Internet any obscene written or graphic material or pornography.
- (11) Must not send threatening (violent), racially, or sexually harassing messages or files.
- (12) Must not attempt to break into any computer whether USDA, federal, or private.
- (13) Must not be used for private or personal business.
- (14) Must not introduce computer viruses, worms, or Trojan horses.
- (15) Software will not be downloaded from the Internet if:

- (a) There is a condition of the downloading that commits GIPSA to purchase the software or incur other expenses and written approval has not been obtained.
 - (b) The software is not approved for use on GIPSA microcomputers and LAN's.
 - (c) The software is not related to official government business.
 - (d) Items such as "screen savers" and sound/music files will not be downloaded from the Internet and installed on GIPSA microcomputers. These items are strictly prohibited.
 - (e) The Internet will not be used for personal audio or video broadcasts unless the use is GIPSA-sponsored training/meeting/conferences.
- (16) GIPSA's CIO has the right to expand upon "inappropriate" uses at any time.
- e. GIPSA will comply with Federal and Departmental policies, regulations, and requirements on Internet use and information systems security.
 - f. GIPSA Program/Business Units that use the Internet must adhere to guidance stated in USDA DR 3140-1, USDA IRM Security Policy. Units also must follow the guidance in USDA DR 3300-1, Telecommunications, and report to USDA OIRM the information requested in Appendix I, Section 4.

5. RESPONSIBILITIES

- a. The Chief Information Officer will:
 - (1) Approve and ensure implementation of Internet security policies for the protection of GIPSA information resources.
 - (2) Have the final say regarding adequacy of security measures and accredit general support systems (GSS) used as gateways to the Internet, in accordance with Federal and USDA requirements.
 - (3) Ensure funding, implementation, and maintenance of computer firewalls and similar protective features for Internet access points.
 - (4) Ensure that contingency plans for Internet access are developed, tested, and maintained in order to:

- (a) Minimize the damage and disruption caused by undesirable events.
 - (b) Provide for the continued performance of essential systems functions and services.
 - (5) Ensure that procedures are in place to obtain consent for monitoring of Internet usage, set forth in section 6 below.
 - (6) Ensure that system administrators are adequately trained and administrative procedures are developed, implemented, and monitored.
 - (7) Establish the Information Systems Security Program Manager (ISSPM) as an integral part of policies, modifications, and enhancements to GIPSA use of the Internet.
- b. Deputy Administrators/Directors of Program Units and heads of Branch/Field offices will:
- (1) Be responsible for protection of GIPSA resources under their control that are available via the Internet. Through their Information Systems Security Program Manager and Security Representative, manage the provisions of this Directive throughout their organization.
 - (2) Ensure that GIPSA users of the Internet are knowledgeable about the provisions of this Directive and that Field Security Representatives have the training and authority to promptly identify, investigate, and help rectify any violations of this Directive.
 - (3) Enforce policies and procedures to govern unauthorized Internet use, including access or downloading of offensive or illegal material.
 - (4) Ensure that procedures are in place to obtain (expressed consent) to monitoring, as defined in section 6 below, and that records of (expressed consent) are maintained by the ISSPM or Field Security Representative.
- c. The ISSPM will:
- (1) Be knowledgeable of and follow through on responsibilities identified in USDA ISS policies and procedures.

- (2) Disseminate information concerning Internet security developments and threats.
- (3) Participate in developing Internet access policies that define those services that will be allowed or explicitly denied, how services will be used, the conditions for exception to this Directive, and rules used to design and implement firewall access policies.
- (4) Ensure that periodic tests are done of firewalls that guard Internet access points, including penetration tests, information systems security risk assessments, security evaluations, and internal control reviews of operational GIPSA Internet gateways and facilities.
- (5) Ensure that system audit trails are developed, installed, maintained, and regularly reviewed for unusual system activity.
- (6) Be involved in all investigations into misuse of Internet access.
- (7) Ensure that a security plan has been prepared or updated to protect Internet access that systems are accredited in accordance with Federal and USDA requirements.

d. Field Office Security Representatives will:

- (1) Administer this Directive and monitor its compliance in their Unit.
- (2) Ensure that training exists to make users aware of their responsibilities for use of GIPSA Internet connections.
- (3) Ensure that system audit trails are developed, installed, maintained, and regularly reviewed for unusual system activity.
- (4) Assist in promptly identifying, investigating, and helping to rectify violations of this Directive.
- (5) Ensure new employees understand their responsibilities as they pertain to GIPSA Internet usage and sign (in ink) a simple statement reflecting this understanding.

e. GIPSA users will:

- (1) Comply with this Directive and other ISS policies.
- (2) Be responsible for proper use of the Internet via GIPSA systems.

- (3) Remain alert to the high potential for threat from the Internet and the steps they must take to protect information resources from Internet-based attacks, including break-in, file tampering, and service disruptions.
Internet related risks can be considerable since it consists of many worldwide, independent networks and operates without a central authority to regulate usage.
- (4) Remember that the Internet is an uncontrolled environment and that information found there may be outdated, inaccurate, or even deliberately misleading. Internet information should be considered suspect until confirmed by another source.
- (5) Protect sensitive and proprietary information. Users must:
 - (a) Not send sensitive information over the Internet without appropriate confidentiality protection (e.g., encryption).
 - (b) Protect customer/cooperator proprietary information in accordance with the conditions under which it is provided.
 - (c) Obey all copyright laws. If copyrighted material is posted on an GIPSA Internet site, a record of the copyright holder's permission to do so must be maintained.
- (6) Refrain from using Internet/WorldWide Web access for purposes that violate ethical standards. This includes harassment, accessing or sending sexually explicit material, racially or ethnically demeaning material, gambling, threatening (violent) material, chain letters, for-profit activities, political activities, promotion or solicitation of activities prohibited by law, and so forth.
- (7) Not attempt to break into any computer whether USDA, Federal, or private.
- (8) Not post information on the Internet that could embarrass GIPSA.
 - (a) Information posted on GIPSA websites must be cleared by supervisors.
 - (b) Posting information about GIPSA or the Agency's activities should be a collaborative effort. Posting information that impacts other Program/Business Units or Agency activities shouldn't be done without prior consultation and coordination with GIPSA's Webmaster.

- (c) Information made available on GIPSA websites should be accurate, relevant, up-to-date, and professionally presented.
 - (9) Be aware that they leave an electronic trail of Internet sites they visit.
 - (10) Logoff/logout of their Internet sessions whenever they leave their workstations for an extended period, including meetings, lunch breaks and at the end of the day. (In a genuine emergency, users are not required to logoff/logout; protection of human life is paramount.)
 - (11) Report security problems to their Supervisor or ISSPM.
- f. Internet system managers/administrators will:
- (1) Be responsible for supporting actions that help ensure compliance with this Directive, including ensuring that appropriate system security features are activated on Internet gateways for which they are responsible and that system “patches” are kept current.
 - (2) Maintain records (audit trails) of unauthorized access (suspected or actual) access to GIPSA information resources and review them at least every three days. While we should avoid diluting the efforts of system administrators or ISS personnel by routinely reporting that security measures are in fact working (unauthorized access attempts thwarted), we need to maintain proper vigilance and be prepared to respond quickly to genuine threats. Verified penetrations of GIPSA ISS safeguards will be reported according to established incident handling procedures.
 - (3) Provide the ISSPM and Security Representatives with audit trails, system logs, and other information to assist with enforcement of this Directive and investigations into violations.
- g. USDA Contracting Officers and Procurement Officials will:
- (1) Ensure that procurement and contract documents clearly state the terms and conditions of this Directive in the Statement of Work (SOW), as appropriate.

6. INTERNET SYSTEM ADMINISTRATION

- a. This Directive establishes GIPSA “Rules of the System” for GIPSA access to the Internet, as defined in Office of Management and Budget (OMB) Circular A-130.
- b. Computer firewalls will be installed and maintained between the GIPSA network and Internet connections. Except for servers that contain only publicly releasable data (both inherently and via links to other sites/systems), all systems will be configured to operate behind the firewalls.
- c. All GIPSA Program/Business Units that operate or plan to operate World Wide Web sites or a gateway to the Internet are responsible for ensuring adequate protection, both for the connections and the website contents. A risk assessment must be conducted and, if appropriate, a security plan and accreditation completed.
- d. Units must coordinate Internet website implementation with the GIPSA CIO to ensure their operation will not jeopardize the security of the overall GIPSA information systems architecture.
- e. Commercially-available penetration testing software will be run at least twice per year against Web servers and other systems connected directly to the Internet (not behind a firewall). The purpose of penetration testing is to check for technical weaknesses that could compromise security.
- f. Executable files (computer programs) downloaded from the Internet must be scanned for the presence of computer viruses or other malicious code before use. When possible, download software onto removable media (not to the system hard disk) for scanning. (If the software won’t fit on available removable media, then the only option is the hard disk.) Once the user is reasonably certain that the downloaded software does not contain malicious code, it can be placed on the hard drive and used. Of course, copyright licensing requirements and software use restrictions must be followed.
- g. Required warnings and notices for monitoring Internet usage.
 - (1) All systems connected to the Internet, including GIPSA websites, must display the following (or similar) warning notice: “All USDA/GIPSA telecommunications and automated information systems and related equipment are for the communication, transmission, processing, and storage of U. S. Government information. These systems are subject to monitoring to ensure proper functioning, and to protect against improper or

unauthorized use or access, and to verify the presence or performance of applicable security features and procedures, and for like purposes. Such monitoring may result in the acquisition, recording and analysis of data being communicated, transmitted, processed or stored in this system by any user.

If monitoring reveals criminal activity, such evidence may be reported to law enforcement personnel. ANYONE USING A USDA/GIPSA SYSTEM OR SYSTEM ACCESSED THROUGH A USDA/GIPSA SYSTEM CONSENTS TO SUCH MONITORING.”

- (2) GIPSA Program/Business Units will ensure that each user signs a consent statement before using GIPSA access to the Internet. By signing the statement, users accept responsibility for use and consent to monitoring according to the conditions of this Directive. This statement may be a GIPSA wide form or one specially developed by the Unit.
- h. System administrators will review logs and other audit trails at least every three days to search for penetrations or other security breaches. Security incidents will be reported immediately to the GIPSA Information Systems Security Program Manager (ISSPM).

7. EXCEPTIONS

Each GIPSA Program/Business Unit must meet the requirements of this Directive. Exceptions that reduce the requirements of this Directive may be approved only in writing by the CIO or the GIPSA Administrator.

8. COMPLIANCE AND SANCTIONS

- a. All GIPSA employees using Internet connections are individually and personally responsible for complying with Federal, USDA, and GIPSA policies on this subject, as well as with the procedures and practices developed in support of this Directive. Willful failure to comply may result in punishment, including dismissal, under the Computer Fraud and Abuse Act and other appropriate Federal statutes.
- b. Anyone suspecting misuse or attempted misuse of GIPSA Internet services or Agency-owned or -operated systems should report it to their supervisor, or to their Security Representative or the GIPSA Information Systems Security Program Manager (ISSPM). GIPSA employees can send anonymous letters to any of the above.

9. INQUIRIES

- a. Direct inquiries or requests for change to this Directive to the GIPSA ISSPM, (202) 690-0044.
- b. 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