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

Directive APHIS 3140.3 5/26/2000

APHIS 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 APHIS data and systems accessible via the Internet from intrusion, tampering, unauthorized modification, and service disruption.

2. AUTHORITIES/REFERENCES

Foundation for the APHIS Information Systems Security (ISS) program is Directive 3140.1, dated 9/15/99. 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 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 and electronic messaging capabilities 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 connections to the Internet. This includes those systems owned, operated, or funded by APHIS or those supplied for APHIS use by contractors.

4. POLICY

a. APHIS 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 APHIS programs and activities. As with other APHIS 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 APHIS 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. APHIS reserves the right to either randomly or systematically monitor use of Agency Internet connections and traffic. APHIS users have no right to expect privacy in their use of APHIS 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.

e. APHIS will comply with Federal and Departmental policies, regulations, and requirements on Internet use and information systems security. APHIS 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, Information Technology community (ITc) will:

(1) Approve and ensure implementation of Internet security policies for the protection of APHIS 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 APHIS use of the Internet.

b. Deputy Administrators/Directors of Program Units and heads of major business offices will:

(1) Be responsible for protection of APHIS resources under their control that are available via the Internet. Through their Information Systems Security Managers (ISSM's) and other organizational security structure, manage the provisions of this Directive throughout their organization.

(2) Ensure that Unit presence (i.e., websites) are coordinated in advance with Technology Resources Management (TRM) to prevent compromise of overall network security, in accordance with section 6., below.

(3) Ensure that APHIS users of the Internet are knowledgeable about the provisions of this Directive and that Unit ISSM's have the training and

authority to promptly identify, investigate, and help rectify any violations of this Directive.

(4) Enforce policies and procedures to govern unauthorized Internet use, including access or downloading of offensive or illegal material.

(5) 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 Unit ISSM or subordinate Information Systems Security Officers (ISSO's).

(6) Ensure that Unit ISSM's have the training and authority to promptly identify, investigate and rectify any violations of this Directive.

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 APHIS 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. Unit Information Systems Security Managers (ISSM's) 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 APHIS 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 rectify violations of this Directive.

(5) Obtain and file (or oversee those actions) records of expressed consent for all users in their area of responsibility, including contractor personnel, in accordance with section 5., above.

e. APHIS users will:

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

(2) Be responsible for proper use of the Internet via APHIS 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 APHIS 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, 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 APHIS.

(a) Information posted on APHIS websites must be cleared by supervisors.

(b) Posting information about APHIS 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.

(c) Information made available on APHIS 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, fire drills, 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 violations of this Directive to the ISSO, ISSM, or supervisor.

f. <u>Internet system managers/administrators</u> 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 APHIS 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 APHIS ISS safeguards will be reported according to established incident handling procedures.

(3) Provide the ISSPM and Unit ISSMs 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, as appropriate.

(2) Assist the ISSPM in the investigation of alleged violations of this Directive by contractor personnel.

6. INTERNET SYSTEM ADMINISTRATION

a. This Directive establishes APHIS "Rules of the System" for APHIS 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 APHIS 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 APHIS 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 APHIS CIO (Technology Resources Management -- TRM) to ensure their operation will not jeopardize the security of the overall APHIS 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. TRM can advise Units about such testing.

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, in accordance with APHIS Directive 3120.1.

g. Required warnings and notices for monitoring Internet usage.

(1) All systems connected to the Internet, including APHIS websites, must display the following (or similar) warning notice: "All USDA/APHIS 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/APHIS SYSTEM OR SYSTEM ACCESSED THROUGH A USDA/APHIS SYSTEM CONSENTS TO SUCH MONITORING."

(2) APHIS Program/Business Units will ensure that each user signs a consent statement before using APHIS 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 an APHISwide form or one specially developed by the Unit.

h. Supervisors or system administrators who suspect misuse of APHIS Internet services may request an investigation through the APHIS Resource Management Systems and Evaluation Staff (RMSES), who will coordinate with Human Resources and the ISSPM. Supervisors may request an investigation when there are reasonable grounds for suspecting that the investigation will produce evidence that an employee has engaged in work-related misconduct. Approved investigations will be documented and documentation retained by RMSES, in coordination with the ISSPM. Disciplinary measures will be decided by the supervisor, in coordination with RMSES and Human Resources.

i. System administrators and/or Information Systems Security Officers (ISSO's) 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 their Unit Information Systems Security Manager (ISSM) and the APHIS Information Systems Security Program Manager (ISSPM).

7. EXCEPTIONS

a. Each APHIS 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 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.

8. COMPLIANCE AND SANCTIONS

a. All users of APHIS Internet connections are individually and personally responsible for complying with Federal, USDA, and APHIS 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 APHIS Internet services or Agency-owned or -operated systems should report it to their supervisor, or to their Program/Business Unit Information Systems Security Manager (ISSM) or the APHIS Information Systems Security Program Manager (ISSPM).

9. INQUIRIES

a. Direct inquiries or requests for change to to this Directive to the APHIS ISSPM, 555 South 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***.

APHIS Chief Information Officer