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

Directive

APHIS 3140.2 **2/28/2013**

APHIS ELECTRONIC MAIL USE, SECURITY, AND PRIVACY POLICY

1. PURPOSE

This Directive sets forth APHIS's policy on electronic messaging. Specifically, this Directive addresses rules relating to recordkeeping of email messages, email deletion, and the appropriate use of the APHIS Enterprise Messaging Service (EMS).

2. REPLACEMENT HIGHLIGHTS

This Directive replaces APHIS Directive 3140.2, APHIS Electronic Mail Security and Privacy Policy, dated 5/26/00.

3. AUTHORITY

Applicable national policy requirements regarding Information Systems Security (ISS) are stated primarily in the Computer Security Act of 1987 (Public Law (PL) 100-235); 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; and FED-STD-1037A, An Electronic Means for Communicating Information.

Use of EMS must comply with Federal laws and regulations. Applicable laws and regulations include, but are not limited to:

a. 5 U.S.C. § 552, the Freedom of Information Act.
http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm

b. 5 U.S.C. § 552a, the Privacy Act.
http://www.justice.gov/opcl/privstat.htm

c. 44 U.S.C. § 2901, *et seq.*, the Federal Records Act.
http://www.archives.gov/about/laws/

d. 44 U.S.C. § 3301, the Federal Records Disposal Act.
http://www.archives.gov/about/laws/disposal-of-records.html

e. 17 U.S.C. § 101 *et seq.*, Copyright Act of 1976.
http://www.copyright.gov/title17/92chap1.html

f. 18 U.S.C. § 1030 [1993] Public Law 99-474, The Computer Fraud and Abuse Act of 1986.
http://www.panix.com/~eck/computer-fraud-act.html

g. 18 U.S.C. 2701, the Electronic Communications Privacy Act.
http://www.cybercrime.gov/usc2701.htm

h. 18 U.S.C. § 1905, which prohibits disclosure of proprietary information and certain other confidential information.
http://www.justice.gov/atr/public/divisionmanual/

i. 41 U.S.C. § 423(a), which prohibits unauthorized disclosure of certain procurement-sensitive information, including proprietary or source selection information.
http://uscode.house.gov/download/pls/41C7.txt

j. 5 CFR Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch, particularly subpart G, which deals with misuse of position.
http://www.usoge.gov/laws_regs/regulations/5cfr2635.aspx

k. 36 CFR Parts 1220, 1222, 1228 and 1234, National Archives and Records Administration regulations on management of email messages.
http://www.archives.gov/about/regulations/subchapter/b.html

l. 5 CFR part 735, Employee Responsibilities and Conduct.
http://www.access.gpo.gov/nara/cfr/waisidx_00/5cfr735_00.html

m. Guidelines on Religious Exercise and Religious Expression in the Federal Workplace, dated August 14, 1997.
http://clinton2.nara.gov/WH/New/html/19970819-3275.html

n. Section 508: Rehabilitation Act of 1973 (29 U.S.C. 794d).
http://www.section508.gov/index.cfm?fuseAction=1998Amend

Taken together, these documents and others not cited, prescribe establishing and maintaining a comprehensive ISS program and set standards for using information systems, including electronic mail. Additionally, the United States Department of Agriculture (USDA) Department Regulation 3140-1, USDA Information System Security Policy, applies, as do other USDA policies and requirements specifically related to email, and Federal requirements related to protecting sensitive information, such as the Privacy Act of 1974 (PL 93-579, 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 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 EMS is a set of messaging services consisting of an international network of centrally administered and managed electronic mail servers, electronic messaging gateways, message switches, and malware protection applications, making up APHIS’ single, Agencywide electronic mail system. EMS is a shared resource that has been procured, implemented, and is maintained to conduct the Agency's business. The National Archives and Records Administration (NARA) has issued Governmentwide regulations governing the way agencies manage email messages (36 CFR Parts 1220, 1222, 1228, and 1234). The regulations direct agencies to issue implementing guidance.

5. DEFINITIONS

a. Authorized Users. Associates of APHIS and other Government organizations who are supported by APHIS, and those contractors, consultants, or other third parties who are specifically granted access for the conducting of business on behalf of or with APHIS or other Government organizations supported by APHIS. Contractors, consultants, or other third party personnel meeting these requirements will be authorized use only if sponsored by an APHIS program.

b. Classified Information. Any material that includes national security information, restricted data, and formerly restricted data.

c. Confidentiality. Authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

d. Denial of Services. Action resulting from interference with official APHIS or Federal Government business by overloading resources, or blocking access to any resources. Examples of such interference include:

(1) Mass mailings, the sending of any "broadcast email messages," or any other similar activity that could cause congestion and disruption of networks and systems or interfere with the work of others.

(2) Sending chain letters, either by initiating or forwarding them to others. This is an abuse of resources and is forbidden. Any non-business correspondence that requests the recipient to forward it on to others is a chain letter. Forwarding any copies of hoaxes relating to email viruses, jokes, cookie recipes, and get-rich-quick schemes falls into this category and also is an abuse of resources.

(3) Sending large attachments that are not business-related. This refers to the ill-advised practice of emailing friends and co-workers attachments of holiday or special event greetings, or an animated cartoon, music, or video clip.

e. Email Account. An account established between an authorized user and EMS for the purpose of creating, sending, and receiving electronic mail messages. Email accounts require a login and password and also may be associated with access to other databases, in addition to email and calendaring services.

f. Email File. The physical email data file consisting of an Inbox, Sent, Trash, and other user-created folders for use in the creation, sending, receiving, and organization of electronic mail messages. This file also may provide calendaring functionality and maintain related information such as meetings, appointments, and reminders. An email account is required to access an email file.

g. Malicious Use. Use designed to embarrass, harm, or otherwise cause others to suffer. Denial of service is one type of malicious use.

h. Message Encryption. Use of software to render a message unreadable to everyone except the sender and its intended recipient.

i. Official Records. All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law, or in connection with the transaction of public business, and preserved, as appropriate, for preservation by that agency, or its legitimate successor, as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government, or because of the informational value of the data in them (44 U.S.C. 3301).

Any document that would be classified as a record if it were issued in paper form is a record if issued via email. Normally, only the originator copy is the record copy.

j. Prohibited Use. Use which is forbidden by or fails to comply with Federal laws, USDA regulations, or APHIS directives.

k. Sensitive Information. Information protected by the Privacy Act. Information that would be withheld from disclosure under the Freedom of Information Act (FOIA), procurement-sensitive information, proprietary information of APHIS service partners and suppliers, or other information deemed sensitive by the Agency.

l. Signature Block. The part of an email message that contains the sender's contact information.

m. System Administrator/Manager. The associate or support contractor who has been designated as having the responsibility for ensuring the continued operation, maintenance, availability, and accessibility of assigned system(s).

n. Transitory Material. Documents of short-term interest having no documentary or evidential value and which normally need not be kept more than 60 days.

Examples of transitory material are:

(1) Routine requests for information or publications and copies of replies that require no administrative action, no directive decision, and no special compilation or research for reply. FOIA requests are not considered transitory material.

(2) Originating office copies of letters of transmittal that do not add any information to that contained in the transmitted material, and the receiving office copy, filed separately from transmitted material.

(3) Quasi-official notices, including memoranda and other records that do not serve as the basis of official actions, such as notices of holidays or charity and welfare fund appeals, bond campaigns, and similar correspondence.

(4) Copies of documents issued to multiple recipients. Usually, copies of documents received by recipients of email are copies, not records, and should be thrown away as soon as they are not needed for reference. However, multiple copies of the same document may meet the definition of records if any copy is used by the recipient to transact Agency business. Copies that have such record status are usually filed in different record-keeping systems and are used for different purposes.

(5) Drafts circulated for comment. In general, draft copies are not records. However, draft documents or working papers that propose or evaluate high-level policies or decisions and provide unique information that contribute to the understanding of major decisions, must be preserved as a Federal record, whether they are in printed or email form.

6. POLICY

a. **Appropriate Use of EMS.**

(1) When using EMS, users are doing so as associates and/or representatives of APHIS and the Federal Government. Users must at all times seek to promote a positive image for APHIS and the Federal Government. They must be careful about how they represent themselves, given that what they say or do could be interpreted as APHIS or Federal Government opinion. Users must be aware that their conduct could reflect on the reputation of

APHIS, the Federal Government, and its associates. At all times, users must use font types and enhancements judiciously in emails.

(2) All users have an obligation to be aware of computer security and privacy concerns and to guard against computer viruses. Users who load files brought in from outside sources on Federal Government computers, then send the files as email attachments, present a heightened risk in this area, unless users first virus-scan all outgoing attachments before the email is sent.

(3) Users must always exercise caution when addressing email messages, as there are users of the Agency's services who are not Agency associates. This will help to avoid inadvertently sending a message meant for APHIS associates and authorized users to outsiders.

(4) Users must exercise caution in conveying sensitive or non-public information. Such information will be treated with the same care as paper documents conveying the same information.

(5) APHIS email resources exist to enhance business capabilities and must be protected against waste, fraud, unauthorized use, or abuse. Use of electronic messaging in ways that violate ethical standards, deprive Americans of rightful value for their tax dollars, or embarrass this Agency will not be tolerated.

(6) APHIS is committed to protecting sensitive information from accidental or unauthorized release, transmission, display, or disclosure via electronic messaging.

(7) Sensitive information includes key Agency information (Privacy Act, contractual, etc.) as well as proprietary information of customers and cooperators. It is the responsibility of each APHIS Program/Business Unit to ensure that users are confident that their information is protected and that such confidence is justified.

(8) All email messages transmitted to or from or stored on APHIS computers are the property of APHIS. APHIS reserves the right to either randomly or systematically scan email for improper materials. APHIS users have no right to expect their messages to remain private. Users who wish to ensure privacy of their communication should use means other than APHIS email.

(9) APHIS employees are permitted limited personal use of email on an occasional basis, provided that the use involves minimal expense to the Government, does not interfere with official business, and takes place during personal time. Employees who have doubts about the meaning of “limited” or “occasional” should consult their supervisor. Employees must

exercise good judgment in all use of email. Official Government business always takes precedence over personal use.

(10) APHIS will comply with Federal and Departmental policies, regulations, and requirements on email use and ISS. Additionally, users have an obligation to be aware of computer security and privacy concerns and to guard against computer viruses.

(11) APHIS email messages will be treated the same way as paper documents which serve the same purpose. Email is no more and no less important than other information used to transact business. Authorized users must apply the same decision-making process to email for record maintenance and disposition that they apply to other documentary materials, regardless of the media used to create them. Email may be archived to another server, copied to the user's workstation, or a printed copy may be made.

(12) APHIS email signature blocks must include and only include the following information:

(a) Name.

(b) Job Title.

(c) Organization.

(d) Office address.

(e) Phone number(s).

(f) Email address.

NOTE: A signature block is typically located at the end of an email message.

(13) When necessary, the confidentiality statement below will be included at the end of the email messages.

CONFIDENTIALITY NOTE: The preceding email message contains information that may be confidential, proprietary, or legally privileged, and may constitute non-public information. This message is intended to be conveyed only to the intended named recipient(s). If you are not an intended recipient of this message, do not read it; instead, please advise the sender by reply email, and delete this message and any attachments. Unauthorized individuals or entities are not permitted access to this information. Any disclosure, copying, distribution or taking any action in

reliance on the contents of this information, except its delivery to the sender, is strictly prohibited and may be unlawful.

b. **Inappropriate Use of EMS**.

(1) The EMS is not a secure system in the context of providing adequate protection for classified data or information. Users must never convey classified data or information in any messages sent over the APHIS electronic mail system.

(2) The use of EMS for the pursuit of private commercial business activities or profit-making ventures is prohibited. This includes any compensated, outside employment. Examples include, but are not limited to:

(a) Consulting for pay;

(b) Sales or administration of business transactions; and,

(c) Sales of goods and services.

(3) Unlawful or malicious activities are prohibited. The activities include, but are not limited to:

(a) Use of offensive, abusive, discriminatory, or objectionable language or graphics in either public or private messages;

(b) Use of lewd or sexually explicit language or graphics that are inappropriate or offensive to co-workers or the public, such as the use of sexually explicit materials, or materials or remarks that ridicule others on the basis of age, race, creed, religion, color, sex, disability, national origin, political belief, or sexual orientation;

(c) Engagement in matters directed toward the success or failure of a political party, candidate for partisan political office, or partisan political group, or an activity in support of political fundraising.

(d) Using EMS to misrepresent oneself, APHIS, or the Federal Government;

(e) Using EMS to "snoop" on or invade another person's privacy merely to satisfy idle curiosity and with no legitimate Federal Governmental purpose; and,

(f) Any use that reflects adversely on APHIS or the Federal Government.

(4) Inappropriate Signature Block Content. Signature blocks are intended for use as a method of providing sender contact information to message recipients. Signature blocks must not include graphics, quotes, sayings, or slogans that express any personal opinions, views, or religious themes. See section 6. a. (12) for mandatory APHIS signature block content.

(5) Violations. All suspected violations will be reported to appropriate Program management who will work with the APHIS Employee and Management Relations Branch (EMRB), Human Resources Division (HRD). The EMRB will review the facts to determine and validate whether or not a violation has occurred. If it is determined that a violation has occurred, the EMRB will consult with appropriate Program management for further action or disposition. Anyone needing assistance in determining whether a violation has occurred may contact EMRB. A current list of EMRB contacts is maintained at: ***http://www.aphis.usda.gov/mrpbs/contact_us/downloads/erphonelst.pdf***

Supervisors or system administrators who suspect misuse of APHIS email may request an investigation through the APHIS Administrative Investigations and Compliance Branch (AICB), HRD, who will coordinate with the Information Systems Security Program Manager (ISSPM). Supervisors may request an investigation when there are reasonable grounds for suspecting that the electronic mail will produce evidence that an employee has engaged in work-related misconduct.

(6) Exceptions. Exceptions that reduce the requirements of this Directive may be approved only in writing by the APHIS Chief Information Officer (CIO) or the APHIS Administrator.

7. RESPONSIBILITIES

a. The APHIS CIO will:

(1) Approve and ensure implementation of email security and privacy policies for the protection of APHIS information resources.

(2) Determine adequacy of security measures and accredit the APHIS email system in accordance with Federal and USDA requirements.

(3) Ensure that procedures are in place to obtain consent for monitoring of email systems, set forth in Section 6. above.

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

(1) Ensure compliance with the provisions of this Directive. Through their Information Systems Security Managers (ISSMs) and other organizational security structure, they will implement and manage the provisions of this Directive throughout their organization.

(2) Ensure that users of email systems are knowledgeable about the provisions of this Directive and that Unit ISSMs 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 material in email messages.

(4) Ensure that the names of employees who leave the Agency are provided to Customer Service as soon as possible prior to separation, but not later than 48 hours after the separation date. Users who are being removed for cause must have their email access terminated immediately.

(5) Ensure that procedures are in place to obtain expressed consent, and records of expressed consent are reviewed by the Program ISSM in AgLearn.

c. The ISSPM will:

(1) Be knowledgeable of and follow through on responsibilities identified in USDA ISS policies and procedures.

(2) Disseminate information concerning Federal and USDA email security and privacy policies and developments.

(3) Develop, coordinate, implement, and maintain email security and privacy policies for APHIS.

(4) Be involved in all investigations into misuse of email systems.

(5) Ensure that a security plan has been prepared or updated to protect email systems and that such systems are accredited in accordance with Federal and USDA requirements.

d. Program CIOs or their delegates will:

(1) Administer this Directive and monitor its compliance in their Program.

(2) Ensure that training exists to make users aware of their responsibilities for email use, privacy, and security.

(3) Assist in promptly identifying, investigating, and helping rectify violations of this Directive, including proper notification of violations to the EMRB, HRD.

(4) Administer processes (or oversee those actions) to ensure that user identifications are disabled or deleted when employees (including contractors) depart the Agency and that other appropriate actions are taken to protect Agency email records and access.

(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 6.b.(5), above.

e. Each APHIS employee who uses Agency email must:

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

(2) Access (or attempt to access) only the email account and messages which he/she has been authorized. Monitoring or accessing others' email messages without their expressed consent is prohibited, and may result in appropriate disciplinary action.

(3) Take the necessary precautions to secure email access from unauthorized users and be accountable for actions taken using his/her email identification. Each employee must:

(a) Implement and maintain password protection for email access.

(b) Not share passwords with others except to appropriate personnel in the course of a security investigation.

(c) Change default passwords immediately when receiving an email account and password for the first time.

(d) Set email preferences to lock access after no more than 5 minutes of inactivity for all non-Outlook client email access methods. For example, mobile device access to email.

(e) Be aware of computer security and privacy concerns and guard against computer viruses.

(f) Treat unusual email messages with caution. Delete without opening any email received from suspicious senders. Detach attachments to a local drive and scan for malware before opening whenever the sender of the email is unknown. Never open suspicious email from a web mail interface.

(g) Never use email for transmitting or storing classified data.

(4) Understand that sending an email from an Agency mailbox or address is like sending a letter on official letterhead and may be interpreted as APHIS endorsement or policy. If sending a personal email under the limited use policy and there is any possibility your personal message could be interpreted as being related to APHIS or your position, add a short disclaimer that states your message or opinion is not associated with your job or APHIS interests.

Listed below is a sample disclaimer that can be used:

Disclaimer
The opinions expressed herein are my own personal opinions and do not represent my employer's view in any way.

(5) Protect sensitive and proprietary information. Users must:

(a) Refrain from sending nonpublic information to non-USDA addresses, except for authorized contractors, cooperators, partners or other Federal agencies.

(b) Protect commercial proprietary information in accordance with the conditions under which it is purchased, provided, or used.

(c) Prevent eavesdropping of sensitive email by using available encryption. The compression of file attachments for the purpose of reducing the file size for transmission is not encryption, and it is a preferred method of handling large messaging attachments.

(6) Learn about email etiquette, customs, and courtesies. Certain procedures and guidelines must be followed when using electronic mail communications, participating in electronic mail discussion groups, and sending attachments. See section 6.a. and b. for guidance on appropriate and inappropriate use.

8. INQUIRIES

a. Direct inquiries or requests for changes to this Directive to the APHIS ISSPM, 4700 River Rd., Riverdale, MD 20737 or call 301-851-2551.

b. This Directive can be accessed on the Internet at ***www.aphis.usda.gov/library***

/s/
Gary S. Washington
APHIS Chief Information Officer