

APHIS NETWORK AUDITING POLICY

1. PURPOSE

This Directive establishes APHIS requirements for the monitoring of the Agency network infrastructure to minimize the risk of unauthorized access.

2. REFERENCES

- a. National Institute of Standards and Technology (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- b. Federal Information Systems Controls Audit Manual (FISCAM), Volume 1: Financial Statement Audits.

3. SCOPE

- a. This Directive applies to all APHIS-owned network devices located in APHIS facilities that transmit data, voice, and video content.
- b. This Directive does not include radio transmitting devices and associated support systems.

4. DEFINITIONS

- a. Intrusion Detection System (IDS). A system composed of several components: sensors that generate security events; a console that monitors events and alerts, and controls the sensors; and a central engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received.
- b. Intrusion Protection Services (IPS). An automated toolset that works in conjunction with Intrusion Detection and Prevention (IDP) hardware to monitor and log attempts at access to the network infrastructure. Analyzing the data from the logs can help identify attempted and successful unauthorized and malicious entry into the network.

- c. Network Device Event. Any activity occurring on a network device that generates a system log (syslog) or System Network Management Protocol (SNMP) trap as defined by the local operating system.

5. POLICY

Security of the APHIS Information Technology (IT) infrastructure is vital to protecting APHIS computer systems and information. Proactive monitoring to detect attempts at unauthorized access is an important tool to accomplish this goal. Section 2. (a) and (b) above provide recommended security controls for protecting IT assets from unauthorized access. This Directive establishes APHIS policy and processes for the implementation of Section 2. (a) and (b) controls, as follows:

- a. APHIS will implement and maintain IDS and IDP in its computing facilities (Riverdale, MD; Ft. Collins, CO; Raleigh, NC; and Minneapolis, MN).
- b. All network device events will be collected, retained, reviewed, and correlated to detect suspicious activity and anomalies. All data telecommunication resources (equipment and services) syslog events must be collected.
- c. Network device event records will include, at a minimum: the user name, a description of the event, the target object for the action, the date and time of the event, and the name of the system where the network device event occurred.
- d. All audit collection systems will receive their timing from a common reliable source in order to correlate date-time stamps.
- e. Audit logs will be reviewed daily by authorized staff for suspicious activity.
- f. Appropriate and timely action will be taken to investigate anomalies and report observations and findings to Agency security and IT management, following appropriate APHIS incident handling procedures.
- g. Documentation pertaining to network auditing, including audit logs, monthly reports, evidentiary supporting documentation of investigations, and documentation of corrective actions, will be retained in calendar year blocks for 5 years (no incremental disposal).

6. RESPONSIBILITIES

- a. The APHIS Chief Information Officer will:
 - (1) Approve and ensure implementation of this Directive.

- (2) Approve any modifications to this Directive.
- b. Deputy Administrators/Directors of Program Units, and Heads of Major Business Offices will:
- (1) Disseminate this Directive to their respective staffs.
 - (2) Ensure that the terms of this Directive are followed within their Program Units.
 - (3) Assist in promptly identifying, investigating, and rectifying violations of this Directive.
- c. The Technology Resources Management (TRM) Staff, Marketing and Regulatory Programs Business Services (MRPBS), Information Technology Division (ITD), will:
- (1) Perform daily examinations of network IDS/IDP audit logs for evidence of suspicious activity, such as attempts at unauthorized access to the APHIS network.
 - (2) Immediately report suspicious activity, e.g., suspected attempts at unauthorized network access, to Agency IT Security staff and the Information Security Officer, MRPBS, ITD.
 - (3) Take immediate and appropriate action to investigate anomalies and suspicious activity, and report findings to the Information Security Officer, MRPBS, ITD.
 - (4) Generate a monthly report of network auditing activities for signature by the Information Security Officer, MRPBS, ITD. Documentation will include a summary of network auditing activities, detected anomalies and/or suspicious activity, a description of resulting investigation(s) and results, and corrective actions taken.
 - (5) File, maintain, and dispose of all network auditing documentation per the terms of this Directive.
- d. The Information System Security Program Manager, MRPBS, ITD, will:
- (1) Maintain this Directive, including receiving requests for, and executing, modifications in response to change requests and/or new requirements.

- (2) Perform a monthly review of APHIS network auditing activities to ensure that the terms of this Directive are being followed, and that APHIS network auditing practices are optimized to ensure the security of the APHIS network infrastructure. This includes:
 - (a) Reviewing, approving, and signing monthly reports of network auditing activities.
 - (b) Reviewing and signing reports of corrective actions performed as a result of anomalies detected during daily network monitoring activities, or subsequent investigations.
- (3) Review, approve, and sign monthly reports to verify that:
 - (a) The security logs have been examined.
 - (b) All actual attempts at unauthorized access have been investigated in a timely manner and corrective actions have been taken, where necessary.
- (4) Take timely action to correct technology or security weaknesses in the Agency network infrastructure discovered as a result of network auditing activities.
- (5) Regularly brief the Chief Information Officer on network audit findings and corrective actions.

7. INQUIRIES

- a. Questions concerning the information and processes described in this Directive should be directed to the TRM Branch Chief, MRPBS, ITD, at 301-734-8845.
- b. This Directive can be accessed at www.aphis.usda.gov/library

/s/

Gregory L. Parham
APHIS Chief Information Officer