



U.S. Department of Agriculture



Office of Inspector General
Midwest Region

Audit Report

Management and Security of APHIS Information Technology Resources

Report No. 33099-0004-Ch
MARCH 2004



UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250



DATE: March 3, 2004

REPLY TO

ATTN OF: 33099-4-Ch

SUBJECT: Management and Security of APHIS Information Technology Resources

TO: Bobby Acord
Administrator
Animal and Plant Health Inspection Service

ATTN: William J. Hudnall
Deputy Administrator
Marketing and Regulatory Programs – Business Services

This report presents the results of our audit of the Animal and Plant Health Inspection Service's management of its information technology resources. Your response to the draft report, dated January 21, 2004, is included in its entirety as exhibit B with excerpts and the Office of Inspector General's position incorporated into the relevant sections of the report.

We agree with your management decisions for Recommendations Nos. 2 through 12 and 14 through 18. Please follow your agency's internal procedures in forwarding final action to the Office of the Chief Financial Officer.

Management decision has not been reached for Recommendations Nos. 1 and 13. To reach management decision for these recommendations, APHIS needs to place the ISSPM in a position to independently oversee and report on the agency's compliance within its IT security program. In addition, APHIS needs to develop and implement configuration management policies and procedures, which will be used with its Patchlink application.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective action taken or planned and the timeframes for implementation for Recommendations Nos. 1 and 13. Please note that the regulation requires a management

decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance, and final action be taken within 1 year of each management decision.

We appreciate the cooperation and courtesies extended to us during this review.

/s/

ROBERT W. YOUNG
Assistant Inspector General
for Audit

Executive Summary

Management and Security of APHIS Information Technology Resources

Results in Brief

The Animal and Plant Health Inspection Service (APHIS), an agency of the U.S. Department of Agriculture, protects and promotes the nation's agricultural health. As a wide-ranging agency, it conducts much of its critical business by way of Information Technology (IT)—principally computers and networks—that share sensitive information across the nation and throughout the world. To ensure that APHIS' IT systems were reasonably secure, we evaluated the agency's IT security and Information Systems Security Program (ISSP).

We concluded that APHIS lacked IT security controls in some key areas, had not adequately implemented controls in other areas, and had not assigned the Information Systems Security Program Manager (ISSPM) to a level within the organizational structure to effectively manage security throughout the agency. These issues make APHIS' systems vulnerable to intrusion by malicious users.

We used security software to scan APHIS' computer systems and identified almost 900 high- and medium-risk vulnerabilities. Some examples included passwords that were left blank, computers that were configured to automatically allow access, and inactive accounts that were not disabled. These vulnerabilities are particularly worrisome because they allow malicious users to circumvent external defenses. In effect, they provide hackers with opportunities to exploit the IT system.

APHIS officials informed us that they had corrected the high-risk vulnerabilities. However, they did not provide documentation, or other means, for us to substantiate their statements. The officials also stated that they had not yet corrected the medium- and low-risk vulnerabilities because of other priorities.

We attributed the vulnerabilities disclosed by our scans to weak or nonexistent management controls. One of the most serious weaknesses was the agencies' management structure, which was not conducive to ensuring that timely security remedies were applied on an agency-wide basis. The ISSPM, who should have been monitoring IT security on an agency-wide basis, was not authorized and positioned to independently monitor parallel and superior division units. Instead, each unit had its own Information System Security Managers (Security Manager). These unit-level managers carried out certain aspects of the ISSPM's policy but reported to supervisors within the unit. Without agency-wide monitoring to ensure that all the unit's security managers had responded adequately, serious security risks threaten APHIS' data and systems.

To prevent these types of vulnerabilities, Departmental regulations require agencies to place ISSPMs at a level where they can 1) apply security across the entire agency's programs and 2) independently report to Administrators or Deputy Administrators¹. However, since the ISSPM does not report to a high enough level of management, APHIS' current management structure does not comply with either requirement. (See exhibit A.)

While APHIS' ISSPM did provide guidance to the security managers within the division units, the ISSPM was not monitoring IT security throughout the agency. The security managers who handled security incidents for the individual units were not required to report to the ISSPM. The inadequate procedures for handling, documenting, and reporting security incidents made APHIS vulnerable to agency-wide internal and external attacks. For example, when we telephonically contacted 15 randomly selected APHIS employees throughout the agency and asked them for their passwords, 10 gave them to us. In two instances, security managers issued new passwords, but did not report the security incidents up the chain of command. As a result, no one recognized that the local security incidents could have been part of an effort to penetrate APHIS' security.

APHIS had not complied with numerous OMB Circular A-130 requirements for agency ISSP's. Specifically, APHIS had not (1) conducted comprehensive risk assessments of critical systems, (2) created a comprehensive contingency plan to ensure that it could recover in the event of a disaster for major disruption in service, (3) developed adequate security plans, (4) adequately configured its systems and firewalls, (5) obtained the proper background investigations and assigned security levels commensurate with employees' duties, and (6) ensured that employees and contractors had received security awareness training. We attributed the agency's noncompliance to a lack of policy and procedures designed to ensure that staff adhered to all requirements. As a result, APHIS' IT resources were at greater risk and less capable of recovery in the event of a disaster.

We also evaluated controls over the modification of selected application software programs and the physical security of computer resources. We did not identify any problems in these areas.

Recommendations In Brief

APHIS needs to take immediate steps to mitigate identified risks to its IT resources. In particular, APHIS should resolve continuing high- and medium-risk vulnerabilities identified during scans of its systems. We also recommend that the ISSPM monitor IT security programs and incidents

¹ USDA DR 3140-0001 (10) (g) (8) dated May 15, 1996.

throughout the agency. Accordingly, APHIS should reposition the ISSPM to a level in the management structure consistent with agency-wide responsibilities and independent reporting to an appropriate level of management. APHIS also needs to comply with all OMB Circular A-130 requirements.

Agency Response

In its response dated January 21, 2004, APHIS agreed with all but one of the recommendations in the report. We have incorporated applicable portions of APHIS' response, along with our position, in the Findings and Recommendations section of the report. The agency's response is included in its entirety as exhibit B of the report.

OIG Position

We agree with APHIS' proposed corrective actions and have reached management decision on all but Recommendations Nos.1 and 13. In order to reach a management decision for Recommendation No. 1, APHIS needs to place the ISSPM in a position to independently oversee and report on the agency's compliance with its' IT security program. For Recommendation No. 13, APHIS needs to develop and implement configuration management policies and procedures, which will be used with the Patchlink application.

Abbreviations Used in This Report

APHIS	Animal and Plant Health Inspection Service
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
DM	Departmental Manual
DR	Departmental Regulation
FY	Fiscal Year
ISS	Information Systems Security
ISSO	Information Systems Security Officer
ISSP	Information Systems Security Program
ISSPM	Information Systems Security Program Manager
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
TCP/IP	Transmission Control Protocol/Internet Protocol
USDA	United States Department of Agriculture

Table of Contents

Executive Summary	i
Abbreviations Used in This Report.....	iv
Background and Objectives.....	1
Findings and Recommendations.....	3
Section 1 Information Systems Security Program (ISSP) Management Was Inadequate.....	3
Finding 1 APHIS Lacked Agency-Wide IT Security Monitoring.....	3
Recommendation No. 1.....	7
Recommendation No. 2.....	8
Recommendation No. 3.....	8
Recommendation No. 4.....	8
Recommendation No. 5.....	9
Recommendation No. 6.....	9
Finding 2 Centralized Reporting Procedures Were Inadequate.....	9
Recommendation No. 7.....	11
Recommendation No. 8.....	12
Section 2 APHIS’ ISSP Did Not Comply With IT Security Requirements	13
Finding 3 Inadequate Precautions to Protect Agency Resources	13
Recommendation No. 9.....	16
Recommendation No. 10.....	17
Recommendation No. 11.....	17
Recommendation No. 12.....	17
Finding 4 Inadequately Configured Systems and Firewalls	18
Recommendation No. 13.....	19
Recommendation No. 14.....	20
Finding 5 Insufficient Management Control Over Personnel Access to IT Systems	20
Recommendation No. 15.....	23
Recommendation No. 16.....	23
Recommendation No. 17.....	24
Recommendation No. 18.....	24
Scope and Methodology.....	25
Exhibit A – Current and Suggested ISSPM Placement in Management Structure	27
Exhibit B – APHIS’ Response To The Draft Report.....	28

Background and Objectives

Background

Information security, improving the overall management of information technology resources, and the transition to electronic business (e-government), has emerged as a top priority within the U.S. Department of Agriculture (USDA). Prior Office of Inspector General (OIG) reviews have identified non-compliance with federally mandated laws, regulations, and guidance relating to the management and security of information technology (IT) resources. As technology has enhanced the ability to share information instantaneously among computers and networks, it has also made organizations more vulnerable to unlawful and destructive penetration and disruptions. This environment poses a threat to the sensitive and critical operations of the Animal and Plant Health Inspection Service (APHIS).

Various laws have emphasized the need to protect agencies' sensitive and critical data, including the Privacy Act of 1974, the Computer Security Act of 1987, and the Paperwork Reduction Act of 1995. Responsibilities regarding information security were reemphasized in the Clinger-Cohen Act of 1997 and Presidential Decision Directive (PDD) 63.² Additionally, the Government Information Security Reform Act (GISRA)³, enacted on October 30, 2000, essentially codifies the existing requirements of the Office of Management and Budget (OMB) Circular A-130.⁴ The National Institute of Standards and Technology (NIST)⁵ has issued numerous Federal Information Processing Standards, as well as a comprehensive description of basic concepts and techniques entitled "An Introduction to Computer Security: The NIST Handbook," Special Publication 800-12. Finally, Departmental Manual (DM) 3140-1⁶ and USDA OCIO Cyber-Security Guidance also provide standards, guidelines, and procedures for the development and administration of automated data processing security programs mandated by Departmental Regulations (DR).

APHIS' mission is an integral part of USDA's efforts to provide safe and affordable food through the protection of the nation's animal and plant resources from agricultural pests and diseases. APHIS has six operational program units, Plant Protection and Quarantine, International Services, Veterinary Services, Animal Care, Biotechnology Regulatory Services, and Wildlife Services. It also has the Marketing Regulatory Programs Business

² PDD 63, Policy on Critical Infrastructure Protection, dated May 22, 1998.

³ The Federal Information Security Management Act of 2002, has replaced GISRA and partially repealed the Computer Security Act.

⁴ OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources.

⁵ The Computer Security Act of 1987 assigned NIST primary responsibility for developing technical standards and providing related guidance. Those responsibilities were reemphasized in the Clinger-Cohen Act of 1997.

⁶ USDA DM 3140-1, Management Automated Data Processing Security Manual.

Services Unit, which provides a variety of support services, including information technology management. In carrying out APHIS' mission, these program areas safeguard our borders, combat pests and diseases, care for animals, protect the environment and manage wildlife damage, lead scientific research, and set international standards.

APHIS' IT operations are primarily located in Riverdale, MD, and its Headquarters is located in Washington, D.C. APHIS' field activities are managed through its regional field offices, including area offices, work stations, technical centers, and animal import centers. Much of the agency's work is conducted in cooperation with State and local agencies, private groups, and foreign Governments. Work is conducted at field locations in the 50 States, Puerto Rico, Virgin Islands, Mexico, Central America, the Caribbean, Western Europe, Asia, and Africa. APHIS conducts agricultural pest and disease inspection services at all major airports, shipping ports, and land borders.

Objectives

Our objectives were to (1) assess the overall management of APHIS' Information Systems Security Program (ISSP); (2) determine the adequacy of security over the Local and Wide Area Networks; (3) determine if adequate logical and physical access controls exist to protect computer resources against unauthorized modification, disclosure, loss, or impairment; (4) evaluate controls over the modification of application software programs; and (5) determine the adequacy of controls over access to and modification of system software.

Findings and Recommendations

Section 1 Information Systems Security Program (ISSP) Management Was Inadequate

APHIS lacked agency-wide oversight of Information Technology (IT) security. The manager who should have been monitoring APHIS' security program throughout the agency, the Information Systems Security Program Manager (ISSPM), had not been empowered to monitor IT security and was not properly positioned in the management hierarchy to ensure compliance with security requirements. Instead, APHIS entrusted Information System Security Managers (Security Managers) within individual divisions to handle security concerns. When these managers encountered security incidents, they did not report them to a centralized authority, such as the ISSPM. The lack of oversight leaves critical agency data and systems vulnerable to destruction, misuse, or manipulation by malicious users.

APHIS managers had not ensured that system administrators timely responded to serious security risks uncovered by vulnerability scans (e.g., blank passwords, standard configuration settings, etc.). As a result, the same types of high-risk vulnerabilities remained when we examined APHIS' networks. From the bottom up, security incidents were not reported up the chain of command and, thus, not addressed, leaving APHIS vulnerable to agency-wide systemic attacks.

Finding 1

APHIS Lacked Agency-Wide IT Security Monitoring

APHIS had not implemented procedures to monitor IT security on an agency-wide basis. The ISSPM, who should have been monitoring IT security, was not performing this function. Instead, the ISSPM was issuing security alerts, creating and reviewing policy, and providing technical support to security staff within the agency.

Agency policy states that the ISSPM should manage the agency's ISSP and ensure compliance with IT security requirements.⁷ It also requires the ISSPM to perform reviews of program units to ensure that they are complying with Federal, departmental, and agency requirements.⁸ However, our review disclosed that APHIS officials had inappropriately assigned the responsibility of managing the ISSP to security managers. The security managers performed as lead system and security specialists within APHIS'

⁷ APHIS Directive 3140.5 (5) c (1), APHIS Information System Security (ISS) Roles and Responsibilities, dated 05/26/00.

⁸ APHIS Directive 3140.5 (5) c (3), APHIS ISS Roles and Responsibilities, dated 05/26/00.

divisions. They were responsible for implementing system security, controlling system access, preparing contingency and disaster recovery plans, and preparing risk assessments of agency systems. The security managers, who reported to supervisors in their respective units, were not monitored by the ISSPM.

The ISSPM did provide guidance in the form of technical support, security alerts, and policy but did not follow up to ensure that agency officials followed the guidance. This lack of management control over the agency's ISSP allowed serious vulnerabilities in APHIS' information systems to go undetected.

We detected some of these vulnerabilities during our scans of the agency's systems and IT infrastructure. Our scans disclosed 873 medium- and high-risk vulnerabilities.⁹ APHIS had previously identified similar weaknesses, but had not corrected them. APHIS relied on computer specialists within the Information Technology Division (ITD), to ensure that vulnerabilities were resolved or mitigated to preserve Privacy Act-protected data maintained by the agency. However, APHIS had no written policy or procedures for the specialists to follow in resolving the vulnerabilities.

We questioned the Deputy ISSPM about the actions taken to resolve the vulnerabilities. He stated that he forwarded the vulnerabilities to the appropriate staff with instructions to resolve the problems. However, at that time, no one had responded to his request. Thus, we asked two computer specialists about the actions they had taken to eliminate the security vulnerabilities identified by the scans. They informed us that no corrective action had been taken; one computer specialist was awaiting approval, and the other stated that the reports contained too many false positives to correct in a timely manner.

Most seriously, APHIS' Transmission Control Protocol/Internet Protocol (TCP/IP) system¹⁰ and its Network Operating System¹¹ were vulnerable. Some examples of vulnerabilities that posed a serious danger to APHIS' TCP/IP system included:

- Workstation computers that had blank or easily guessed administrator passwords. The administrator is the most trusted user on the system with complete control over system activities. Given this level of

⁹ We also identified 1,499 low-risk vulnerabilities. High-risk vulnerabilities are those that provide access to the computer, and possibly the network of computers. Medium-risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low-risk vulnerabilities are those that provide access to sensitive, but less significant network data.

¹⁰ TCP/IP is a series of agreed upon formats for transmitting data—protocols—used on the Internet as the primary standard for the movement of data.

¹¹ An Operating System is a program on a network (or individual computer) that runs all the other programs in addition to maintaining system security.

access, an attacker could easily alter or destroy critical data stored on APHIS' networks.

- Systems that had easily guessed user account names and passwords for transferring files and administering the system from remote locations. Hackers use system penetration software that runs through lists of commonly used account names and passwords (e.g., "1111," "abcdef," blank, etc.) to gain access to network systems. Once in, an attacker can infect crucial files with viruses, or change configuration settings to cause other damage.
- Users had stored identification and passwords for remote access on their computers so they could automatically dial into the network without going through the authentication process. This method of dialing in, however, also allows hackers to circumvent the network security.
- Software used to manage the network had been left in the manufacturer's standard configuration. Since these settings are widely known, an attacker could use the program to obtain or change system information and gain information about open links to other systems.

Some examples of vulnerabilities that posed serious access control weaknesses included:

- User account lockouts that expired after 30 minutes. A lockout time of 30 minutes leaves systems highly susceptible to brute force attacks. In a brute force attack, a hacker will continuously enter different passwords in an attempt to access a system. To prevent this, accounts should remain locked out until they are reset by the Administrator.
- User accounts that were not locked until after five failed logon attempts. Departmental guidance¹² requires a maximum setting of three failed logon attempts before locking the user account. If this setting is too long, an attacker has more opportunity to try different passwords in an attempt to gain access to a system.
- Passwords for 222 of 1,980 user accounts that were set to never expire. Departmental guidance¹³ requires that passwords for all systems, applications, or processes be changed every 60 days for general users. Passwords issued to system administrators, system managers, software

¹² USDA DM 3140-1.6, Appendix D, Amendment 6, Section 5.

¹³ USDA OCIO Cyber Security Guidance Regarding C2 Controlled Access Protection, CS-013, page 11.

engineers, or those that are using dial-in access should be changed every 30-45 days.

- Remote access software that was set to automatic startup for three servers. This configuration sidesteps network security by allowing the server to be automatically started rather than being manually started with the required passwords. Thus, the network could be compromised from a remote location.
- Inactive accounts that had not been disabled. User accounts that become inactive, but are not disabled, provide opportunities for unauthorized users to gain access to the network.

We also conducted a detailed assessment of APHIS' telephone system to identify active modems on its network. Active modems provide a gateway into the network system by converting digital and analog signals for transmission between components. We identified 45 potential lines into APHIS' network. APHIS officials stated that these lines were connected to facsimile machines. However, when we tested all 45 numbers, two of the numbers rang but did not answer. APHIS officials said that one facsimile machine did not accept incoming calls, and the other was not connected. However, an open telephone line is ripe to become a connected modem and a link into APHIS' systems. Unsecured modems are also susceptible to war dialing—the common hacker practice of systematically calling telephone numbers to find an unsecured gateway into a network.

Departmental regulations require agencies to evaluate security measures in place on network gateways¹⁴ and to assess risks and vulnerabilities each year.¹⁵ However, at the time of our review, APHIS had no written policy and procedures to implement these requirements. Consequently, there had been no agency-wide monitoring of the gateways into APHIS' network.

The lack of monitoring IT security on an agency-wide basis creates a dangerous situation for APHIS' IT structure. With no one ensuring that identified high- and medium-risk vulnerabilities are mitigated, APHIS continues to be susceptible to attack and is exposed to common hacker penetration techniques. Thus, sensitive information, critical systems, and overall functions are correspondingly endangered.

DR 3140-001¹⁶ states that the ISSPM must be able to apply security throughout an agency and allows for APHIS' ISSPM to work at the top level

¹⁴USDA DR 3140-001, Section 16, USDA Information System Security Policy, dated May 15, 1996.

¹⁵USDA DR. 3140-002, USDA Internet Security Policy, Section 7 (b)(1), dated March 7, 1995.

¹⁶ USDA DR 3140-001 Section 10 (g)(8), USDA Information Systems Security Policy, dated May 15, 1996.

of management, reporting directly to the Administrator. As it stands, APHIS' ISSPM is located near the bottom of the agency's management structure. With three intervening layers of control (see exhibit A), the agency's ISSPM lacks the authority and independence to oversee IT security, and ensure that departmental policies and procedures are effected.

We also noted that the ISSPM works in a branch of the ITD and reports to the Chief Information Officer (CIO) who implements the agency's IT activities (see exhibit A). Consequently, there is a potential for a conflict of interest within the CIO's authority. That conflict involves the goal of the ISSPM (to maintain IT security) and the goal of the ITD (to ensure systems run efficiently). The conflict occurs because security measures slow down IT efficiency. This potential for conflict is increased by the ISSPM's lack of independence from the IT functions. It also runs counter to departmental regulations which focus on the ISSPM's ability to report findings independently. The second chart in exhibit A illustrates an independent IT Security position.

Recommendation No. 1

Reposition the ISSPM to report directly to the APHIS Administrator.

Agency Response.

APHIS stated that the ISSPM function is appropriately placed under the CIO's area of responsibility. The Administrator has delegated authority to the CIO to issue agency security policy. The CIO is a member of the APHIS management team and has unrestricted access to senior agency officials.

OIG Position.

We disagree with APHIS' proposed management decision. The ISSPM should be in a position to independently report security weaknesses and noncompliance with security requirements throughout APHIS, including those related to the CIO and the Information Technology Department. The ISSPM reporting directly to the CIO reduces the level of assurance that all weaknesses will be properly reported to the appropriate level of management.

To reach management decision, APHIS needs to place the ISSPM in a position to independently oversee and report on the agency's compliance with its IT security program.

Recommendation No. 2

Develop and implement agency-wide IT security monitoring procedures.

Agency Response

APHIS has implemented a monthly scanning process in accordance with cyber security directives. APHIS will improve agency-wide IT security monitoring procedures by September 30, 2004.

OIG Position.

We accept APHIS' management decision for this recommendation.

Recommendation No. 3

Correct all high-and medium-risk vulnerabilities identified by our scans in the TCP/IP Systems.

Agency Response.

APHIS has resolved all the vulnerabilities identified by OIG's scans and will develop a compliance review program for resolving vulnerabilities by September 30, 2004.

OIG Position.

We accept APHIS' management decision for this recommendation.

Recommendation No. 4

Ensure that corrective actions are taken on all the vulnerabilities identified in APHIS' network operating system.

Agency Response.

APHIS has corrected all vulnerabilities identified in APHIS' network operating system. In addition, the remote access mechanism was recently replaced with a more secure solution.

OIG Position.

We accept APHIS' management decision for this recommendation.

Recommendation No. 5

Develop formal policies and procedures on the use and annual review of modems and remote access software that conforms to departmental guidance.

Agency Response.

APHIS will create formal policies and procedures in conjunction with a compliance review program on the use and annual review of modems, and remote access software, by September 30, 2004.

OIG Position.

We accept APHIS' management decision for this recommendation.

Recommendation No. 6

Develop and implement policy and procedures that comply with departmental regulations on periodic vulnerability scans of network resources.

Agency Response.

APHIS has adopted the policy and procedures in the recommendation.

OIG Position.

We accept APHIS' management decision for this recommendation.

Finding 2

Centralized Reporting Procedures Were Inadequate

APHIS had inadequate procedures for handling, documenting, and reporting security incidents. Agency officials informed us that their practice was to handle security incidents at the lowest possible level (e.g., by a security manager). We do not disagree with the policy of having security managers or other security officers respond to security incidents. However, security incidents must be documented and timely reported to a centralized authority, such as the ISSPM. An agency must have formal written procedures about relaying identified security violations to a central security management office so that related incidents can be recognized, reported, and addressed before they disrupt agency activities.

APHIS policy¹⁷ requires that system administrators and/or Information Systems Security Officers (ISSO's) review Internet logs and other audit trails at least every three days. System audit logs provide management with valuable information about activity on its computer systems, including reviews and analyses of management, operational, and technical controls. However, it does not have policies and procedures that outline the logs and reports to review, the appropriate actions to identify and correct violations, and the documentation to maintain.

NIST SP 800-14¹⁸ recommends that all aspects of computer support and operations be documented to ensure continuity and consistency. NIST also recommends a periodic review of system-generated logs to detect security problems, including attempts to exceed access authority or gain system access during unusual hours. The Cyber Security Manual, "USDA Computer Incident Response Reporting Procedures," establishes departmental policy and procedures for reporting IT security incidents.¹⁹ It requires all agencies to implement internal incident handling procedures that define how to report intrusions and attempted intrusions. The manual also specifies that these procedures should include a policy for reporting incidents through the chain of command and requires that all IT security incidents regardless of the source of notification or level of magnitude be reported to the ISSPM.

With almost 9,000 employees, only one IT security incident was reported to APHIS' ISSPM in fiscal year 2002—a stolen computer. Many of the manual's examples of security incidents, though, are events that occur on a regular basis: loss of passwords, detection of computer viruses, termination of disgruntled employees, etc. Given the size of APHIS, and the recurrent nature of these events, we thought it unlikely that there had been only one incident during the entire year.

To determine if officials throughout the agency were reporting IT security incidents as required, we employed a common hacker technique called social engineering and contacted 15 randomly selected employees via the telephone to ask for their user identifications and passwords. We were able to obtain the information from 10 employees, and one even provided us with the user identification and password needed to access the Department's Federal Financial Information System.

Employees, their supervisors, or the security manager for their program area, should have immediately contacted the ISSPM to report the incident. However, only two employees contacted their security managers. Instead of

¹⁷ APHIS Directive 3140.3 (6) (i) Internet Administration, dated May 26, 2000.

¹⁸ NIST SP 800-14, Sections 3.9 and 3.4.5, dated September 1996.

¹⁹ USDA DM 3500-001 dated October 25, 2001.

reporting the incident up the chain of command, the security managers just changed their passwords in accordance with APHIS' policy of handling incidents at the lowest level. These security incidents should have been reported to the ISSPM. Hackers typically work by probing constantly for weakness throughout a system. To defend against these kinds of widespread assaults, an effective security program must facilitate recognizing attacks on its local IT systems for what they really could be, an effort to break through its defenses.

Given procedures to alert the ISSPM to agency-wide security problems, a security manager can apply the security program appropriately to protect APHIS' information systems (e.g., issue a security alert) before an attacker finds a weak point (e.g., someone gives out a password over the phone). Without procedures to inform the ISSPM of security incidents, APHIS' IT systems are susceptible to agency-wide attacks.

Agency officials stated that they were in the process of developing formal procedures for reporting IT security incidents. We viewed the draft procedures and concluded that they provided adequate direction for handling IT security incidents except, crucially, they do not require that all security incidents be reported to the ISSPM.

Recommendation No. 7

Formulate and implement procedures for reporting all security incidents to the ISSPM.

Agency Response.

APHIS will finalize written procedures concerning the reporting of security-related incidents by April 30, 2004. In addition, APHIS plans to update its security training, to include the reporting requirements, by September 30, 2004

OIG Position.

We accept APHIS' management decision for this recommendation.

Recommendation No. 8

Establish and implement procedures for monitoring systems logs and documenting actions taken.

Agency Response.

APHIS will develop procedures by April 30, 2004, requiring all Systems Administrators to review system audit logs every three days. Documentation of the reviews will be implemented by September 30, 2004.

OIG Position.

We accept APHIS' management decision for this recommendation.

Section 2 APHIS' ISSP Did Not Comply With IT Security Requirements

APHIS had not complied with numerous IT Security requirements for agency ISSPs. We attributed this to the lack of agency-wide requirements designed to ensure that the agency's plans, policies, and procedures, met applicable IT security requirements. (See Finding No. 1 for our discussion regarding the ISSPM's monitoring responsibilities.) As a result, APHIS' IT resources were more at risk and less capable of recovery in the event of a disaster.

We specifically determined that APHIS had not (1) conducted comprehensive risk assessments of critical systems, (2) identified sensitive data on its systems, (3) created a comprehensive contingency plan to ensure that it could recover in the event of a disaster or major disruption in service, (4) developed adequate security plans, (5) adequately configured its firewall system, (6) obtained the proper background investigations and assigned security levels commensurate with employees' duties, and (7) provided adequate training to employees and contractors.

Finding 3

Inadequate Precautions to Protect Agency Resources

APHIS had not adequately planned for the continued operations of its IT systems. This occurred because the agency had no written procedures for assessing risk in its systems and for preparing contingency and security plans. Thus, the agency lacked a coherent security approach that assessed its systems, took reasonable steps to mitigate risks, or planned to recover quickly in case of disaster.

Risk Assessment

OMB Circular A-130²⁰ states that for general support systems and major applications agencies must demonstrate specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time. In addition, PDD 63²¹ requires each agency to identify critical infrastructure, the vulnerabilities that threaten the infrastructure, and to develop a remediation plan to correct those vulnerabilities. NIST²²

²⁰ OMB Circular A-130, Section 8-Policy b (3)(b) iv-vi, dated November 30, 2000.

²¹ PDD-63, dated May 22, 1998.

²² NIST SP 800-30 dated October 2001 (January 2002 on website, <http://csrc.nist.gov/publications/nistpubs/index.html>).

guidance gives the first step to assessing risk for IT systems as defining the scope of the effort. Essentially, this step is an information gathering stage intended to delimit the operational environment. Collecting the necessary system related information includes detailing: a network diagram, the physical security environment (e.g., facility security), and the operational controls (e.g., backup procedures, system maintenance policies, etc.). An adequate risk assessment must also include a threat statement that lists the potential threat-sources for a given IT system (e.g., natural threats like earthquakes, human threats like malicious attacks, or environmental threats like power-failure), and a list identifying IT vulnerabilities that could be exploited by threat-sources. In addition, an adequate risk assessment should generate a list of controls that will mitigate the likelihood of a vulnerability being exploited, and a set of recommended controls and solutions to mitigate risk.

Agency officials informed us that they had conducted risk assessments on mission critical applications using the APHIS Rapid Risk Assessment Tool. However, we concluded that the APHIS Risk Assessment was incomplete because it did not include necessary information such as a network diagram, a description of the physical security environment, an explanation of back-up procedures, and a system maintenance policy. It had also not identified system weaknesses and sources of potential threats. Specifically, APHIS' risk assessment did not specify:

- a. system vulnerabilities that could be exploited,
- b. threats that could exploit those vulnerabilities,
- c. controls that protected IT weak points and reduced the impact of adverse events, and
- d. recommendations for alternative ways to mitigate identified risks.

APHIS also had not identified sensitive data on its systems. Sensitive data is unclassified information that should not be disclosed to any individual without the need to know. This could include data on permits to import biohazardous materials and on inspection activities at airports, seaports, and border crossings. According to NIST 800-12²³ APHIS is required to perform sensitivity assessments to identify the critical data processed on its systems.

Contingency Plans

APHIS did not have a comprehensive contingency plan to ensure recovery of critical systems in the event of a disaster or major disruption in service. Officials informed us that the agency had a Continuity of Operations Plan

²³ NIST SP 800-12 Chapter 8.4.1.1 Conducting a Sensitivity Assessment

(COOP) that was also used as a contingency plan. The plan listed APHIS' management team, program coordinators, and back-up personnel (as of May 9, 2002). It also delegated APHIS' Administrator's authority and gave a list of suggested actions for each COOP member. The COOP is a critical document to have in case of emergency, but it deals primarily with organizational planning and not information systems. Attached to APHIS' COOP is the APHIS Emergency Operation Centers and Continuity of Operation Plan Strategic Initiative dated May 31, 2002, which outlines how Emergency Operation Centers (IT systems) and COOP procedures (organizational structure) can be merged. This document, however, does not describe what is in place, but what should be in place.

OMB Circular A-130²⁵ requires agencies to establish a contingency plan, which allows them to function if automated support (IT systems) fails. It further states that managers should plan how they will perform their mission in the event of system loss or failure. NIST draft guidance²⁶ states that contingency plans should focus on information systems. In particular, a contingency plan should address the details of the systems and the steps needed to restore them, as well as how to recover data from backup tapes.²⁷

Agency officials agreed that the COOP was inadequate as a contingency plan. They are currently addressing this and other IT issues. As it stands, APHIS cannot be assured that its network and operations can recover quickly and effectively to accomplish its mission in the event of an emergency.

Security Plans

APHIS' security plans for three mission critical systems did not contain all the requirements of OMB Circular A-130 and NIST SP 800-18. APHIS officials were aware of the deficiencies from an OCIO review in fiscal year (FY) 2001 that identified the same issues.

For calendar year 2002, OCIO waived the requirement for submission of security plans and encouraged agencies to correct deficiencies in their plans during this time period. Therefore, at the time of our review, the agency was working on correcting the deficiencies. Until the security plans are updated and properly certified, APHIS cannot be assured that information collected, processed, transmitted, stored, or disseminated in general support systems and major applications is secure.

²⁵ OMB Circular A-130, Appendix III, B (a) (2) (a) and B(b)(2)(d) dated November 30, 2000.

²⁶ NIST SP 800-34, Executive Summary, December 2001.

²⁷ We noted as well that APHIS has not designated an offsite facility for the storage of its backup tapes.

We reviewed the security plans for three agency systems and determined that they did not include the requirements; rules of behavior, training, personnel controls, incidence response, continuity of support, technical security, and system interconnection. The information provided in APHIS' plans was either absent, insufficiently documented, or too brief.

APHIS had not documented, for example, whether system users received security training. There was no indication that individuals with security responsibilities received sufficient training to perform their duties. In general, personnel controls were not sufficiently documented and there were no written procedures for requesting, establishing, issuing, maintaining, and closing user accounts.

APHIS' plans also did not include rules of behavior for individual users with clearly delineated expectations and consequences of misbehavior although such rules were a significant issue in OCIO's review. The rules should—but did not—cover dial in access, work from home, connection to the Internet, use of copyrighted works, unofficial use of government equipment, and the assignment and limitation of system privileges and individual accountability.

APHIS responded that the mission critical system security plans detailed the rules of behavior. These plans, though, only include the following statement: "Currently users are instructed on security measures during training. In the future, these measures will be added to user documentation and in memorandums to supervisors/managers for their awareness." Clearly this does not substitute for fully developed and documented rules of behavior policy, which addresses security training.

Recommendation No. 9

Perform a risk-assessment that meets NIST guidelines.

Agency Response.

APHIS submitted a certification and accreditation timeline to the CIO, covering all major applications and underlying general support systems in the APHIS IT infrastructure. APHIS plans to complete the risk assessment by September 30, 2004.

OIG Position.

We accept APHIS' management decision for this recommendation.

Recommendation No. 10

Develop a contingency plan based on the risk assessment and geared toward the needs of the ISSP.

Agency Response.

APHIS submitted a certification and accreditation timeline to the CIO, covering all major applications and underlying general support systems in the APHIS IT infrastructure. APHIS plans to develop a contingency plan by September 30, 2004.

OIG Position.

We accept APHIS' management decision for this recommendation.

Recommendation No. 11

Ensure that security plans for mission critical systems meet regulatory requirements.

Agency Response.

APHIS submitted a certification and accreditation timeline to the CIO, which stated that security plans for mission critical systems would meet regulatory requirements by September 30, 2004.

OIG Position.

We accept APHIS' management decision for this recommendation.

Recommendation No. 12

Establish policy and procedures to ensure that all applicable requirements for performing risk assessments, and developing contingency and security plans, are met.

Agency Response.

APHIS submitted a certification and accreditation timeline to the CIO, covering all major applications and underlying general support systems in the APHIS IT infrastructure, including performing risk assessments, and developing contingency and security plans.

OIG Position.

We accept APHIS' management decision to this recommendation.

Finding 4

Inadequately Configured Systems and Firewalls

APHIS did not configure its security systems to full advantage. Both its configuration management program and its firewalls were not set to provide maximum protection. We attributed this to a lack of formal policy and procedures that describe the proper configuration of systems and firewalls.

Configuration Management

NIST²⁸ guidelines recommend that agencies develop a configuration management program, which ensures that systems are routinely updated with recent security patches and other software updates.²⁹ APHIS had not developed such a program. As a result, servers and workstations were not protected from the latest threats.

Software companies release new patches daily to address vulnerabilities or weaknesses in software that can be exploited by malicious users. The failure to keep operating system and application software updated is a common mistake made by IT professionals. In addition, a common misperception among some system administrators is that a secure firewall reduces the need for timely patching. While APHIS' systems are behind firewalls, these firewalls should not be the only defense against commonly known vulnerabilities. (A firewall is a system designed to prevent unauthorized access into or from a network.) NIST guidance states that the implementation of a firewall should not preclude an agency from patching its system.

We attributed 183 of the 266 high-risk vulnerabilities disclosed by our scans to APHIS not applying available patches to its systems. During our review, APHIS officials completed the installation of appropriate patches to address all high-risk vulnerabilities. While this corrects existing vulnerabilities, it does not ensure that patches will be applied in the future to correct additional vulnerabilities. APHIS needs a configuration management program to ensure that patches are applied as they become available.

²⁸ NIST SP 800-40 "Procedures for Handling Security Patches," dated August 2002.

²⁹ Patches are pieces of program that are intended to fit into previously released software in order to protect (patch) newly identified vulnerabilities. Software companies release patches as well as more comprehensive software updates daily.

Firewall Configuration

APHIS had not maintained its firewall in accordance with NIST guidelines.³⁰ We identified two critical rules that were missing from the agency's firewall configuration. APHIS had also not monitored its rules on at least a quarterly basis and ensured that they were maintained at a manageable number as required by NIST guidelines. Our analysis of APHIS' firewall rules also revealed that several were either no longer needed, were redundant, or were not configured in the best interest of network security. For example, we found several rules with notes attached to them stating "will not need." We question why these rules still exist.

Some redundant rules included one that allowed Internet traffic through the firewall and into the agency's Demilitarized Zone, but not farther. Another rule allowed email through the firewall to a list server, while a third rule allowed Internet traffic through to a web server. Redundant rules can lead to system degradation and can accidentally introduce holes in the firewall. Maintaining rules that are no longer needed may cause other rules to work incorrectly if accidentally or intentionally activated.

Recommendation No. 13

Develop and implement configuration management policies and procedures, which require the application of all recent security patches and software updates.

Agency Response.

APHIS intends to implement Patchlink patch management software. In addition, APHIS' compliance review program will assess compliance with configuration management procedures.

OIG Position.

We disagree with APHIS' proposed management decision. In order to reach management decision, APHIS needs to develop and implement configuration management policies and procedures, which will be used with the Patchlink application to apply security patches and software updates.

³⁰ NIST SP 800-41, "Guidelines on Firewalls and Firewall Policy," dated January 2002, page 47/74.

Recommendation No. 14

Develop and implement policies and procedures for conducting quarterly reviews of the firewall configuration that are consistent with NIST guidance.

Agency Response.

The CIO will create procedures requiring quarterly reviews. In addition, the compliance review program will require evaluation of compliance efforts. Completion is expected by September 30, 2004.

OIG Position.

We accept APHIS' management decision for this recommendation.

Finding 5

Insufficient Management Control Over Personnel Access to IT Systems

APHIS did not ensure that its employees were properly investigated for access to its systems, or trained to use those systems securely. In addition, it did not have control over employees' access to its systems. We also found APHIS was not matching user accounts with employee records. We attributed this to the agency's lack of formal requirements in these areas.

Background Investigations

APHIS had not performed required background investigations of critical IT staff. This occurred because the agency did not have requirements for higher-level security clearances written into IT job descriptions. Consequently, APHIS had not assigned security clearances commensurate with employee duties and access to confidential information.

Federal Law³¹ and OMB Circular A-130 require that persons who are authorized to bypass significant technical and operational security controls have periodic background investigations commensurate with the risk and magnitude of harm they could cause. DM 3140-1.1³² also requires personnel, including contractors, working in the automated data processing environment to have appropriate security clearances.

³¹ Title 5, CFR731.106, dated January 1, 2003.

³² USDA DM 3140-1.1 (6)(a)(6), dated March 5, 1992.

APHIS officials had identified 77 employees who should receive a higher clearance and corresponding background investigation. However, those employees only had a basic level security clearance. At the time of our review, APHIS officials were in the process of determining the appropriate security clearance levels for all staff. One official said that network and systems administrators would receive higher-level security clearances. The CIO, ISSPM, Deputy ISSPM, and two ITD managers would be investigated for top-secret security level clearances.

Security Training

APHIS had not ensured that employees and contractors had received annual security awareness training before allowing them to access its systems. This occurred because the agency had not developed and implemented procedures requiring such training.

The Computer Security Act requires agencies to provide periodic mandatory training to all employees involved in the management or use of Federal computer systems.³³ OMB Circular A-130 requires that all individuals be appropriately trained to fulfill their security responsibilities before allowing them access to agency systems. DR 3140-001³⁴ sets two of USDA's ISSP goals as providing annual IT security awareness training and ensuring that employees and contractors have sufficient guidance to discharge their security responsibilities.

We found that no formal security awareness training had been provided since April 2001. An agency official stated that he verbally provided computer security training to newly hired employees, but had not documented the dates, nature of training, and employees' names.

APHIS officials were in the process of initiating a web-based training program for general security awareness and some types of specialized training for those employees with significant security responsibilities. This new training was originally scheduled for completion in November 2002. However at the time of our review, APHIS had not initiated the program.

Employee Access

APHIS could not provide adequate assurance that former employees and contractors no longer had access to agency systems. We attributed this to a lack of procedures to remove system users when they left the agency, and to a lack of an agency-wide verification process. In addition, APHIS did not

³³ PL 100-235, The Computer Security Act of 1987 Section 2 (b) (4).

³⁴ USDA DR 3140-001 (12), USDA Information System Security Policy, dated May 15, 1996.

maintain users' identifications in one central file. Instead, that information was maintained in 43 separate files.

OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," requires accountability of logical access through identification and authentication of users of the system. NIST³⁵ guidance also requires auditing and periodically verifying the legitimacy of current accounts and access authorizations.

To determine if APHIS was complying with these requirements, we requested a current list of employees' names and user identifications for its General Support systems. APHIS provided us with 7,022 user identifications (from the 43 files). Based on comparable files, we combined 4,656 of the user identifications and compared them to a list of current APHIS employees, which APHIS queried from National Finance Center records.

Our analysis disclosed 1,253 user identifications (about 18 percent) that were not on the current employee list. In addition, 651 of the 1,253 user identifications were not identified by first and last name of the employee. Thus, there was no way for us to determine if they were duplicates (one employee with two accounts), belonged to terminated employees, or were used by unauthorized individuals with access to APHIS' systems.

From the user identifications that remained (602), 12 belonged to APHIS contractors. We also compared a sample selected from the first three pages (121 user identifications) against a hard-copy employee list provided by APHIS. Although agency officials said that the electronic list from NFC and the hard copy should be identical, we ascertained that there were additional employee names on the manual list. We identified an additional 54 employees or contractors from the manual lists. After accounting for these employees, there were still user identifications assigned to people that were not identified on the employee lists provided by APHIS.

Since APHIS has user identifications unaccounted for, there is a potential for unauthorized user access to its systems. To determine how these user identifications came to be on APHIS' system, we reviewed controls over issuing and removing user identifications.

APHIS' customer support employees informed us that they do not require employees to complete request forms for initial access to APHIS' system and that they do not document changes to employees' status. Customer support administrators are not always informed when an employee's access should be

³⁵ NIST SP-800-12 (10.2) p112 Introduction to Computer Security

deleted. In general, employees did not know whom they should notify to delete an employee's access, and who should do the notification.

APHIS Directive 3140.5³⁶ charges the Deputy Administrators/Directors of Program Units and Heads of Major Business Offices with the responsibility to ensure that controls are established and maintained to modify/revoke information access privileges for employees transferring to a new position or leaving the agency entirely. However, these individuals had not established controls.

A lack of access controls, including access removal, unnecessarily exposes APHIS to system attack. Former employees pose a particular threat to IT security because they may feel privileged to access by virtue of the fact that they had prior access. In addition, terminated employees pose a more serious security concern.

Recommendation No. 15

Develop and implement procedures to ensure that background investigations are written into the job descriptions of IT staff identified as warranting higher security clearances.

Agency Response.

APHIS created a security clearance directive, which addresses background investigations and security clearances. The directive will be issued and effective by April 30, 2004.

OIG Position.

We accept APHIS' management decision for this recommendation.

Recommendation No. 16

Develop and implement procedures to provide annual security awareness training to employees and contractors.

Agency Response.

APHIS will develop a comprehensive training package and complete a pilot of the new program by September 30, 2004.

³⁶ APHIS Directive 3140.5 (5)(b)(8), APHIS ISS Roles and Responsibilities, dated May 26, 2000.

OIG Position.

We accept APHIS' management decision for this recommendation.

Recommendation No. 17

Develop and implement procedures to reconcile authorized system users to APHIS employees and contractors agency-wide on an annual basis.

Agency Response.

APHIS' compliance review program will require the annual reconciliation of authorized users to APHIS employees and contractors. This will be completed by September 30, 2004.

OIG Position.

We accept APHIS' management decision for this recommendation.

Recommendation No. 18

Develop and implement procedures to document changes in employees' status, complete access request forms, and to notify the appropriate officials to delete employee access when necessary.

Agency Response.

The CIO will coordinate the implementation of this recommendation with APHIS' Human Resources, Technology Resource Management, Customer Service, and program officials. The new compliance review program will incorporate this requirement and be completed by September 30, 2004.

OIG Position.

We accept APHIS' management decision for this recommendation.

Scope and Methodology

Our audit was performed as part of a nationwide audit of selected USDA agencies' computer systems. We reviewed general system controls to ensure the integrity of information security over the network at APHIS, and in place over computer operations in the agency as a whole.

We conducted our audit from October 2002 through February 2003, in accordance with Government Auditing Standards.

To accomplish our objectives, we performed the following audit procedures:

- Reviewed agency, departmental, and other Federally mandated information technology security policies and procedures.
- Interviewed responsible APHIS officials managing the computer systems.
- Conducted scans on APHIS' networks using operating system vulnerability software.
- Analyzed records and controls established to ensure the integrity and security of APHIS' computer systems.
- Observed the physical controls over computer resources.

We assessed selected APHIS networks, including APHIS' LAN in Riverdale, Maryland and Ft. Collins, Colorado. We chose the Riverdale location because it is APHIS' IT Headquarters and Fort Collins because they maintained the computer applications we intended to review. We used commercially available software scanning products that:

- Identified over 1,100 vulnerabilities associated with various operating systems that use Transmission Control Protocol/Internet Protocol (TCP/IP),³⁷
- Tested system policy settings in networks, and

³⁷ TCP/IP is a series of protocols originally developed for use by the US Military and now used on the Internet as the primary standard for the movement of data on multiple, diverse platforms.

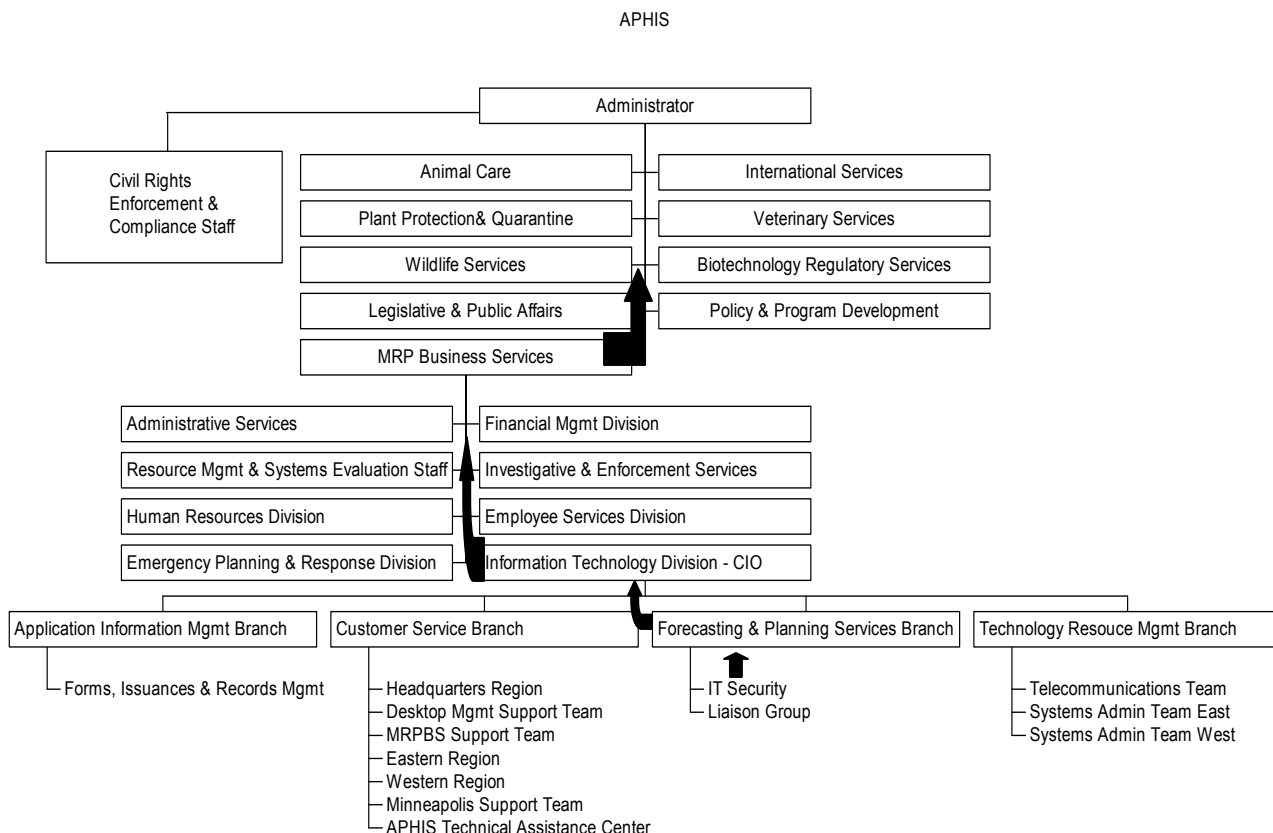
- Searched for modems within a set of telephone numbers to identify potentially unsecured carrier lines.

We assessed server and workstation security patches and updates to determine if all resources were routinely updated with recent security patches and other software updates as required by NIST. We also assessed firewall settings to determine if agency firewall rules were consistent with NIST guidance.

We also reviewed the change control process and procedures for two of APHIS' twenty-one mission critical computer applications. We selected the applications primarily due to their material relationship to the financial statements, and the high level of risk for information confidentiality. We also tested application controls for one system.

Exhibit A – Current and Suggested ISSPM Placement in Management Structure

Current APHIS ISSPM Position within APHIS Management Structure



Recommended APHIS ISSPM Position within APHIS Management Structure

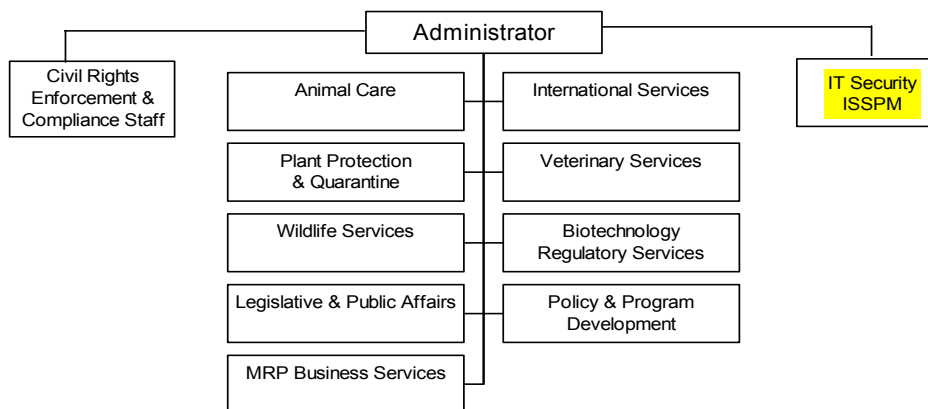


Exhibit B –APHIS' Response To The Draft Report



United States
Department of
Agriculture

Marketing and
Regulatory
Programs

Animal and
Plant Health
Inspection
Service

Washington, DC
20250

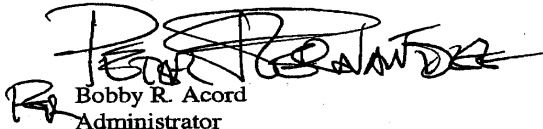
JAN 21 2004

SUBJECT: Management and Security of APHIS Information
and Technology Resources, Audit 33099-0004-Ch

TO: Richard J. Davis
Director
Administration and Finance Division, OIG

The enclosed information contains our comments for each recommendation identified in OIG's recent audit. Animal and Plant Health Inspection Service is committed to strengthening the security of our computer systems by reducing or eliminating critical areas of vulnerability, by improving overall controls; and, by addressing the OIG concerns regarding compliance with regulations. We have accomplished some corrective actions, and others are in various stages of completion.

Thank you for the opportunity to review the report. We look forward to receiving the final version of your audit pending publication and release.


Bobby R. Acord
Administrator

Enclosure



Recommendation 1: Reposition the Information Systems Security Program Manager (ISSPM) to report directly to the APHIS Administrator.

Response: We believe the function is appropriately placed under the Chief Information Officer's (CIO) area of responsibility. The Administrator has delegated authority to the CIO to issue Agency security policy. The CIO is a member of the APHIS Management Team and has unrestricted access to senior Agency officials.

Recommendation 2: Develop and implement Agency-wide Information Technology (IT) security monitoring procedures.

Response: We have implemented a monthly scanning process in accordance with cyber security directives. APHIS will improve our Agency-wide IT security monitoring procedures by the end of the current fiscal year.

Recommendation 3: Correct all high- and medium-risk vulnerabilities identified by OIG scans of the Transmission Control Protocol/Internet Protocol (TCP/IP) systems.

Response: We have resolved all the vulnerabilities identified by OIG's scans. The APHIS ISSP will develop a compliance review program for resolving vulnerabilities, and this will be effective by the end of the fiscal year.

Recommendation 4: Ensure corrective actions are taken on all vulnerabilities identified in the APHIS network operating system.

Response: ISSP has already implemented this recommendation. In addition, the remote access mechanism was recently replaced with a more secure solution.

Recommendation 5: Develop procedures and policies on the use and annual review of modems and remote access software which conforms to departmental guidance.

Response: ISSP will create procedures in conjunction with a compliance review program. The estimated timeframe for completion is the end of the current fiscal year.

Recommendation 6: Develop and implement policies and procedures to comply with departmental regulations on periodic vulnerability scans of network resources.

Response: The APHIS-ISSP has already adopted this recommendation.

Recommendation 7: Formulate and implement procedures for reporting all security incidents to the ISSPM.

Response: We will finalize written procedures concerning the reporting of security-related incidents. (Auditors reviewed the draft version of our procedures.) ISSP expects to complete this task within 90 days.

In addition, we plan to update training to include the reporting requirement. This second phase of implementation is scheduled to be in place before the end of the fiscal year.

Recommendation 8: Establish and implement procedures for monitoring systems logs and documenting actions taken.

Response: Procedures will be developed within 90 days requiring all Systems Administrators to review system audit logs every three days. This monitoring will improve compliance with APHIS 3140.3 (6) (i), Internet Administration.

As stated in the audit report, documentation enhances continuity and consistency of computer support and operations. The documentation requirement will be addressed pending the development of ISSP's compliance review program. Our corrective actions will be undertaken in accordance with the National Institute of Standards and Technology (NIST), Special Publication 800-14, which is referenced in OIG's report. This phase of recommendation 8 is scheduled for implementation by the end of fiscal year 2004.

Recommendation 9: Perform a risk assessment that meets NIST guidelines.

Recommendation 10: Develop a contingency plan based on the risk assessment and geared toward the needs of the ISSP.

Recommendation 11: Ensure security plans for mission critical systems meet regulatory requirements.

Recommendation 12: Establish policy and procedures to ensure all applicable requirements for performing risk assessments, and for developing contingency and security plans are met.

Response to 9-12: APHIS concurs with these recommendations. ISSP submitted a certification and accreditation (C&A) timeline to the Chief Information Officer. It covers all major applications and underlying general support system in the APHIS

Information Technology Infrastructure (AITI). Our C&A timeline was established in accordance with both NIST and departmental guidelines and will include risk assessments, contingency and security plans, as well as security testing/evaluation. Completion is anticipated before the end of the fiscal year.

Recommendation 13: Develop and implement configuration management policies and procedures requiring the application of all recent security patches/software updates.

Response: In conjunction with Patchlink patch management software implementations, the APHIS CIO unit will implement this recommendation. Actions will comply with departmental guidance and NIST, Special Publication 800-40, Procedure for Handling Security Patches. The estimated completion is prior to the end of the fiscal year. ISSP's compliance review program will require an assessment of compliance with configuration management procedures.

Recommendation 14: Develop and implement policies and procedures for conducting quarterly reviews of the firewall configuration that are consistent with NIST guidance.

Response: The APHIS CIO's office will create procedures requiring quarterly reviews. The aforementioned compliance review program will also require the evaluation of compliance efforts. Completion is expected by the end of the fiscal year.

Recommendation 15: Develop and implement procedures to ensure background investigations are written into job descriptions of IT staff identified as warranting higher security clearances.

Response: A security clearance directive was created which addresses these issues. Within 90 days, the directive will be issued and effective.

Recommendation 16: Develop and implement procedures to provide annual security awareness training to employees and contractors.

Response: APHIS will develop a comprehensive training package and complete a pilot of the new program this fiscal year.

Recommendation 17: Develop and implement procedures to reconcile authorized systems users to APHIS employees and contractors agency-wide on an annual basis.

Richard J. Davis

4

Response: ISSP's compliance review program will require the annual reconciliation suggested by auditors. This will be incorporated before the end of the fiscal year.

Recommendation 18: Develop and implement procedures to document: changes in employee status; completion of access request forms; and, notification of appropriate officials to delete employee access when necessary.

Response: The CIO's office will coordinate the implementation of this recommendation with APHIS' Human Resources, Technology Resource Management, Customer Service, and program officials. The new compliance review program will incorporate this requirement. The timeline for completion is designated as the end of the fiscal year.

Informational copies of this report have been distributed to:

Agency Liaison Officer, APHIS	9
Office of the Chief Financial Officer	
Director, Planning and Accountability Division	1
General Accounting Office	1
Office of Management and Budget	1