U.S. Department of Agriculture
Office of Inspector General
Financial and IT Operations
Audit Report

SECURITY OF INFORMATION TECHNOLOGY RESOURCES AT USDA DEPARTMENTAL ADMINISTRATION

Report No.
23099-2-FM
May 2002

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: May 22, 2002

REPLY TO
ATTN OF: 23099-2-FM

SUBJECT: Security of Information Technology Resources at
USDA Departmental Administration

TO: Lou Gallegos
Assistant Secretary for Administration

This report presents the results of our audit of the Security of Information Technology Resources at USDA Departmental Administration (DA). The report identifies weaknesses in DA's ability to protect its critical information technology resources.

Your response to our draft report is included in its entirety in exhibit A, with excerpts incorporated in the findings and recommendations section of the report. Based on the information provided in the response, we have reached management decision for Recommendations Nos. 1, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, and 14. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer.

We concur with your proposed actions for Recommendations Nos. 2 and 5. However, to achieve management decision, you need to provide us with additional information. Please refer to the OIG Response sections of the report for specific details.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective actions taken or planned and the timeframes for implementation of the outstanding recommendations noted above. Please note that the regulation requires management decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance.

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

/s/

RICHARD D. LONG
Assistant Inspector General
for Audit

EXECUTIVE SUMMARY

SECURITY OF INFORMATION TECHNOLOGY RESOURCES AT USDA DEPARTMENTAL ADMINISTRATION

AUDIT REPORT NO. 23099-2-FM

RESULTS IN BRIEF

We identified weaknesses in the Departmental Administration's (DA) ability to adequately protect its (1) assets from potential fraud and misuse, (2) sensitive information from inappropriate disclosure, and (3) critical operations from potential disruptions. Information security weaknesses were identified during our review of DA's network and systems, including inadequately restricting access to sensitive data. This and other identified weaknesses place critical operations, as well as the assets associated with these operations, at high-risk. These material weaknesses were caused by a need for additional management oversight in this critical area. DA management did not ensure adequate policies and procedures were in place to verify that only authorized users had access to its information technology (IT) resources and did not adhere to the departmental and other Federally mandated IT security requirements. DA relies on its IT infrastructure and individual systems to preserve Privacy Act-protected data maintained by offices reporting to the Assistant Secretary for Administration such as the Office of Civil Rights, Office of Human Resources Management, Office of Administrative Law Judges, and Board of Contract Appeals.

To test the vulnerability of DA to security intrusions, we assessed the security of selected network components using a commercially available software product designed to identify risk indicators associated with various operating systems. DA personnel advised us they were using a software package similar to what we used to identify risk indicators; however, they had not consistently run the software against all of their computer systems. Our audit tests, performed between October 3 and October 12, 2001, on 191 network devices, identified 837 high and medium-risk IT security vulnerabilities[1] and 1,543 low-risk vulnerabilities.

During our review, we reported these weaknesses to DA management. In its response, DA management did not address the recommendations we

[1] 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.

made to eliminate the identified high and medium-risk vulnerabilities, or to implement a policy and establish controls to perform regular agency-wide assessments. DA officials later informed us that they had taken significant actions to eliminate the vulnerabilities, including patching its systems or removing the systems from its network.

We found that the DA needs to take additional measures to strengthen the management of its IT resources to ensure compliance with Federal requirements. We believe these problems, in aggregate, constitute a material internal control weakness. This weakness should be reported in the agency's Federal Manager's Financial Integrity Act report until corrected. DA has not:

- Conducted the necessary risk assessments of its networks as required by Office of Management and Budget (OMB) Circular A-130 and Presidential Decision Directive 63. Without risk assessments, DA cannot be assured that all the risks attributable to its mission critical systems are identified and that appropriate steps are taken to mitigate these risks;

- adequately documented network security in its security plan, prepared for potential service disruptions by developing comprehensive contingency plans, or certified to the security for its major systems as required by the OMB Circular A-130. Without adequate security plans, comprehensive contingency plans, and certifying system security, DA cannot be assured that it has sufficiently addressed its security needs and key operations can be quickly and effectively recovered to accomplish its mission in the event of an emergency;

- effectively documented change control processes over its major applications and various operating systems. Without proper software change controls, DA systems are at risk of processing irregularities that could occur or security features that could be inadvertently or deliberately omitted or rendered inoperable;

- addressed security in DA's Government Performance and Results Act performance measures. Without a security related performance measure, DA cannot adequately measure IT resources' security control effectiveness;

- removed separated employees' access authorizations from network and mission critical systems. We found user accounts hidden from the system administrator and inactive accounts that had not been disabled. We found that the intruder detection and auditing status settings were not turned on; and

- developed a configuration management program that ensured all systems are routinely updated with recent security patches and other software updates.

The types of weaknesses we disclosed make it possible for a malicious user to inappropriately modify or destroy sensitive data or computer programs or inappropriately obtain and disclose confidential information. In today's increasingly interconnected computing environment, inadequate access controls can expose an agency's information and operations to attacks internally or from remote locations by individuals with minimal computer or telecommunications resources and expertise.

KEY RECOMMENDATIONS

We recommended that DA:

- Update its agency security plan and prepare one for all major applications that complies with OMB Circular A-130 requirements including preparation of risk assessments and system certifications.

- Document comprehensive contingency plans and ensure backup files are stored offsite or in a fireproof safe for the network and each major application and initiate procedures for periodic testing of the contingency plan.

- Implement a change control process that includes key controls such as software change authorization, testing, and approval.

- Ensure corrective actions are taken on the vulnerabilities we identified.

- Routinely scan its entire network for vulnerabilities and track corrective actions to assure remediation.

- Strengthen controls to ensure procedures are followed to timely remove network and system access for separated employees and contractors.

- Develop, test and implement a configuration management program for DA's systems.

- Develop a policy limiting the use of modems to access DA systems, periodically test to ensure only approved modems are on DA's network, and ensure that approved modems are properly configured.

AGENCY RESPONSE

DA generally agreed with the Findings and Recommendations in this report.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

Information security, improving the overall management of information technology (IT) resources, and the transition to electronic business (e-government), are top priorities within the U.S. Department of Agriculture (USDA). 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. Threats range from those posed by insiders, and recreational and institutional hackers to attacks by intelligence organizations of other countries. Unless appropriate security is established these threats could jeopardize the integrity and confidentiality of the vast amount of Privacy Act-protected data maintained by the Office of Civil Rights, Office of Human Resources Management, Office of Administrative Law Judges, and Board of Contract Appeals.

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. Departmental responsibilities regarding information security were recently reemphasized in the Clinger-Cohen Act of 1996 and Presidential Decision Directive (PDD) 63, "Policy on Critical Infrastructure Protection." Additionally, the Government Information Security Reform Act (GISRA) was enacted on October 30, 2000; which essentially codifies the existing requirements of Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Resources." It also requires agencies to incorporate security into the life cycle of agency information systems, as well as requiring annual security program reviews, and annual reporting requirements.

Considerable guidance on information security has also been developed. The National Institute of Standards and Technology (NIST)[2] 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, October 1995, and "Generally Accepted Principles and Practices for Security Information Technology Systems," Special Publication 800-14, published in September 1996.

[2] The Computer Security Act of 1987 assigned NIST primary responsibility for developing technical standards and providing related guidance. Their responsibilities were reemphasized in the Clinger-Cohen Act of 1996.

Departmental Regulation (DR) 3300-1, "Telecommunications and Internet Services and Use," dated March 23, 1999, establishes policies and procedures, and assigns responsibilities for the management and use of all aspects of telecommunications services, equipment, and resources within the Department.

Departmental Administration (DA) uses a wide range of computers and telecommunication systems to process and manage its programs. Some of the data that is processed through these systems include sensitive and Privacy Act databases on civil rights program complaints, employee complaints, Government personnel, and other critical operations.

OBJECTIVES

The objectives of this audit were to (1) assess the threat of penetration of agency systems, (2) determine the adequacy of the security over the agency networks, (3) determine if adequate logical and physical access controls exist to protect computer resources, (4) evaluate the controls over the modifications of application software programs, (5) determine the adequacy of controls over access to and modification of system software, and (6) evaluate controls over commercial software programs and Government IT resources.

SCOPE

We tested the DA's Washington, D.C. computer network to identify vulnerabilities that could enable unauthorized users to access sensitive data stored on or transmitted over DA's systems. DA covers the Office of Civil Rights, Office of Administrative Law Judges, Office of Human Resources Management, Board of Contract Appeals, Office of Operations, Office of Procurement and Property Management, and a few other small agencies. We reviewed controls established on seven DA computer systems to ensure the integrity of the information security program. The sample selection of DA computer systems was based on the mission critical listing of systems identified by DA as top priorities or mission critical systems identified within DA's cyber security plan. According to DA, these systems would have the greatest impact on USDA's ability to deliver its programs.

We conducted this audit in accordance with "Government Auditing Standards" from May 2001 through October 2001.

METHODOLOGY

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

- We reviewed DA, departmental, and other Federally mandated IT security policies and procedures.

- We interviewed responsible DA officials managing the computer systems.

- We interviewed DA's mission critical system owners.

- We conducted vulnerability scans on several DA networks using commercially available operating system vulnerability software.

- We performed detailed testing of DA's entity-wide security program, both physical and logical access controls, application change controls, and service continuity by analyzing records and controls established to ensure the security of the DA's computer systems.

FINDINGS AND RECOMMENDATIONS

CHAPTER 1	DA HAS NOT ENSURED COMPLIANCE WITH FEDERALLY MANDATED SECURITY GUIDELINES AND IS LACKING IN ITS OVERALL MANAGEMENT OF INFORMATION TECHNOLOGY RESOURCES

FINDING NO. 1

DA needs to improve its management of IT resources, and ensure compliance with existing Federal requirements for managing and securing IT resources. Specifically, DA has not (1) conducted the necessary risk assessments of its networks, (2) adequately planned for network security and contingencies, (3) properly certified to the security of its major systems, (4) addressed security in the agency's Government Performance and Results Act (GPRA)[3] performance measures, or (5) documented system software change controls. We attribute these weaknesses to a need for additional management oversight. DA officials informed us that they were not aware of the requirements outlined in the OMB Circular A-130,[4] PDD 63,[5] and NIST 800-18[6] guidance. This guidance documents a framework for securing information systems and networks; therefore, DA's lack of compliance is a material internal control weakness. As a result, DA's network and the major applications that reside on that network may be vulnerable to an attack by malicious users, jeopardizing DA's ability to accomplish its mission.

OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," established a minimum set of controls for agencies' automated information security programs, including certifying to the security of any systems that maintain sensitive data, establishing contingency plans and recovery procedures in the event of a disaster, and establishing a comprehensive security plan. Further, PDD 63, "Policy on Critical Infrastructure Protection," requires agencies to assess the risks to their networks and establish a plan to mitigate the identified risks.

[3] GPRA, Public Law 103-62.

[4] OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," November 30, 2000.

[5] PDD 63, "Policy on Critical Infrastructure Protection," May 22, 1998.

[6] NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," December 1998.

Departmental Manual (DM) 3140-1[7] provides standards, guidelines, and procedures for the development and administration of automated data processing security programs. DM 3200-2.2[8] requires a change control process for all major application systems, which properly documents the change process including approval and acceptance of changes and testing the changes in a system test environment. In addition, the GPRA of 1993 requires annual performance plans to establish performance goals. Finally, GISRA[9] provides a comprehensive framework for establishing and ensuring the effectiveness of controls over IT resources that support Federal operations and assets.

Risk Assessments

DA has not performed an agency risk assessment or risk assessments of its seven major applications, as required by OMB Circular A-130, NIST 800-18,[10] and PDD 63. DA officials informed us that they were not aware of the requirement to prepare risk assessments. Risk assessments, as defined by OMB, are a formal, systematic approach to assessing the vulnerability of information system assets; identifying threats; quantifying the potential losses from threat realization; and developing countermeasures to eliminate or reduce the threat or amount of potential loss. Conducting a risk assessment is important to ensure that adequate, cost-effective security measures are included in DA's security plans. Without risk assessments, DA cannot be assured that all the risks attributable to its mission critical systems are identified and that appropriate steps are taken to mitigate these risks.

Security Plans

DA's security plan for its general support system does not meet all of the OMB Circular A-130 requirements, and did not conform to departmental Office of Chief Information Officer (OCIO) guidance for its preparation. Further, DA had not prepared a security plan for its seven major applications. DA's general support security plan was deficient in that it did not (1) address the areas of Continuity of Support and System Interconnection, (2) require management's written authorization for use of applications or re-authorization of the applications every 3 years, nor (3) address periodic review of security controls. DA officials informed us that they were not aware of the requirement that security plans were to be prepared for each of its major applications. DA needs to ensure that its security plans meet OMB guidelines and ensure that its security plans are communicated to the system users and administrators at all levels. Until

[7] DM 3140-1, "Management ADP Security Manual," Part 1 of 8, Section 1, July 19, 1984.

[8] DM 3200-2.2, "A Project Manager's Guide to Application Systems Life Cycle Management," Section 1.3.B (7)(a), (b), (d), and (8)(b), dated March 3, 1988.

[9] GISRA, Public Law 106-398, Title X, subtitle G, was enacted on October 30, 2000.

[10] NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," December 1998.

such steps are taken, DA cannot be assured that it has adequately addressed its security needs and that its security policies and practices have become an integral part of its operations.

Security Training

Our review disclosed that DA network security administrators had not received security training until after we started inquiring about training records. In addition, only about three percent of the DA's staff received some type of system security-related training since October 1, 2000. Federal guidelines[11] direct agencies to provide mandatory training for current and new employees. Training is also required whenever there is a significant change in the agency's IT security environment or procedures, or when an employee enters a new position that involves sensitive information. Further, periodic refresher training should be provided, based on the sensitivity of the information the employee handles. OMB Circular A-130[12] reinforces these requirements that all individuals be appropriately trained in how to fulfill their security responsibilities prior to being granted access to IT resources and provided periodic refresher training. DR 3140-1,[13] "USDA Information Systems Security Policy," also requires agencies to ensure that information systems security requirements, procedures, and practices are included in computer security training material, to provide new employees an orientation outlining security responsibilities, and to provide training to employees on a regular basis. IT trends and their evolving security implications have become too complex to be successfully achieved by individuals lacking a comprehensive set of competencies. Hence, without appropriate training, DA personnel are unable to fulfill their security responsibilities which has contributed to ineffective implementation of logical access controls identified in Finding No. 3, as well as, the lack of management control and oversight in completing Federal and departmental mandated requirements.

Background Checks

We identified two network system administrators that have not yet undergone background checks. OMB Circular A-130[14] requires that the agency "screen individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause. Such screening shall occur prior to an individual being authorized to bypass controls and periodically thereafter." Without proper background checks on its trusted

[11] The Computer Security Act of 1987, Public Law 100-235, Section 5, dated, January 8, 1988, and NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998, Chapter 1.1.
[12] OMB Circular A-130, Appendix III, Section A.3.(a)(2)(b), November 30, 2000.
[13] DR 3140-1, "USDA Information Systems Security Policy," Section 12, May 15, 1996.
[14] OMB Circular A-130, Appendix III, Section A.3.(a)(2)(c), November 30, 2000.

users, DA does not have assurance that those users can be entrusted with the network resources and data under its control.

Contingency Plans and Backup/Recovery Plans

DA did not prepare contingency plans for the agency or for its seven major applications, and did not properly store system backup files for a mission-critical system. We found that DA did not store backup files for a facility security management system offsite, or in a fireproof safe because of a lack of management control. After we identified this deficiency, the security official agreed to purchase a fireproof safe to store system backups. The security management system is used to monitor access, security, and alarms in the Agriculture building complex. If faced with an emergency, physical security to the Agriculture building complex could be compromised. DA officials later informed us that they had purchased three fireproof safes for the storage of backup tapes and that those tapes are rotated on a regular basis.

DM 3140-1.8[15] requires that data files be backed-up frequently and stored off-site or in a secured environment. OMB Circular A-130[16] requires that agencies plan for how they will continue to perform their mission or recover from the loss of application support in the event of a system failure. While contingency plans can be written to make a distinction between the recovery from system failure and recovery of business operations, our reliance on information technology makes the return to manual processing an unrealistic option to disaster recovery. For this reason, DA should have procedures in place to protect information resources and minimize the risk of unplanned interruptions, and establish a plan to recover critical operations should interruptions occur.

DA's network and key operations involve a vast amount of Privacy Act-protected data maintained by the Office of Civil Rights, Office of Human Resources Management, Office of Administrative Law Judges, and Board of Contract Appeals. Without well-thought-out contingency plans and adequate backup procedures, DA cannot be assured that its network and key operations can be quickly and effectively recovered to accomplish its mission in the event of an emergency.

System Certification/Authorization

DA had not ensured that any of its seven major applications were certified in accordance with OMB Circular A-130. DA has not reviewed computer security internal control weaknesses, nor considered identifying computer security deficiencies for its seven major applications in its Federal

[15] DM 3140-1.8, "Management ADP Security Manual," Part 8 of 8, Section 6, Part j, July 19, 1984.
[16] OMB Circular A-130, Appendix III, Section B.4.(b)(2)(d), November 30, 2000.

Manager's Financial Integrity Act (FMFIA) report. OMB Circular A-130[17] states that agencies should perform an independent review or audit of the security controls in each application at least every 3 years. Without adequate certification/authorization of DA's mission critical systems, DA cannot be assured that adequate security controls have been established for these systems and controls operate effectively.

Performance Measures

The GPRA of 1993 requires annual performance plans to establish performance goals. The GPRA provides a comprehensive framework for establishing and ensuring the effectiveness of controls over IT resources that support Federal operations and assets.

DA established a performance goal to "Provide effective LAN and desktop computer support to DA customers: To provide virtually uninterrupted network access to all DA employees with 95 percent network uptime." DA's performance goal does not address IT resource security. Based on the issues identified in this report, DA should implement a GPRA performance measure relating to improving its IT security.

Change Controls

DA has not properly documented the change control process of its major applications and various operating systems software. DA did not have official policies requiring changes to be documented and DA did not follow departmental system life cycle guidance. Controls over access to and modification of software are essential in providing reasonable assurance that system-based security controls are not compromised. As a result, DA lacks assurance that major applications will perform as intended and that management controls will adequately safeguard the integrity of these applications.

DM 3200-2.2[18] states that all major application systems must use a change control process and properly document the process and the changes made by it. A procedure must exist for approval and acceptance of changes and the changes must be tested in a system test environment. An effective change control process includes control points such as (1) a formal change control procedure, (2) centralized review and approval of change requests, and (3) testing of changes.

DA's Information Resources Division (IRD) is responsible for upgrading software, installing patches, modifying user interfaces, and adding and/or deleting user accounts. We found that IRD did not have a formal change

[17] OMB Circular A-130, Appendix III, Section A.3.(b)(3) and (4), November 30, 2000.

[18] Department Manual 3200-2.2, 1.3.B(7)(a), (b), (d), dated March 3, 1988.

control procedure in place. For example, network software changes were made when the system administrator noted the availability of software upgrades and new software patches. DA did not maintain documentation of changes made to its router and switch configuration settings, nor did it document supervisory approval of system changes or tests of these changes before implementation. Without proper software change controls, DA's systems are at risk that (1) security features could be inadvertently or deliberately omitted or rendered inoperable, (2) processing irregularities could occur, or (3) malicious code could be introduced.

Due to the deficiencies we identified, DA cannot assure the integrity and confidentiality of the Privacy Act-protected data maintained by the Office of Civil Rights, Office of Human Resources Management, Office of Administrative Law Judges, and Board of Contract Appeals. DA needs to take the necessary steps to ensure its compliance with OMB Circular A-130 and Department requirements relating to security plans, contingency plans, risk assessments, and contingency/disaster recovery plans, and change controls.

RECOMMENDATION NO. 1

Require DA IT officials to prepare an overall plan to address the significant issues identified in this report such as system security plans and contingency plans. Require monthly status reports to the OCIO until these weaknesses are corrected.

DA Response

DA stated that it is preparing an overall plan to address the significant issues identified in the OIG report. DA will implement short-term remedial actions immediately with long term issues being incorporated into its IT security policy and procedural guidance. DA estimates complete development and approval to finalize and implement its IT security policy by August 15, 2002. DA intends to update the table provided in its response on a monthly basis to submit to the OCIO.

OIG Position

We concur with the management decision.

RECOMMENDATION NO. 2

Provide training to IT officials so they are aware of governmental and departmental IT security and other requirements.

DA Response

DA stated that it will provide IT officials with security awareness training after approval of its security policy and procedural guidance. DA intends to complete its security policy and procedural guidance by August 15, 2002.

OIG Position

To reach management decision, DA needs to provide us its timeframe for completing security awareness training to its IT officials.

RECOMMENDATION NO. 3

Establish performance goals and measurements relating to information technology security and ensure reporting of security weaknesses in its FMFIA report.

DA Response

DA stated that it will establish performance goals and measurements relating to information technology security by June 15, 2002. DA stated that it will review its progress and determine reporting of security weaknesses in its FMFIA report by December 1, 2002.

OIG Position

We concur with the management decision.

RECOMMENDATION NO. 4

Develop policies requiring major application and general system changes be documented according to DM 3200-2.2. Implement procedures that include key controls such as software change authorization, testing, and approval.

DA Response

DA stated that it has initiated an IT security policy and procedural guidance project. This policy will address system security controls, certification and accreditation, and configuration management. DA stated that compliance with DM 3200-2.2 and other guidance will be assured. IT security procedural guidance will be developed to assist program offices in development of procedures including these key controls. DA estimates completion of these policies and procedures by August 15, 2002.

OIG Position

We concur with the management decision.

CHAPTER 2	VULNERABILITIES EXPOSE DA'S SYSTEMS TO THE RISK OF MALICIOUS ATTACKS

FINDING NO. 2

Our vulnerability scans disclosed weaknesses in DA's system security administration. We found that (1) scans of selected DA systems disclosed a large number of risk indicators that could be exploited from both inside DA's networks, and externally, and (2) system policy settings did not provide for optimum security and were not uniform throughout DA. These weaknesses were caused by a need for additional management oversight in this critical area. DA had not taken sufficient actions to identify and eliminate security vulnerabilities within its systems, even though we identified similar vulnerabilities on DA's network during a prior IT security audit.[19] DA acquired similar scanning tools and officials stated that they scanned selected servers on their network on a weekly basis; however, DA did not aggressively use the scan results to eliminate network vulnerabilities. As a result, DA's systems and networks are vulnerable to cyber-related attacks, jeopardizing the integrity and confidentiality of the Privacy Act-protected data maintained by the Office of Civil Rights, Office of Human Resources Management, Office of Administrative Law Judges, and Board of Contract Appeals. This is a material internal control weakness.

OMB Circular A-130[20] requires agencies to assess the vulnerability of information system assets, identify threats, quantify the potential losses from threat realization, and develop countermeasures to eliminate or reduce the threat or amount of potential loss.

We assessed selected DA networks, including the DA Local Area Networks (LAN) at Washington, D.C. and the DA DMZ[21] servers during October 3 through October 12, 2001. We used 3 commercially available software products, 1 designed to identify over 950 vulnerabilities associated with various operating systems that use Transmission Control Protocol/Internet Protocol (TCP/IP),[22] 1 that tests system policy settings in Novell networks, and another that searches for modems within a set of telephone numbers to identify potentially unsecured carrier lines.

[19] Report No. 50099-27-FM, "Security of USDA Information Technology Resources," dated March 30, 2001.

[20] OMB Circular A-130, Appendix III, Section B, November 30, 2000.

[21] DMZ servers are public access servers located outside the departmental firewalls.

[22] 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.

TCP/IP System Vulnerabilities

We conducted vulnerability scans of 191 DA network components. Our assessments revealed 837 high and medium-risk vulnerabilities.[23] In addition, we identified 1,543 low-risk vulnerabilities. The high and medium-risk vulnerabilities, if left uncorrected, could allow unauthorized users access to critical and sensitive DA data. Additionally, the large number of low-risk vulnerabilities identified indicates that DA needs to strengthen its system administration. Although DA has acquired similar scanning tools, DA was not aggressively using them to eliminate network vulnerabilities.

We identified similar vulnerabilities on DA's network during a prior IT security audit.[24] That audit found that two DA systems had weak administrator-level passwords. At that time, we recommended and DA agreed, that it should take a more proactive role in maintaining those systems. Considering the severity and the significant number of potential vulnerabilities identified in our current review, we considered DA's actions to be ineffective and reflective of the need to develop a substantially improved IT security program in DA.

Detailed below are examples of the high-risk vulnerabilities disclosed during our DA scans:

- Windows NT machines were not properly secured because some contain either blank administrator passwords, or have been assigned easily guessed passwords. The administrator is the most trusted user on a Windows NT system; therefore, the administrator has complete control over the computer and can perform any function. This could allow an attacker to obtain, or possibly alter, the information being stored on DA networks.

- A software utility used to manage the network was left configured with the original default settings, which are well known by attackers. This could allow an attacker to easily obtain or change system information, and gain information about open connections with other DA systems.

- An error in the system's log could allow an attacker to run programs, including malicious code, and disguise them as having full administrative privileges. For instance, an attacker could execute some type of Trojan horse virus or denial of service program that could cause substantial harm to data and/or systems.

[23] 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.

[24] Report No. 50099-27-FM, "Security of USDA Information Technology Resources," dated March 30, 2001.

- Configuration problems existed which allow automatic logon and readable system user passwords. As a result, an attacker could execute commands to freely access a system and take over or destroy any critical or sensitive information maintained on the systems.

Our scans further supported that DA had not developed a configuration management program for its systems. We identified servers and workstations that did not have recent security patches and updates. A configuration management program ensures that all systems are routinely updated with recent security patches and other software updates. We believe a system configuration management program, along with regularly scheduled vulnerability assessments on all DA resources and remediation of the risks discovered, would substantially enhance the security of DA's computer systems.

We issued a management alert to DA management to report the weaknesses we identified, and made recommendations necessary to mitigate the vulnerabilities. In its response, DA management did not address the recommendations we made to eliminate the high and medium-risk vulnerabilities identified, or to implement a policy and establish controls to perform regular agency-wide assessments. Instead, DA questioned our assessments and asserted that the seriousness of DA's security problems were overstated. DA offered explanations, which it said, minimized the significance of the cited vulnerabilities, and it chose to ignore our identification of significant known vulnerabilities on its systems. DA asserted that because our scans were conducted from inside the DA network, our assessments ignored other security mechanisms DA had in place, such as firewalls and access control lists. While DA's agencies' systems are behind the Department's firewalls, these firewalls should not be DA's only defense against commonly known vulnerabilities. Recently issued NIST guidance[25] recommends that the implementation of a firewall should not preclude agencies from patching their systems.

DA's response also pointed out that our management alert did not take into account that the scanning software sometimes reports the potential existence of vulnerabilities that do not exist, known as "false positives." OIG recognizes that the software can report false positives; however, it has been our experience that there are relatively few false positives in the high and medium-risk categories. The effort expended to ensure appropriate security measures are in place, is worth the alternative of these conditions running uncorrected and being exploited. If DA's IT management has identified false positives, they simply needed to inform us of this fact along with reporting to us the conditions present making the vulnerabilities false.

[25] NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy," dated January 2002.

Further, DA's response pointed out that the vulnerabilities we identified in the prior audit were on two print servers that contain no critical DA data and; therefore, pose a minimal-risk. We disagree with this position. The two systems in question had weak administrative passwords, making it very easy for malicious software to be installed on those systems, or for those systems to be used as an access point to other systems within the DA network.

Novell System Policies

We also conducted a detailed assessment of the security of the DA's Novell networks. Our assessment software allowed us to compare the DA's security practices to the actual settings on the Novell systems. We were also able to compare each system's security settings to the software product's "best practices," which are based on standard practices from a wide variety of Government and private institutions. The software product reports weaknesses that may leave the system open to potential threats in the following areas (1) account restrictions, (2) password strength, (3) access control, (4) system monitoring, (5) data integrity, and (6) data confidentiality.

Our assessments disclosed that the majority of weaknesses on DA's Novell systems were in the account restrictions, password strength, and access control, the areas that define a user's ability to access the system.

Examples of where DA policies did not meet best practices follow:

- User accounts were hidden from the system administrator. A malicious user can use hidden accounts as a means to set up an unauthorized access account to the server. Some of these accounts hold administrator access privileges, which are the most trusted users on a Novell system and allow complete control of the system. Additionally, because of these privileges, unauthorized users can modify system logs to hide their activities from the system administrator.

- Inactive accounts had not been disabled. User accounts that become inactive, but are not disabled, provide opportunities for unauthorized users to gain access to the network. An attacker can try different passwords on these inactive accounts and attempt to gain access to the network. Once that access is gained, unauthorized activity cannot be traced to the responsible person.

- Minimal account lockout time-set does not meet best practices. This setting defines how long a user's account is locked after attempting to log into the system with a bad password. If this setting is too short it can adversely affect the security of the system by allowing an attacker to try numerous passwords on that account in an attempt to gain access.

- The number of grace logins exceeded best practices. This setting defines how many times a user can attempt to login after their password has expired before the system locks that user's account. This setting helps strengthen system security by limiting the number of times a user can login using an expired password before the system requires the user to change their password.

In addition to the above policy settings, we found indicators of inadequate system administration. For instance, we found that the agency had failed to disable about 92 percent (154 of 168) of the inactive user accounts or set expiration dates on 96 percent (161 of 168) of the inactive user accounts, so the system would automatically disable them. We identified 67 user accounts that had never been accessed and 59 of these accounts were still active. We discovered that 69 percent of users are not required to use minimum password lengths. We found that the intruder detection and auditing status settings were not turned on. All of these policies could lead to exposing any sensitive data to unnecessary risk, as well as make it easier for an unauthorized user to potentially gain access to the systems without being detected. Further, no record of what was accessed or changed would be available. Systematically scanning security vulnerabilities of DA's network components would help mitigate internal exposures.

Modem Security

We conducted a detailed assessment of DA's telephone system to identify active modems on its network. Modems provide a back door to agency systems and can undermine existing security practices. Our assessment software allowed us to test over 1,200 DA telephone numbers to identify areas of inadequate security over modems on its telephone network. DA's 2001 Information Cyber Security Plan states that all modems were configured for dial-out only; however, our assessment software identified six telephone numbers which it identified modems with dial-in capabilities. Therefore, DA's system administrator had not ensured that the modems were configured properly. The presence of unauthorized modems attached to computers on its networks can undermine a well-thought-out security plan. If a computer with an unauthorized modem is connected to an organization's network, anyone with minimal computer skills and malicious intent can use the unsecured modem as a back door into the network.

In addition, DA officials were not able to readily provide a complete listing of modem telephone numbers. Active modems provide a gateway into the agency's network by converting digital and analog signals for transmission between components. DR 3140-1,[26] "USDA Information System Security Policy," Section 16, requires agencies to evaluate security measures in place on network gateways. DR 3140-2,[27] "USDA Internet Security Policy," Section 6.1, mandates vulnerability and risk assessments of existing gateways at an annual interval. The lack of a comprehensive modem listing by DA indicates lack of control over network gateways and non-compliance with departmental requirements.

RECOMMENDATION NO. 5

Ensure that necessary corrective actions were taken on all high and medium-risk vulnerabilities identified during our audit. Require IT officials to track each vulnerability and certify that actions have been taken to remedy the problem for all vulnerabilities identified by OIG.

DA Response

DA has fixed the high vulnerabilities and verified correction by scanning its systems. DA stated that it will monitor vulnerabilities on an ongoing basis and take corrective actions immediately.

OIG Position

While not as invasive, medium-risk vulnerabilities could lead to the exploitation of higher-risk vulnerabilities. In order to reach management decision, DA needs to inform us of its actions and timeframes for addressing the medium vulnerabilities we identified on its systems.

RECOMMENDATION NO. 6

Require IT officials to scan DA's entire network on a routine basis and take prompt action to eliminate noted vulnerabilities. Establish a comprehensive plan that will assure effective testing of DA's network so that sensitive data is safeguarded.

DA Response

DA stated that routine scan procedures have been established for the DA network, and that the security controls section of its security policy and procedural guidance will address network testing. DA estimates

[26] DR 3140-1, "USDA Information Systems Security Policy," Section 16, May 15, 1996.
[27] DR 3140-2, "USDA Internet Security Policy," Section 6.1, March 7, 1995.

completion of its security policy and procedural guidance by August 15, 2002.

OIG Position

We concur with the management decision.

RECOMMENDATION NO. 7

Develop a policy establishing minimum security setting guidelines for the various operating systems used by DA. Periodically assess those settings and correct those that have been misapplied.

DA Response

DA stated that it has initiated development of IT security policies. IT security procedural guidance will follow the approval of the policy. The security controls section of the policy and guidance documents will address security setting guidelines. DA estimates completion of its security policy and procedural guidance by August 15, 2002.

OIG Position

We concur with the management decision.

RECOMMENDATION NO. 8

Enable the auditing function on its network servers.

DA Response

DA stated that it enabled its network's audit function on April 30, 2002. DA will also address audit function and audit trails in its IT policy and procedural guidance. DA estimates completion of its security policy and procedural guidance by August 15, 2002.

OIG Position

We concur with the management decision.

RECOMMENDATION NO. 9

Require IT officials to develop and follow a configuration management program for DA's systems. Assure periodic tests are made to ensure that the plan is in place and operating effectively.

DA Response

DA stated that it has initiated the development of an IT security policy. IT security procedural guidance will follow the approval of the policy. The security controls section of the policy and guidance documents will address configuration management guidelines. These guidelines will include requirements for periodic testing. DA estimates completion of its security policy and procedural guidance by August 15, 2002.

OIG Position

We concur with the management decision.

RECOMMENDATION NO. 10

Develop a policy that limits the use of modems to access DA systems. Periodically conduct tests to ensure that only approved modems are on its network and that approved modems are properly configured.

DA Response

DA stated that the security controls section of its policy and guidance documents will address logical access control guidelines. DA estimates completion of its security policy and procedural guidance by August 15, 2002. DA further stated that all authorized modems are dial-out only and that other modems have been blocked. DA will conduct periodic testing to verify that modem access is appropriately limited and that approved modems are properly configured.

OIG Position

We concur with the management decision.

CHAPTER 3	WEAK ACCESS CONTROLS JEOPARDIZE THE INTEGRITY AND CONFIDENTIALITY OF DA'S CRITICAL DATA

FINDING NO. 3

DA has inadequate internal controls in place over access to IT resources. DA did not (1) remove separated employees from network and a mission critical systems, (2) follow the Department's or its own employee exit procedures, or (3) configure the network's operating system according to departmental policies and procedures. We attribute this weakness to a lack of management oversight. DA did not have adequate procedures in place to ensure that only authorized users had access to its IT resources. In today's increasingly interconnected computing environment, inadequate access controls can expose an agency's information and operations to attacks from remote locations by individuals with minimal computer or telecommunications resources and expertise. As a result, confidential DA systems are vulnerable to potential fraud and misuse, inappropriate disclosure, and potential disruption.

OMB Circular A-130[28] stresses management controls affecting users of information technology. These controls help to protect operating systems and other software from unauthorized modification and to protect the integrity, availability, and confidentiality of information by restricting the number of users, and provide protection from disclosure of information to unauthorized individuals. DM 3140-1.6[29] requires security staff to remove employee user identifications (ID) and passwords when the employee is no longer with the agency.

Logical Access Controls

DA had not periodically reconciled user accounts on its systems to a list of current employees and contractors. We identified 251 active network user accounts that were not traceable to DA's current employee, separated employee, or contractor listings. We identified 29 separated employees that still had active network accounts and 36 separated employees that still had active Civil Rights' employee complaint system user accounts. Complicating the identification of valid user accounts was the fact that DA management did not maintain a listing of contractors it employed. We also determined that the Office of Civil Rights had a practice of keeping a separated temporary employee's user account active. This account was used for a future employee hired to fill the separated temporary employee's position; thereby, eliminating internal access control

[28] OMB Circular A-130, Appendix III, Section A, November 30, 2000.

[29] DM 3140-1.6, part 6 of 8, Section 6c, "Management ADP Security Manual," July 19, 1984.

procedures. We consider this problem a significant internal control weakness.

Logical access controls can prescribe not only who or what is to have access to a specific system resource, but also the type of access permitted. Logical access controls such as user names, passwords, and access permissions, ensure that only authorized users have access to network resources, and users are granted only the access needed to conduct their job responsibilities.

DA Instruction 400-1, "Issuance of Employee Exit Clearance Procedures," requires that an agency notify the IRD or the helpdesk when an employee separates so network or system access can be terminated. On a quarterly basis, the IRD provides a listing of inactive user IDs to each agency's resource manager to identify accounts that should be terminated. We noted that 10 of the separated employees with active user IDs left the agency more than 6 months before our review.

We also noted that DA had not limited network logon attempts to three attempts or set the maximum password life for network access to 90 days, as required by the DM.[30] DA also did not configure the network operating system properly. DA configured the operating system to allow six logon attempts before dropping the connection, and passwords were set to expire in 180 days. As a result, DA is not in compliance with its own policy, making its network vulnerable to intrusion.

Further, DA had not configured its network servers to track employee accesses to its systems. System auditing would provide management with valuable information about activity on its computer systems, including a review and analysis of management, operational, and technical controls. OMB Circular A-130[31] states that identifying and authenticating system users, and subsequently tracing actions on the system to the users who initiated them, normally accomplishes accountability. In addition, DM 3140-1.3, "Management ADP Security Manual," Part 3 of 8, Section 16, requires maintaining access logs sufficient to permit reconstruction of events in case of unauthorized data or program access or use. DA did not use audit logs to capture system activity audit trails; therefore, system administrators could not be assured that hackers, insiders, or technical problems had not harmed system resources.

[30] DM 3140-1.6, "Management ADP Security Manual," Part 6 of 8, Appendix D, Amendment 6, sections 5 and 6b, July 19, 1984.
[31] OMB Circular A-130, Appendix III, Section B (a)(2)(c), November 30, 2000.

RECOMMENDATION NO. 11

Strengthen controls to ensure procedures are followed to timely remove network and system access for separated employees and contractors. Those procedures should include a requirement to periodically reconcile authorized network and systems users to DA employees and contractors, and immediately remove those that no longer need access.

DA Response

DA stated that it has removed network and systems access of former employees identified in the OIG audit. DA stated that its security controls section of its policy and guidance documents will address identification and authentication as well as logical access control guidelines. DA estimates completion of its security policy and procedural guidance by August 15, 2002. DA stated that it is investigating password management software that that will periodically pull encrypted passwords from the system and run password checker against passwords. DA will also investigate the use of third party software to force user selection of passwords.

OIG Position

We concur with the management decision.

RECOMMENDATION NO. 12

Immediately remove network and system access for the former employees identified in this report who are no longer DA or UDSA employees.

DA Response

DA stated that by March 28, 2002, they had removed the network and system access for the former employees we identified. DA also stated that the security controls section of the policy and guidance documents currently under development will address identification and authentication as well as logical access control guidelines. DA estimates completion of its security policy and procedural guidance by August 15, 2002.

OIG Position

We concur with the management decision.

CHAPTER 4 IMPROVEMENTS ARE NEEDED IN DA'S MANAGEMENT AND CONTROL OF COMMERCIAL SOFTWARE AND ILLEGAL OR INAPPROPRIATE USE OF GOVERNMENT RESOURCES

FINDING NO. 4

DA needs to improve its management and control of commercial software and internal controls of Government computers and networks. We found commercial software programs installed on workstations for which applicable purchase documents or other acceptable license evidence was not available. We identified instances where users inappropriately used DA IT resources. This occurred because DA management (1) had not developed policies for installing software on Government equipment, (2) had not enforced DRs on the use of telecommunications equipment and services, and (3) had not monitored its employees' and contractors' usage to ensure that they adhered to the departmental requirements in conducting official USDA business. As a result, DA's network and major applications may be vulnerable to intrusion, and DA's IT resources' security may be compromised. Additionally, DA may expose the Department to copyright infringement issues if it continues to allow its users to download or use inappropriately licensed software.

Department Regulation (DR) 3130-2, "Microcomputer Policy," section 10e, dated August 18, 1986, states that agencies will establish a means to manage automated data processing, computer software, and related files effectively in the highly distributed microcomputer environment. DR 3140-1[32] states that users and contractors will (1) comply with all software licensing agreements, (2) not make illegal copies of software, and (3) not use USDA computers for personal gain.

Inadequate Commercial Software Controls

DA's controls were not adequate to ensure that only appropriate and/or licensed commercial software was available on DA workstations. We reviewed 20 workstations in offices at DA, Office of Civil Rights, Office of Operations, Office of Ethics, and Office of Human Resource Management. We found discrepancies at each office we visited. We identified 82 software applications and requested a license for each application. After several requests, DA provided software license agreements, purchase records, and/or justification for only 19 of the 82 software applications. DA was not able to provide software purchase records, software license agreements, or any other form of documentation for the remaining 63 applications. Of the 82 software applications, we identified 28 applications that are inappropriate for use on Government computers, including online

[32] DR 3140-1, Sections 10p, 13d, and 13e, May 15, 1996.

messaging services and personal finance software. During the course of our review, DA's Office of Civil Rights informed us that they had removed the illegal copies of the software we identified from its workstations.

DA officials did not have an inventory of commercial software readily available on their resources. DA officials stated that they had not performed any reviews to ensure that their resources complied with commercial licensing agreements.

Unauthorized Use of Government Computer Resources

We found 11 users within the DA network were engaged in downloading software, music, graphics, or videos that are protected by copyright laws. In four instances, users downloaded pornography. Some of these users were using a number of "Peer to Peer," file sharing software products that are available on the Internet. These programs give users the ability to search for, send, and receive files. They also can make the network vulnerable to intrusion; therefore, compromising network security.

RECOMMENDATION NO. 13

Establish procedures to account for, periodically reconcile, and remove unlicensed and inappropriate applications.

DA Response

DA stated that as of March 28, 2002, it has completed an inventory of corporate software and will centrally maintain that inventory. In its response to Recommendation No. 14, DA also stated that it's IT security procedural guidance will address rules of behavior, and that it will instruct help desk personnel to review all desktop computers for unauthorized software. DA will include these procedures in its IT security policy manual which it anticipates completion by August 15, 2002.

OIG Position

We concur with the management decision.

RECOMMENDATION NO. 14

Develop and implement internal controls sufficient to comply with personal use of Government equipment as directed in DR 3300-1, "Telecommunications and Internet Services and Use," dated March 23, 1999.

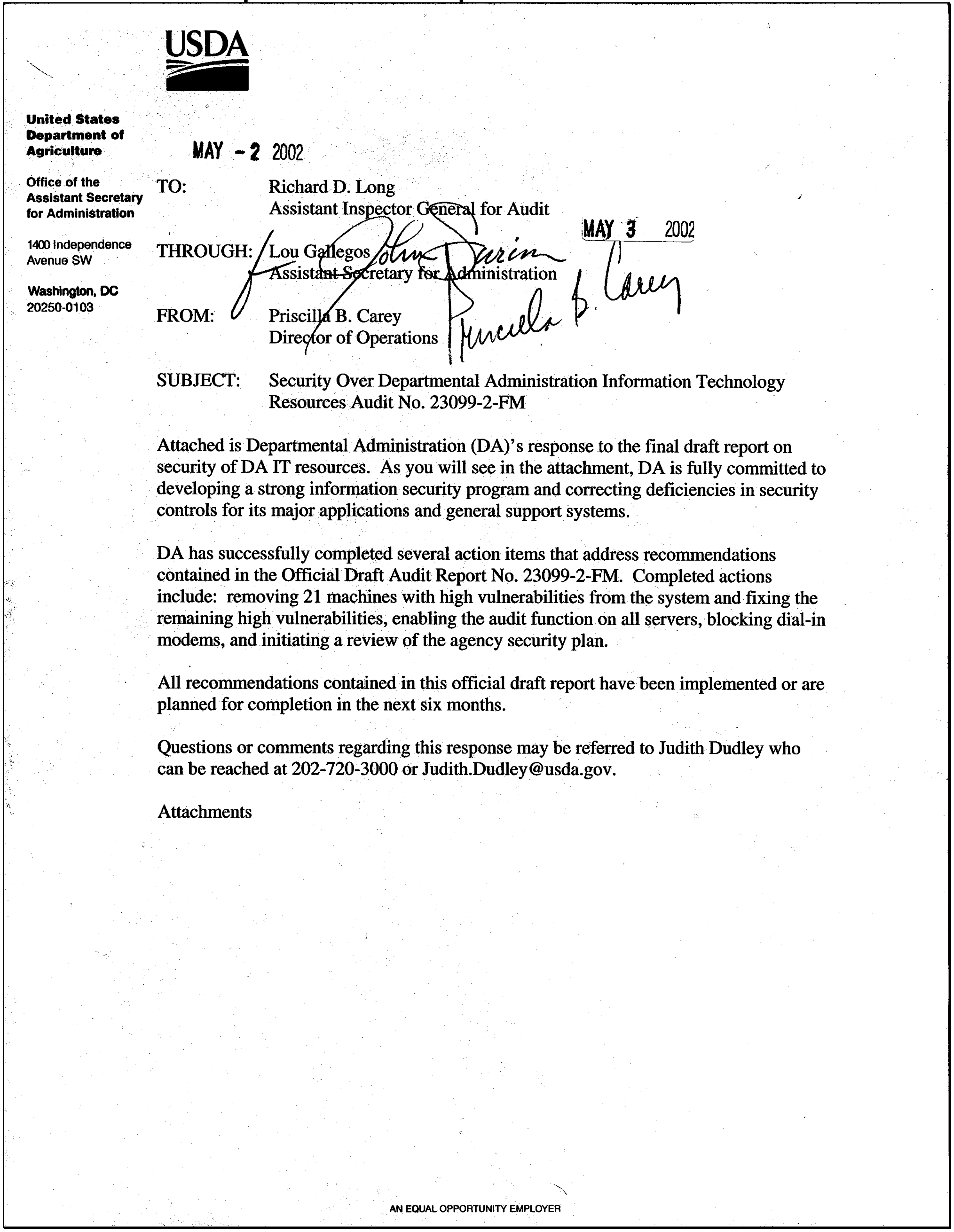
DA Response

DA stated that as of March 28, 2002, it has already blocked several types of illegal usage of its computer systems. DA also stated that it will immediately prepare rules of behavior for all DA systems which address unauthorized or inappropriate use of DA systems. DA stated that it will instruct help desk personnel to review all desktop computer for unauthorized software before instituting repairs or responding to requests for assistance. DA will include these procedures in its IT security policy manual which it anticipates completion by August 15, 2002.

OIG Position

We concur with the management decision.

EXHIBIT A – DA Response To Draft Report



USDA

United States Department of Agriculture

Office of the Assistant Secretary for Administration

1400 Independence Avenue SW

Washington, DC 20250-0103

MAY - 2 2002

TO: Richard D. Long
Assistant Inspector General for Audit

MAY 3 2002

THROUGH: Lou Gallegos
Assistant Secretary for Administration

FROM: Priscilla B. Carey
Director of Operations

Priscilla B. Carey

SUBJECT: Security Over Departmental Administration Information Technology Resources Audit No. 23099-2-FM

Attached is Departmental Administration (DA)'s response to the final draft report on security of DA IT resources. As you will see in the attachment, DA is fully committed to developing a strong information security program and correcting deficiencies in security controls for its major applications and general support systems.

DA has successfully completed several action items that address recommendations contained in the Official Draft Audit Report No. 23099-2-FM. Completed actions include: removing 21 machines with high vulnerabilities from the system and fixing the remaining high vulnerabilities, enabling the audit function on all servers, blocking dial-in modems, and initiating a review of the agency security plan.

All recommendations contained in this official draft report have been implemented or are planned for completion in the next six months.

Questions or comments regarding this response may be referred to Judith Dudley who can be reached at 202-720-3000 or Judith.Dudley@usda.gov.

Attachments

AN EQUAL OPPORTUNITY EMPLOYER