USDA

U.S. Department of Agriculture

Office of Inspector General
Southeast Region

Audit Report

Management and Security of Office of Budget and Program Analysis Information Technology Resources

Report No. 39099-1-AT
January 2004

USDA

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: January 12, 2004

REPLY TO
ATTN OF: 39099-1-At

SUBJECT: Management and Security of Office of Budget and Program Analysis Information Technology Resources

TO: Stephen B. Dewhurst
Director
Office of Budget and Program Analysis

ATTN: Larry Wachs
Associate Director
Office of Budget and Program Analysis

This report presents the results of our audit of the management and security of the Office of Budget and Program Analysis' (OBPA) information technology (IT) resources. Our assessment identified vulnerabilities, which could have allowed an attacker to gain access to the OBPA network.

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 and 10. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer.

To reach management decision for the remaining recommendations, we need additional information, generally, detailed corrective plans and timeframes for implementation. Please refer to the OIG Position 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.

Robert W. Young
ROBERT W. YOUNG
Assistant Inspector General
for Audit

Attachment

Executive Summary

Management and Security of Office of Budget and Program Analysis Information Technology Resources (Audit Report No. 39099-01-At)

Results in Brief

This report presents the results of our audit of the management and security of the Office of Budget and Program Analysis (OBPA) information technology (IT) resources. OBPA relies on its IT infrastructure to track legislation and regulations, to communicate and coordinate budget information, and selected program analysis.

To test the vulnerability of OBPA to the threat of internal and external intrusions, we conducted an assessment of the OBPA networks, using commercially available software, which is designed to identify vulnerabilities associated with various operating systems. Our assessment identified 1 high--and 27 medium-risk IT vulnerabilities[1] and numerous low-risk vulnerabilities. These vulnerabilities could have allowed an attacker to gain access to the OBPA network. The high- and medium-risk vulnerabilities that we discovered at OBPA are significantly lower than the vulnerabilities found at other agencies. During our fieldwork, OBPA officials advised us that they took immediate action to implement the changes and enhancements necessary to resolve each of the high- and medium-risk vulnerabilities we identified.

We found that OBPA needs to improve its management of IT resources and ensure compliance with existing Federal requirements for managing and securing IT resources. OBPA has not (1) documented the necessary risk assessments of their network, (2) adequately planned for network security and contingencies, or (3) properly certified to the security of their systems. This occurred because OBPA management has not placed a priority on implementing and documenting Office of Management and Budget (OMB) Circular A-130 requirements such as risk assessments, security plans, contingency planning, and system certifications.

Our audit disclosed that OBPA needs to strengthen its access controls to protect against unauthorized access. Logical and physical controls are not adequate because detailed risk assessments of the controls have not been accomplished. Logical controls such as alphanumeric passwords are needed. Also, physical controls such as locks on cabinets that protect network switches are needed. Without additional controls, IT resources are not adequately protected against incidental or intentional damage. We evaluated the controls over the modification of application software programs and the

[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.

adequacy of controls over access to and modification of system software. Our evaluation disclosed no weaknesses in these controls.

The type of weaknesses we found in our audit made it possible for a person to inappropriately modify or destroy data or computer programs or inappropriately obtain and disclose confidential information. In today's increasingly interconnected computing environment, inadequate access controls can expose agency information and operations to attacks from remote locations by individuals with minimum computer or telecommunications resources and expertise.

Recommendations in Brief

We recommend that OBPA take corrective action on the vulnerabilities identified. Also, document risk assessments to determine the vulnerability of system assets and countermeasures to eliminate or reduce the threat of potential loss.

We recommend that written plans for contingencies, and system certifications be created as required by OMB Circular A-130.

Finally, we recommend that logical and physical controls be implemented to strengthen security over IT assets.

Agency Response

On September 26, 2003, we received a written response from OBPA on the findings and recommendations contained in the draft. OBPA management generally agreed with the findings and recommendations in the draft report. Its specific comments and the Office of Inspector General's position are presented in the relevant sections of the report for each finding. OBPA's entire response is shown in exhibit A of the report.

OIG Position

We were able to reach management decision on Recommendations Nos. 1 and 10. Our position on what is needed to reach management decision on the remaining recommendations is outlined in the findings and recommendations section of the report.

Abbreviations Used in this Report

IT
information technology 1
LAN
local area network 1
MEI
minimum essential infrastructure 6
OBPA
Office of Budget and Program Analysis 1
OCFO
Office of the Chief Financial Officer 4
OCIO
Chief Information Officer 3
OMB
Office of Management and Budget 1
PDD
Presidential Decision Directive 6
TCP/IP
Transmission Control Protocol/Internet Protocol 2
USDA
U.S. Department of Agriculture 1

Table of Contents

Background and Objectives

Background

The Office of Budget and Program Analysis (OBPA) provides analyses and information to the Office of the Secretary and other policy officials to support informed decision-making regarding the Department's program and policies, budget, legislative proposals, and regulatory actions. OBPA also provides Departmentwide coordination for the presentation of budget-related matters to the committees of the Congress, the news media, and the public, as well as for the preparation, coordination, and processing of the U.S. Department of Agriculture's (USDA) legislative program, legislative reports, and regulatory actions.

OBPA's information technology (IT) resources are comprised of a local area network (LAN) and computer servers that provide the office with the capability to complete budget and program analyses. The LAN is composed of workstations and servers that provide employees with office software, Internet access and e-mail. Computer servers allow OBPA to track, monitor, and comment on regulations and legislation. To protect the integrity and security of this system, OBPA uses software and physical security measures to prevent incidental or malicious damage to its IT resources.

Office of Management and Budget (OMB) Circular A-130, dated November 30, 2000, establishes policy for the management of Federal IT resources. The policy requires security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. The OMB circular requires risk assessments, security plans, and contingency planning and system certifications to lessen the risk and magnitude of damage to information.

Objectives

The objectives of this audit were to (1) assess the management of OBPA's information systems security program; (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 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. Vulnerabilities

Finding 1 — Vulnerabilities Expose OBPA Systems To Risk From Internal and External Threats

Although OBPA does a good job of assessing its LAN for vulnerabilities and applying patches for mitigating any problems and properly updating the network, our vulnerability scans disclosed weaknesses in IT security administration. Specifically, scans of OBPA systems disclosed vulnerabilities that could be exploited from both inside and outside of the OBPA network, and system settings did not provide for optimum security. OMB Circular A-130 requires agencies to assess the vulnerability of information system assets, identify threats, quantify the potential losses from threats, and develop countermeasures to eliminate or reduce the threat or amount of potential loss. Vulnerabilities existed because OBPA did not take sufficient actions to identify and eliminate security vulnerabilities within its systems. If corrections are not made, OBPA's network could be vulnerable to cyber-related attacks, jeopardizing the integrity and confidentiality of OBPA systems.

We conducted our scans of the OBPA network between December 2002 and January 2003. We utilized two commercial off-the-shelf software products, one designed to perform over 1,100 tests for security vulnerabilities on systems that utilize Transmission Control Protocol/Internet Protocol (TCP/IP); and the other, which tests system settings in network operating system.

TCP/IP Vulnerabilities

We conducted vulnerability scans on OBPA network components. Our assessments revealed 1 high-risk, 27 medium-risk, and 90 low-risk vulnerabilities. The high- and medium-risk vulnerabilities, if left uncorrected, could allow unauthorized users access to OBPA data. Additionally, the large number of low-risk vulnerabilities identified indicates the need to strengthen system administration. During our fieldwork, OBPA officials advised us that they took immediate action to begin implementing the changes and enhancements necessary to resolve each of the high-risk and medium-risk vulnerabilities we identified. However, the vulnerabilities found at OBPA are significantly lower than the numerous vulnerabilities we found at other USDA agencies.

Examples of high- or medium-risk vulnerabilities revealed during our scans of OBPA systems included:

- One host was running an old version of a protocol used to manage systems and network devices. This version was vulnerable to a wide range of attacks known by the hacker community. These vulnerabilities may be exploited remotely, allowing an attacker to gain control of the system, and possibly other devices on the network.
- Four user accounts have a blank password. Any individual can log in to these accounts without using a password.

Network Operating System Policies

We conducted a detailed assessment of the security of the operating networks. Our assessment software allowed us to compare OBPA established security practices to the actual settings on the network operating systems. Our review of the software scanning results identified access control weaknesses. Specifically, we found (1) accounts with passwords more than 90 days old; (2) passwords set to never expire, including accounts belonging to system administrators; and (3) accounts that have never been accessed. These weaknesses could allow hackers to use these accounts making it difficult to detect their intrusion.

OBPA's systems had 19 accounts with non-expiring passwords. Seven of the 19 were administrator accounts that were more than 45 days old. Further, two of these had passwords that were more than 2 years old. USDA Office of the Chief Information Officer (OCIO) "Cyber Security Guidance Regarding C2 Controlled Access Protection, CS-013" states, "* * * passwords for all systems, applications or processes shall be changed every 60 days for general users. Passwords issued to system administrators, system managers and software engineers or those that are used for dial-in access shall be changed every 30-45 days. * * *"

Our review revealed 17 accounts had not been logged on to in the last 90 days. Of the 17 accounts, 14 had never been logged on to and only 6 of the 17 were disabled.

Recommendation No. 1

Complete corrective actions on all high- and medium-risk vulnerabilities identified on assessment reports provided to OBPA officials.

Agency Response. In its September 26, 2003, response, OBPA stated,

> *OBPA accepts and agrees with the recommendation with regards to taking appropriate corrective action on all high and medium risk vulnerabilities. As noted in the audit, the one high risk vulnerability identified by OIG audit had already been corrected. We have, to the maximum extent practicable, also eliminated the medium risk vulnerabilities. Some medium risk vulnerabilities cannot be eliminated without the loss of business functionality. We have taken note of these risks, without necessarily eliminating them*

OIG Position. We accept management decision for this recommendation. For final action, provide documentation to the Office of the Chief Financial Officer (OCFO) on corrective actions that have been taken.

Recommendation No. 2

Assess low-risk vulnerabilities to identify trends and initiate action on those areas that could lead to more serious vulnerabilities.

Agency Response. In its September 26, 2003, response, OBPA stated, "OBPA accepts and agrees with the recommendation to continue monitoring low risk vulnerabilities lest they become elevated in severity. This is a normal and integral aspect of good IT security management."

OIG Position. We cannot accept management decision for this recommendation. OBPA should provide plans on when low-risk vulnerabilities will be assessed and the estimated completion date of these actions.

Recommendation No. 3

Establish and implement controls to delete accounts that are no longer needed, disable those accounts that have not been accessed in 90 days, and ensure passwords expire as required by OCIO Cyber Security guidance.

Agency Response. In its September 26, 2003, response, OBPA stated,

> *OBPA agrees, and has in place procedures and controls to monitor and delete or disable user accounts that are no longer needed and to ensure that passwords expire appropriately. Some system accounts are rarely used but cannot be disabled or deleted as suggested by OIG. Other security measures are in effect for those accounts.*

OIG Position. We cannot accept management decision for this recommendation. OBPA should provide specific details on the actions taken to correct the deficiencies noted, procedures or controls established, and other security measures for accounts that cannot be disabled or deleted.

Finding 2 OBPA Information Security Program Management Needs Improvement

OBPA needs to improve its management of IT resources and ensure compliance with existing Federal requirements for managing and securing IT resources. OBPA has not (1) conducted the necessary risk assessments of their network, (2) adequately planned for network security and contingencies, or (3) properly certified to the security of their systems. OBPA officials stated that they have not placed a priority on OMB Circular A-130 requirements such as risk assessments, security plans, contingency planning, and system certifications due to lack of staffing while upgrading operating systems. We concluded that OBPA's written policies focus on user security and not general security administration. Since OBPA relies on its IT infrastructure to track legislation and regulations, and to communicate and coordinate budget information, it needs to ensure compliance with OMB Circular A-130 to prevent interruptions of its systems.

Risk Assessments

OBPA management stated that they had not documented risk assessments thus we could not identify or determine what areas were assessed. Risk assessments, as defined by OMB, which 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. Additionally, Presidential Decision Directive (PDD) 63 requires agencies to proactively manage and protect its minimum essential infrastructure (MEI). Specific requirements of PDD 63 include (1) identifying MEI, (2) assessing the vulnerability of MEI, (3) establishing a remediation plan for correcting vulnerabilities, and (4) creating a system for responding to significant infrastructure attack.

Security Plans

OBPA has not prepared a security plan that adequately addressed the requirements of OMB Circular A-130. Subsequent to our fieldwork, OBPA management stated that they had prepared and submitted a security plan to the OCIO on April 30, 2003. OMB Circular A-130 requires agencies to prepare a security plan to provide an overview of the security requirements of their systems. Security plans should define the technical security appropriate for the system, who has authority to access the system, background screening of system administrators, appropriate limits on interconnectivity with other systems, and security training of individuals authorized to use the system. In addition, USDA Departmental Manual 3140 requires each agency to submit an automated data processing security plan or an annual update to an existing plan to OCIO. As a result, OBPA was not assured it had adequately addressed its security needs and that security policies and practices have become an integral part of its operations. We were unable to review the recently completed security plan due to time constraints.

Contingency Plans and Backup/Recovery Plans

OBPA does not have a contingency plan in place to ensure an adequate recovery of computer resources in the event of a disaster or other major disruption in service. Although OBPA regularly backs up its systems, it does not have adequate offsite storage. We found that offsite storage was maintained at an employee's home. For proper disaster recovery, backup files should be rotated offsite to avoid disruption if current files are lost or damaged. Copies of system and application documentation should also be maintained at an offsite storage location. OBPA officials stated that the cost of offsite storage is greater than the benefit to be received, but they were exploring alternatives to the current method of storing backup tapes. Since OBPA does not have adequate offsite storage, it cannot be assured that its network can quickly and effectively be recovered in the event of an emergency.

OMB Circular A-130 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, OMB Circular A-130 states that reliance on IT makes the return to manual processing an unrealistic option for disaster recovery. For this reason, an agency should have procedures in place to protect information resources and minimize the risk of unplanned interruptions, and a plan to recover critical operations should interruptions occur. Although often referred to as disaster recovery plans, controls to ensure service continuity should address the entire range of potential disruptions from minor interruptions to major disasters. Further, OMB Circular A-130 states that contingency plans be tested; as untested or outdated contingency plans create the false sense of ability to recover in a timely manner.

Background Investigations

Federal law and OMB Circular A-130 require that persons in positions of public trust and those who are authorized to bypass significant technical and operational security controls have periodic background checks. None of the four employees that are system administrators have undergone background investigations. OBPA management stated that the employees had undergone initial screening when hired and that annual performance evaluations were the only screening that had been conducted since employees were hired. Furthermore, OBPA had not determined if the systems administrators' positions were ones of public trust. Without proper background checks or screening on its system administrators, OBPA does not have any level of assurance that those administrators can be entrusted with the network resources and data under their control.

System Certification/Authorization

OBPA has not performed system certifications and authorizations as required by OMB Circular A-130. Without adequate certification and authorization of OBPA systems, it cannot be assured that adequate security controls have been established for those systems and that appropriate controls are operating effectively. OBPA systems are used to track and monitor legislation and regulations and to communicate and coordinate budget information, which are critical to its operations.

OMB Circular A-130 requires agencies to provide a written authorization by a management official for the system to process information. Management authorization is based on an assessment of management, operational, and technical controls. Authorization is supported by a technical evaluation, risk assessment, contingency plan, and signed rules of behavior. Re-authorization should occur after any significant change in the system, but at least every 3 years. It should be done more often where there is high risk and potential magnitude of harm.

Recommendation No. 4

Prepare and document periodic risk assessments to determine the vulnerability of system assets and develop countermeasures to eliminate or reduce the threat of potential loss.

Agency Response. In its September 26, 2003, response, OBPA stated, “Risk assessments are an integral part of good management and have always been a part of OBPA’s IT security measures. A formal risk assessment was submitted to OCIO on August 21, 2003.”

OIG Position. We cannot accept management decision for this recommendation. Although OBPA has recently submitted a risk assessment to OCIO, we need specific details on plans to conduct future periodic risk assessments.

Recommendation No. 5

Develop controls to insure computer security plans and any periodic updates to those plans are completed to address security needs, policies and practices.

Agency Response. In its September 26, 2003, response, OBPA stated, "OBPA adheres to OCIO guidance with regards to preparing its security plans. A formal security plan was submitted to OCIO on April 30, 2003."

OIG Position. We cannot accept management decision for this recommendation. OBPA needs to provide specific details on controls established to ensure timely periodic updates to the security plans.

Recommendation No. 6

Develop a contingency plan, adequate backup storage, and periodically test the contingency plan to ensure timely recovery of computer resources.

Agency Response. In its September 26, 2003, response, OBPA stated,

> *All current data and system files are backed up daily to removable media which is stored in a secure and fire proof safe. This system is considered adequate for OBPA's recovery needs. OBPA will, however, continue to explore additional cost effective options for alternate back up locations and procedures. In addition, OBPA IT staff is documenting its disaster prevention, recovery, and contingency plans.*

OIG Position. We cannot accept management decision for this recommendation. OBPA needs to complete its analysis for alternate backup locations, provide the results to OIG, and provide timeframes for completing its disaster prevention, recovery, and contingency plans.

Recommendation No. 7

Coordinate with OCIO to determine if individuals with trusted access to systems and data are in a position of public trust requiring background investigations and if so, perform complete background investigations for all individuals. If not, conduct periodic screenings for all systems administrators.

Agency Response. In its September 26, 2003, response, OBPA stated, "OBPA is coordinating this recommendation with OCIO. Should it become necessary to perform background checks, or obtain security classifications, such checks and clearances as are necessary will be obtained for IT staff."

OIG Position. We cannot accept management decision for this recommendation. OBPA should provide the results of its efforts to coordinate with OCIO and timeframes of actions needed to implement this recommendation.

Recommendation No. 8

Obtain management's system authorization and certification for OBPA's computer systems.

Agency Response. In its September 26, 2003, response, OBPA stated, "OBPA adheres to the written policies of the OCIO and is reviewing its requirements for system certification and authorization to obtain any necessary Departmental approvals to continue to operate its non major, general support system."

OIG Position. We cannot accept management decision for this recommendation. OBPA should provide its review results for system certification and authorization, and estimated timeframes of actions needed for implementation of this recommendation.

Finding 3 OBPA Access Controls Need Improvement

OBPA needs to strengthen its access controls to protect against unauthorized access. Logical and physical controls are not adequate because detailed risk assessments of the controls have not been accomplished. Without additional controls, IT resources are not adequately protected against incidental or intentional damage.

Departmental regulations require access controls to mitigate security risks on information systems. Access controls are required by the Department Manual 3140-1, "Management ADP Security", which establishes standards for physical security and controls. OCIO has also published detailed checklists for logical controls on IT resources.

Access controls should provide reasonable assurance that computer resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Such controls include physical controls, such as keeping computers in locked rooms to limit physical access, and logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. Our review identified several physical and logical controls that are needed to protect computer resources.

Logical Controls

Logical controls need to be strengthened to protect IT resources from incidental or intentional damage. Specifically, the password history needs to be increased and passwords for users need to be alphanumeric. Also, some administrator accounts have shared passwords that make it impossible to track the actions of users in the event that inappropriate or malicious actions are taken.

Increasing the password history from three to at least five iterations per the USDA Security Assessment Guide and requiring alphanumeric passwords decreases the ability of unauthorized individuals from accessing the system. The increased password history helps to prevent break-ins due to stolen passwords. Requiring passwords to be alphanumeric helps prevent break-ins to the system from individuals using password cracking programs or dictionaries to guess passwords.

Physical Controls

We observed several physical weaknesses in the facilities that could lead to unauthorized modification, disclosure, loss, or impairment of computer resources, if not corrected. Specifically, we identified:

- combination locks are needed on computer center doors,
- door windows that allow observation of the computer center operations,
- OBPA network switches that are in an unlocked cabinet, and
- a cable networks that is exposed without protective conduits.

The computer center is located in a nondescript office that is indistinguishable from other OBPA offices. Although the door windows are made of pique glass, many terminals in the room can be observed through the window. To protect the center from casual observation, door offices need shades or other obstructions on the interior to deny observation. Also, doors leading into the computer network center need combination locks to reduce access by master keys, which add additional security that the current deadbolts do not provide.

Safeguards are also needed on major switches and the cables leading from those switches to avoid incidental or intentional disconnection or loss. A network switch is located in an unlocked cabinet. The cables that connect those switches to the rest of OBPA are directly exposed. Locks and protective coverings are needed to safeguard the switches and cables.

Recommendation No. 9

Strengthen logical controls by requiring users to develop and implement alphanumeric passwords and increase password histories to at least five.

Agency Response. In its September 26, 2003, response, OBPA stated, "OBPA has issued instructions to all users requiring them to use alphanumeric passwords."

OIG Position. We cannot accept management decision for this recommendation. OBPA needs to address the portion of the recommendation regarding increasing password histories to at least five.

Recommendation No. 10

Conduct and document physical control assessments to determine any needed security measures that must be corrected.

Agency Response. In its September 26, 2003, response, OBPA stated, "After reviewing our security needs with staff of USDA's Office of Operations, several enhancements to physical security were implemented. For example, combination locks were added to computer center doors; and door windows that might allow observation of the computer center operations were blocked."

OIG Position. We accept management decision on this recommendation. For final action, provide documentation to OCFO on the enhancements that have been made.

Scope and Methodology

We tested OBPA computer systems to identify vulnerabilities that could enable unauthorized users to access sensitive data stored on or transmitted over OBPA's systems. We conducted our audit at OBPA offices located in Washington, D.C. We reviewed controls over the computer systems to ensure the integrity of OBPA's information security program. We used commercially available software applications to assist us in our security reviews of network components. Fieldwork was performed from October 2002 through March 2003.

We conducted this audit in accordance with generally accepted government auditing standards. To accomplish our audit objectives, we performed the following procedures:

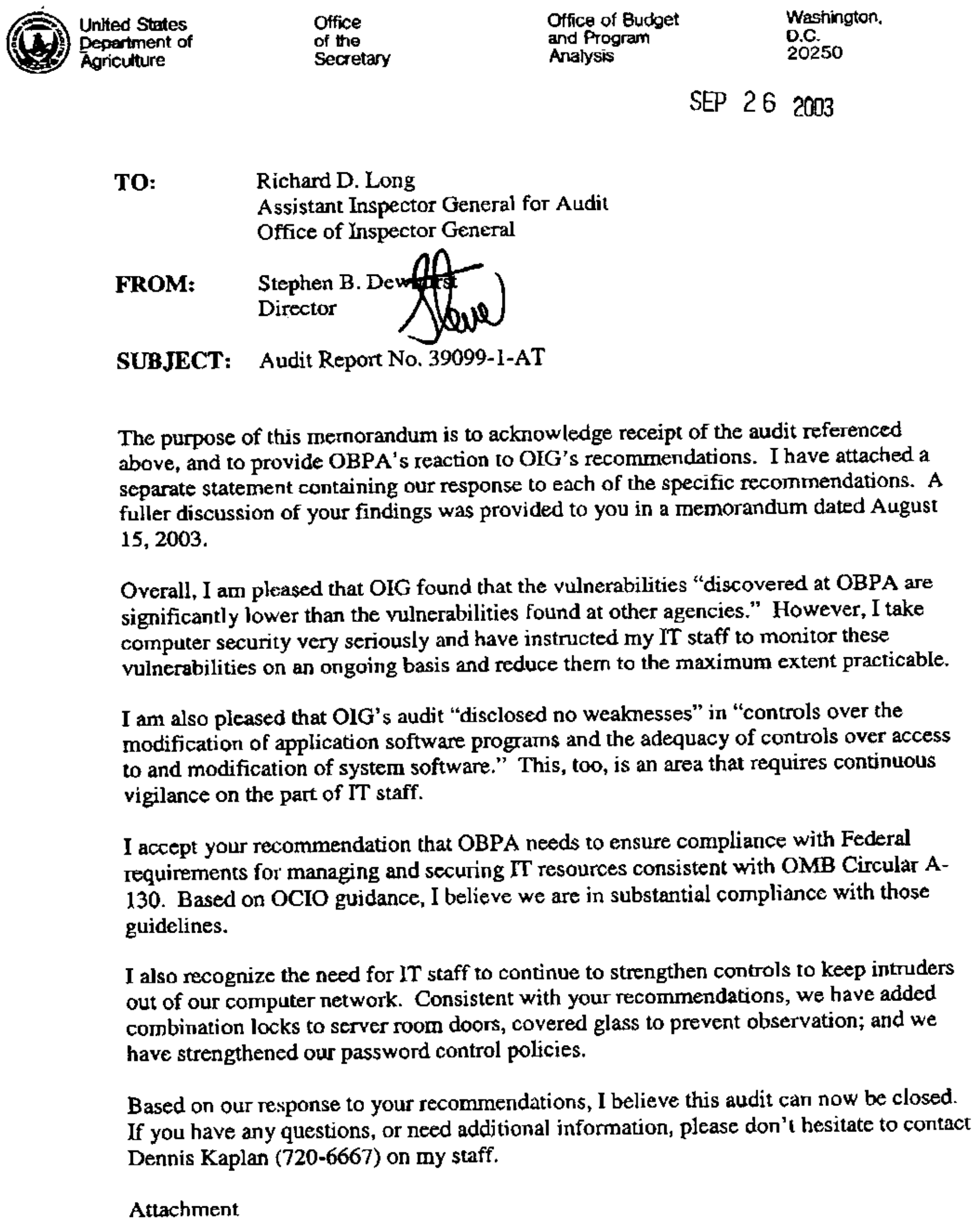
- Performed detailed testing of OBPA's security program, including both physical and logical access controls, by analyzing records and controls established to ensure that the security of its computer systems was sufficient.

- Reviewed IT security policies and procedures from OBPA, the Department, OMB, and other sources.

- Interviewed responsible agency and program officials managing the computer systems.

- Performed TCP/IP vulnerability scans on various network components.

Exhibit A - *Agency Response*



United States
Department of
Agriculture

Office
of the
Secretary

Office of Budget
and Program
Analysis

Washington,
D.C.
20250

SEP 26 2003

TO: Richard D. Long
Assistant Inspector General for Audit
Office of Inspector General

FROM: Stephen B. Dewhurst
Director

Steve

SUBJECT: Audit Report No. 39099-1-AT

The purpose of this memorandum is to acknowledge receipt of the audit referenced above, and to provide OBPA's reaction to OIG's recommendations. I have attached a separate statement containing our response to each of the specific recommendations. A fuller discussion of your findings was provided to you in a memorandum dated August 15, 2003.

Overall, I am pleased that OIG found that the vulnerabilities "discovered at OBPA are significantly lower than the vulnerabilities found at other agencies." However, I take computer security very seriously and have instructed my IT staff to monitor these vulnerabilities on an ongoing basis and reduce them to the maximum extent practicable.

I am also pleased that OIG's audit "disclosed no weaknesses" in "controls over the modification of application software programs and the adequacy of controls over access to and modification of system software." This, too, is an area that requires continuous vigilance on the part of IT staff.

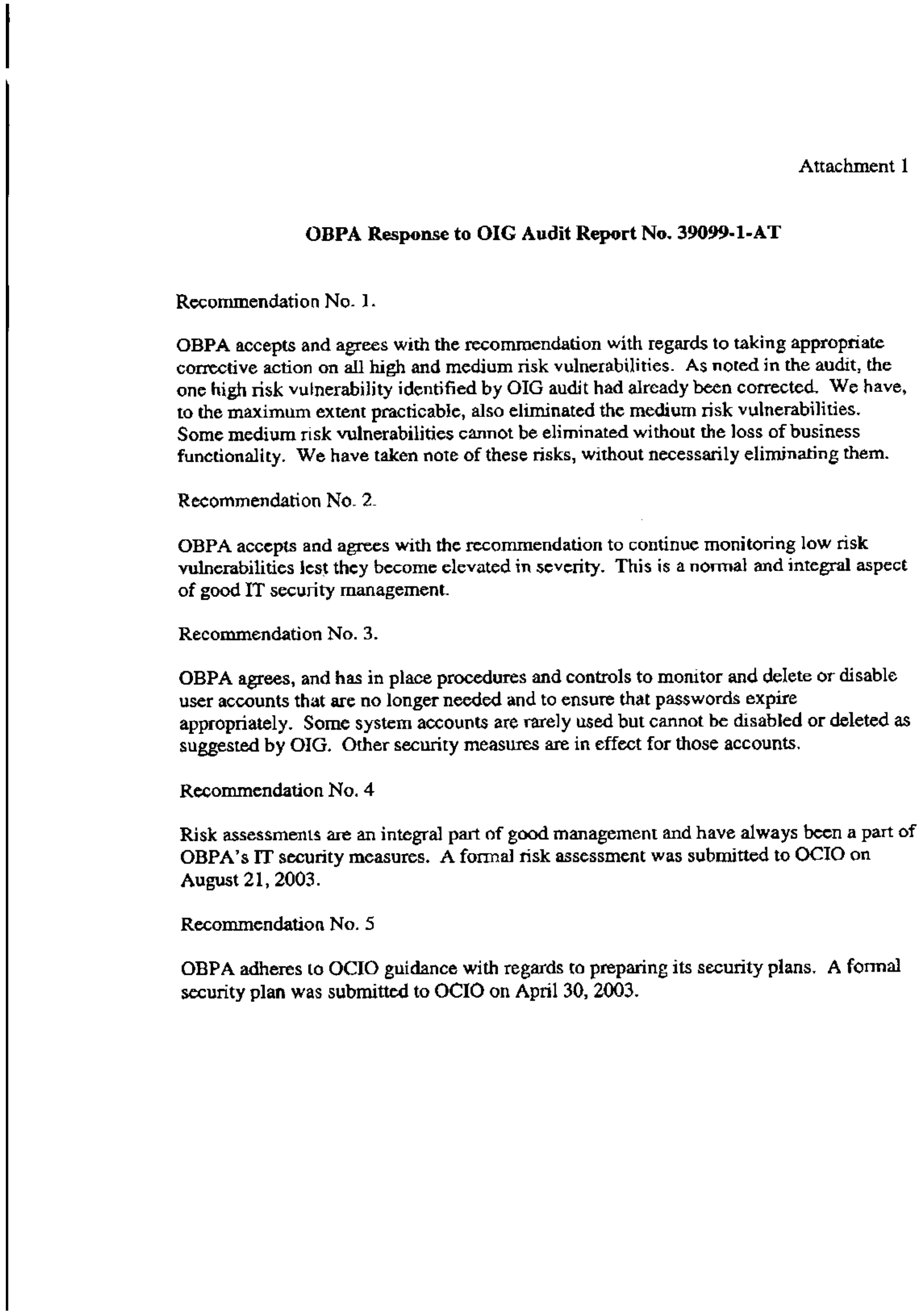
I accept your recommendation that OBPA needs to ensure compliance with Federal requirements for managing and securing IT resources consistent with OMB Circular A-130. Based on OCIO guidance, I believe we are in substantial compliance with those guidelines.

I also recognize the need for IT staff to continue to strengthen controls to keep intruders out of our computer network. Consistent with your recommendations, we have added combination locks to server room doors, covered glass to prevent observation; and we have strengthened our password control policies.

Based on our response to your recommendations, I believe this audit can now be closed. If you have any questions, or need additional information, please don't hesitate to contact Dennis Kaplan (720-6667) on my staff.

Attachment

Exhibit A - Agency Response



Attachment 1

OBPA Response to OIG Audit Report No. 39099-1-AT

Recommendation No. 1.

OBPA accepts and agrees with the recommendation with regards to taking appropriate corrective action on all high and medium risk vulnerabilities. As noted in the audit, the one high risk vulnerability identified by OIG audit had already been corrected. We have, to the maximum extent practicable, also eliminated the medium risk vulnerabilities. Some medium risk vulnerabilities cannot be eliminated without the loss of business functionality. We have taken note of these risks, without necessarily eliminating them.

Recommendation No. 2.

OBPA accepts and agrees with the recommendation to continue monitoring low risk vulnerabilities lest they become elevated in severity. This is a normal and integral aspect of good IT security management.

Recommendation No. 3.

OBPA agrees, and has in place procedures and controls to monitor and delete or disable user accounts that are no longer needed and to ensure that passwords expire appropriately. Some system accounts are rarely used but cannot be disabled or deleted as suggested by OIG. Other security measures are in effect for those accounts.

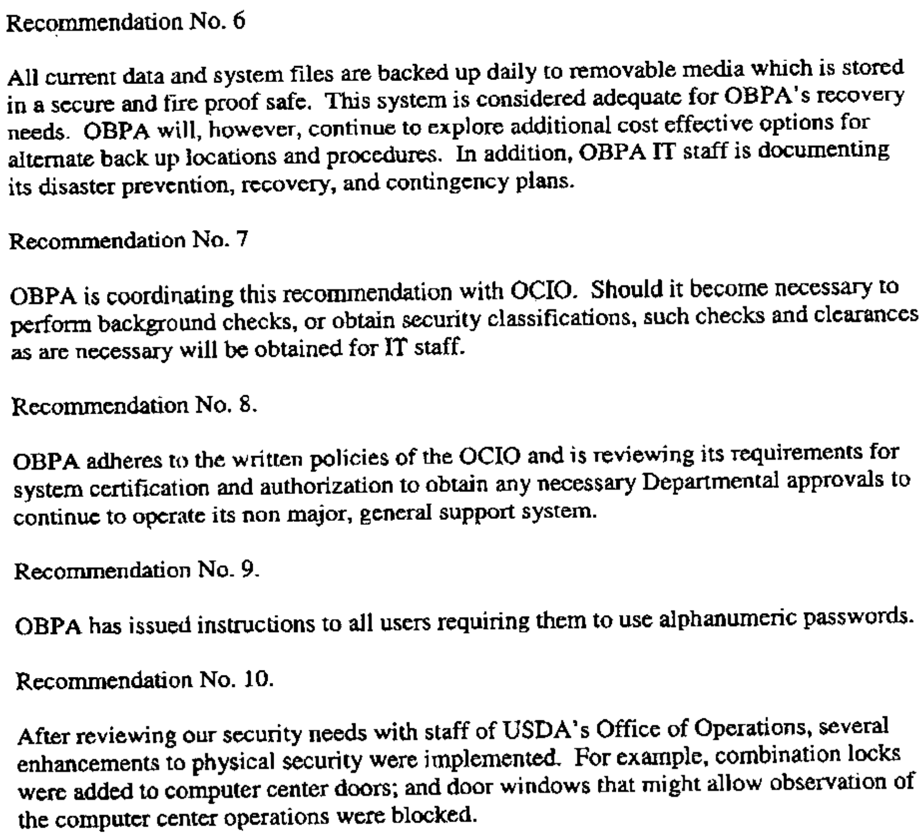
Recommendation No. 4

Risk assessments are an integral part of good management and have always been a part of OBPA's IT security measures. A formal risk assessment was submitted to OCIO on August 21, 2003.

Recommendation No. 5

OBPA adheres to OCIO guidance with regards to preparing its security plans. A formal security plan was submitted to OCIO on April 30, 2003.

Exhibit A - Agency Response



Recommendation No. 6

All current data and system files are backed up daily to removable media which is stored in a secure and fire proof safe. This system is considered adequate for OBPA's recovery needs. OBPA will, however, continue to explore additional cost effective options for alternate back up locations and procedures. In addition, OBPA IT staff is documenting its disaster prevention, recovery, and contingency plans.

Recommendation No. 7

OBPA is coordinating this recommendation with OCIO. Should it become necessary to perform background checks, or obtain security classifications, such checks and clearances as are necessary will be obtained for IT staff.

Recommendation No. 8.

OBPA adheres to the written policies of the OCIO and is reviewing its requirements for system certification and authorization to obtain any necessary Departmental approvals to continue to operate its non major, general support system.

Recommendation No. 9.

OBPA has issued instructions to all users requiring them to use alphanumeric passwords.

Recommendation No. 10.

After reviewing our security needs with staff of USDA's Office of Operations, several enhancements to physical security were implemented. For example, combination locks were added to computer center doors; and door windows that might allow observation of the computer center operations were blocked.