



U.S. Department of Agriculture



Office of Inspector General
Southeast Region

Audit Report

Management and Security of Office of the Chief Economist Information Technology Resources

Report No. 12099-1-AT
January 2004



UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington, D.C. 20250



DATE: **January 23, 2004**

REPLY TO

ATTN OF: 12099-1-A1

SUBJECT: Management and Security of the Office of the Chief Economist
Information Technology Resources

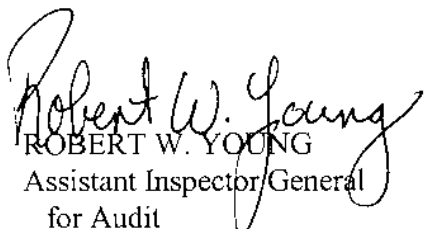
TO: Keith Collins
Chief Economist
Office of the Chief Economist

This report presents the results of our audit of the Office of the Chief Economist's management and security of Information Technology Resources. Your October 15, 2003, response to the draft report is included as exhibit A with excerpts and the Office of Inspector General's position incorporated into the relevant sections of the report.

We agree with your management decisions for Recommendations Nos. 1, 2, 3, 4, 6, 8, and 11. Management decisions have not yet been reached for Recommendations Nos. 5, 7, 9, 10, and 12. The findings and recommendations section of the report includes a description of the status of the management decision for each recommendation.

In accordance with Department Regulation 1720-1, please furnish a reply within 60 days describing the corrective action taken or planned and the timeframes for implementation for those recommendations for which a management decision has not yet been reached. Please note that the regulation requires a management decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance, and final action to be taken within 1 year of each management decision. Correspondence concerning final actions should be addressed to the Office of the Chief Financial Officer.

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


ROBERT W. YOUNG
Assistant Inspector General
for Audit

Executive Summary

Management and Security of Office of the Chief Economist Information Technology Resources (Audit Report No. 12099-1-AT)

Results in Brief

This report presents the results of our audit of the management and security of the Office of the Chief Economist's (OCE) information technology (IT) resources. OCE relies on its IT infrastructure to collect, analyze, and produce data and other information concerning agricultural commodities that are market sensitive. OCE's ability to complete this mission would be jeopardized if its IT infrastructure were compromised.

Our objectives were to assess the overall management of OCE's Information System Security Program (ISSP), determine the adequacy of security over local and wide area networks and to determine if adequate logical and physical access controls exist to protect computer resources against unauthorized modification, disclosure, loss, or impairment.

Overall, we identified weaknesses in logical access controls to computer resources and in security program planning and management oversight.

To test the vulnerability of OCE to the threat of internal and external intrusions, we conducted an assessment of OCE networks, using commercially available software, which is designed to identify vulnerabilities associated with various operating systems. Our assessment identified three medium-risk IT vulnerabilities. Compared to other U.S. Department of Agriculture agencies, which we have audited and found numerous high and medium-risk vulnerabilities, OCE is commended for the relatively low number of medium-risk vulnerabilities we found. OCE officials advised us that they took immediate action to implement the changes and enhancements necessary to resolve each of the medium-risk vulnerabilities identified. However, our assessment software also identified several low-risk vulnerabilities pertaining to logical access controls. Low-risk vulnerabilities are those that provide access to sensitive, but less significant data. While OCE has taken adequate actions to mitigate some of the low-risk vulnerabilities, further action is required to strengthen access controls. Weak access controls leave critical information vulnerable to unauthorized access, modification, and intentional or accidental destruction.

We found that OCE needs to ensure compliance with Federal and departmental requirements. Specifically, we noted that OCE had not

- effectively controlled logical access controls to its network and
- adequately implemented an entitywide program for security management and planning.

Recommendations in Brief

We recommend that OCE:

- Strengthen logical access controls to enhance security over IT assets.
- Establish controls to conduct periodic risk assessments to determine the vulnerability of system assets.
- Establish procedures and controls to prepare and continually update a disaster recovery/business resumption plan in preparation of a disaster or other significant network or system outage.
- Establish controls so that background investigations are periodically conducted on individuals with computer security responsibilities.
- Establish controls to ensure that systems are certified and authorized immediately, and then, on a 3-year schedule or when significant changes are made.
- Provide for a separation of duties within the IT functional area.
- Establish written policies and procedures for responding to computer security incidents.
- Prepare and distribute formal written procedures for computer security training to inform computer users of security policies and requirements.

Agency Position

In its October 15, 2003, written response to the draft report, OCE was in general agreement with the findings and recommendations. Its specific comments and OIG's position are presented in the relevant sections of the report for each finding. OCE's entire response is shown in exhibit A of the report.

OIG Position

Our position for each recommendation is presented in the relevant sections of the report for each finding. We agreed with management decisions for Recommendations Nos. 1, 2, 3, 4, 6, 8, and 11. We requested additional information on Recommendations Nos. 5, 7, 9, 10, and 12.

Abbreviations Used in this Report

ADP
automated data processing 1

CM
configuration management..... 3

CSA
Computer Security Act 1

DM
Departmental Manual..... 1

DR
Departmental Regulations..... 1

FISCAM
Federal Information System Controls Audit Manual..... 13

GAO
General Accounting Office 13

GISRA
Government Information Security Reform Act 1

ISSP
Information System Security Program..... 14

ISSPM
Information System Security Program Manager 14

IT
information technology 1

LAN
local area network 2

MEI
minimum essential infrastructure..... 10

NASS
National Agricultural Statistics Service..... 12

NAWIS
National Agricultural Weather Information System..... 2

NAWON
National Agricultural Weather Observation Network 2

NIST
National Institute of Standards and Technology..... 1

NITC
National Information Technology Center 12

OCE
Office of the Chief Economist 1

OCFO
Office of the Chief Financial Officer 6

OCIO
Office of the Chief Information Officer..... 4

OMB
Office of Management and Budget..... 1

PDD	
Presidential Decision Directive.....	1
SIRMO	
Senior Information Resources Management Official	14
<u>SP</u>	
<u>Special Publication</u>	1
TCP/IP	
Transmission Control Protocol/Internet Protocol	3
USDA	
U.S. Department of Agriculture.....	1
WAOB	
World Agricultural Outlook Board.....	14
WASDE	
World Agricultural Supply and Demand Estimates Report.....	2

Table of Contents

Executive Summary	i
Abbreviations Used in this Report	iii
Table of Contents	v
Background and Objectives	1
Findings and Recommendations	3
Section 1. Security of OCE’s Local Area Network	3
<i>Finding 1 OCE Needs to Strengthen its Access Controls</i>	3
Recommendation No. 1	6
Recommendation No. 2	6
Recommendation No. 3	7
Recommendation No. 4	7
Recommendation No. 5	8
Section 2. Security Program Planning and Management Oversight.....	9
<i>Finding 2 OCE Information System Security Program Management Needs Improvement</i>	9
Recommendation No. 6	11
Recommendation No. 7	12
Recommendation No. 8	12
Recommendation No. 9	13
<i>Finding 3 OCE’s Security Management Structure Has Insufficient Separation of Duties</i>	13
Recommendation No. 10	14
<i>Finding 4 OCE Has Not Formalized An Incident Response Capability</i>	16
Recommendation No. 11	16
<i>Finding 5 OCE Computer System Users Not Informed of Security Policies</i>	17
Recommendation No. 12	18
Scope and Methodology	19
Exhibit A - Agency Response	20

Background and Objectives

Background

Information security, improving the overall management of information technology (IT) resources, and the transition to electronic business (e-government) have emerged as 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. This environment poses a threat to the sensitive and critical operations of the Office of the Chief Economist (OCE).

Various laws have emphasized the need to protect agencies' sensitive and critical data, including the Privacy Act of 1974, the Computer Security Act (CSA) of 1987, and the Paperwork Reduction Act of 1995. Responsibilities regarding information security were reemphasized in the Clinger-Cohen Act of 1997 and Presidential Decision Directive (PDD) 63. Additionally, the Government Information Security Reform Act (GISRA), enacted on October 30, 2000, essentially codifies the existing requirements of the Office of Management and Budget (OMB) Circular A-130. The National Institute of Standards and Technology (NIST) 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 (SP) 800-12, October 1995.

Finally, Departmental Manual (DM) 3140-1 also provides standards, guidelines, and procedures for the development and administration of automated data processing (ADP) security programs mandated by departmental regulations (DR).

OCE was created by the Secretary of Agriculture on October 20, 1994, under the authority of the Federal Crop Insurance Reform and Department of Agriculture Reorganization Act of 1994, Public Law 103-354. OCE's mission is to (1) advise the Secretary on the economic prospects in agricultural markets and the economic implications of policies, programs, and economic events affecting the United States agriculture and rural communities; (2) ensure the public has consistent, objective, and reliable agricultural forecasts; and (3) promote effective and efficient rules governing departmental programs.

OCE carries out three major functions: (1) economic intelligence, policy and program analysis, and coordination, which includes responsibility for advancing USDA policy and principles relating to global change, energy, and sustainable developmental activities; (2) agricultural estimates and projections; and (3) regulatory analysis.

OCE's IT resources are comprised of a local area network (LAN) that provides the office with the capability to complete its mission. The LAN is composed of workstations and servers that provide employees with office software, Internet access, and e-mail. OCE's production of the monthly World Agricultural Supply and Demand Estimates Report (WASDE) is housed on this system. The WASDE report is a forecast of supply and demand for major farm crops. OCE also operates the National Agricultural Weather Observation Network (NAWON) and the National Agricultural Weather Information System (NAWIS). The purpose of NAWON and NAWIS is to provide for the collection of domestic meteorological data for use by Federal agencies and the private sector. To protect the integrity and security of these computer systems, OCE uses logical access controls and physical security measures to prevent incidental or malicious damage to its IT resources.

OMB Circular A-130, dated November 30, 2000, establishes policy for the management of Federal IT resources. Such 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, 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 the agency's information systems security program, (2) determine the adequacy of the security over the agency networks, and (3) determine if adequate logical and physical access controls exist to protect computer resources.

Findings and Recommendations

Section 1. Security of OCE's Local Area Network

OCE's information system includes a LAN. 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.

We conducted our assessment of OCE's network between December 2002 and January 2003. We utilized 2 commercial off-the-shelf software products, 1 designed to perform over 1100 tests for security vulnerabilities on systems that utilize Transmission Control Protocol/Internet Protocol (TCP/IP), and the other, which tests system policy settings in network operating systems.

We found that OCE 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 identified three medium-risk vulnerabilities. OCE took immediate steps to correct the vulnerabilities. We determined that OCE adequately patched the known vulnerabilities. However, we also identified a number of low-risk vulnerabilities that indicate weaknesses in computer access controls. A contributing factor in identifying low-risk vulnerabilities was OCE's lack of a configuration management (CM) program for the LAN.

Finding 1

OCE Needs to Strengthen its Access Controls

OCE needs to improve logical access controls in order to ensure integrity, confidentiality, and availability of the data maintained in their systems. OCE did not (1) always remove access for terminated employees, (2) maintain access authorizations for each individual user, or (3) establish adequate account and password controls. OCE had not implemented adequate and complete written procedures. Inadequate access controls leave critical information vulnerable to unauthorized access, modification, and intentional or accidental destruction.

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 software programs designed to prevent or detect unauthorized access to sensitive files.

Two of the 11 employees separated from OCE in the last year are listed as authorized users in the system. These individuals have retired from OCE, but still have user identifications. DM 3140-1.6, Management ADP Security¹, requires staff to remove employees' user accounts and passwords when an employee is no longer with the agency.

Access authorizations are not documented for all users of OCE's systems and applications; and therefore, authorizations are not periodically reviewed to determine if they still remain appropriate. NIST SP 800-12, Introduction to Computer Security, section 10.2.1², states that if a user is to have access to a particular application, a formal approval is required stating the level of access to be granted to the user. It is also necessary to only allow users access to functions necessary to accomplish their responsibilities; and therefore, access and authorization administration is a continuing process of review.

Numerous account and password access control weaknesses were identified with our scanning software. We conducted a detailed assessment of the security of OCE's network operating system. Our scanning software provides comprehensive and flexible reporting capabilities of access control lists, user account characteristics, password controls, and many other security features. OCE's system is vulnerable to intruders without the proper security of account and password controls.

- Generally, most of OCE's account settings require passwords to be changed every 40 days. We identified six accounts that were set up with passwords that will never expire. Additionally, we identified an account with administrative privileges that required the password to be changed every 365 days. According to NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, dated September 1996, passwords should be changed periodically. The Office of the Chief Information Officer's (OCIO) Cyber Security Policy CS-013, dated March 6, 2002, requires passwords for all systems, applications, or processes to be changed every 60 days for general users. Passwords issued to system administrators or those that are used for dial-in access are to be changed every 30-45 days. OCE changed the password change interval of one account to 30 days and agreed to fix the settings of all other accounts to meet standards.
- We identified six accounts setup with unlimited grace logins, technically allowing the user to keep the same password forever, because the system would never force the user to change the password. We identified another user account with eight grace logins. Seven accounts were found with excessive grace logins. Six of the seven accounts had "unlimited"

¹ USDA DM 3140-1.6, Management of ADP Security Manual, part 6 of 8, appendix D, section 6c, dated June 19, 1984.

² NIST, An Introduction to Computer Security: The NIST Handbook, SP 800-12, Section 10.2.1 "User Account Management," dated October 1995.

grace logins and one of the seven accounts had eight grace logins. According to NIST SP 800-14³ organizations should limit the number of logon attempts. Lockout should occur after a set number of failed login attempts.

- Twenty-three accounts were identified that had not logged on within the last 90 days. Thirteen of the 23 accounts had never been logged on, 3 of the 23 accounts had not been accessed in over a year, and 4 accounts had not been logged on for 6 months. Only 3 of the 23 accounts were disabled. NIST SP 800-14, section 3.11.1⁴, states that user identifications that are inactive on the system for a specified period of time (e.g., 3 months) should be disabled.
- Two accounts had been logged in for longer than one day. Accounts should be automatically logged off after a set period of inactivity. This prevents someone from using an unoccupied machine to gain unauthorized access.
- Three out of 87 accounts had the password minimum length set too low. OCIO's Office of Cyber Security's Guidance⁵ states that the minimum password length requirement should be set at six to eight characters. OCE changed the password minimum length for all accounts to eight characters. This weakness was identified in the Plans of Action and Milestones in the GISRA report by OCE.
- Nine accounts did not require the user to change an expired password to one unique from those previously used by that user. OCIO Cyber Security Policy, CS-013, dated March 6, 2002, prohibits systems from allowing the reuse of a previously used password until after five other different passwords have been used.

Configuration Management

A factor in our computer scans identifying the low-risk vulnerabilities cited above is that OCE has not developed a CM program for its LAN. CM ensures that all systems are configured alike by routinely updating systems with recent security patches and other software updates. Departmental policy concerning CM⁶ states that all USDA offices and agencies will implement an effective CM program for all IT systems under their control. Failure to exercise control of LAN system configuration and changes result in weak or ineffective security controls protecting system data. We believe this

³ NIST Generally Accepted Principles and Practices for Securing Information Technology Systems, section 3.11.2, dated September 1996.

⁴ NIST Generally Accepted Principles and Practices for Securing Information Technology Systems, section 3.11.1, dated September 1996.

⁵ Cyber Security Guidance Regarding C2 Controlled Access Protection, CS-013.

⁶ Interim Guidance on USDA CM, Part 1 – Policy and Responsibilities, CS-009, Draft 10/15/01.

corporate-level approach to system configuration, along with regularly scheduled vulnerability assessments and remediation of the risks discovered, would substantially enhance the security of OCE's computer systems.

CM processes are used to establish and maintain control of system/application software, and system and network physical infrastructure changes, ensuring that the system in operation is the correct system.

OCE informed us that they are looking into acquiring a commercial CM product. We concluded that the security of OCE's LAN and data integrity could be compromised without a CM program.

Recommendation No. 1

OCE security officials should establish written procedures and controls to remove computer system access for separated employees within 24 hours of separation.

Agency Response. In its October 15, 2003, response, OCE stated,

Current policy is to maintain separated employee files on the system to assure that necessary files are available for the successor. While the files remain on the server, the ID of the separated employee is disabled and cannot be accessed without the assistance of the system administrator. OCE will develop written procedures and controls to address this recommendation.

Target date for completion: December 2003.

OIG Position. We accept management decision for this recommendation. For final action, provide documentation to the Office of the Chief Financial Officer (OCFO) that written procedures and controls to remove computer system access for separated employees within 24 hours of separation have been established.

Recommendation No. 2

OCE should document access authorizations on standard forms and maintain the access authorizations forms on file. OCE should ensure forms are approved by senior managers and securely transferred to security managers. OCE should review access authorizations periodically for appropriateness.

Agency Response. In its October 15, 2003, response, OCE stated, "At present, management approves individual access authority on "needs access" basis. In addition, each OCE office is assigned segregated disk space. OCE

will establish an authorization file and review this file periodically. Target date for completion: June 2004.”

OIG Position. We accept management decision for this recommendation. For final action, provide documentation to OCFO that access authorizations are documented on standard forms and that access authorizations are maintained on file. OCE should also provide documentation to OCFO ensuring access authorization forms are approved by senior managers and securely transferred to security managers as well as reviewed periodically for appropriateness.

Recommendation No. 3

Ensure that all OCE user accounts meet USDA, OCIO, and cyber security standards, including password length and expiration.

Agency Response. In its October 15, 2003, response, OCE stated, “This recommendation has been adopted.”

OIG Position. We accept management decision for this recommendation. For final action, provide documentation to OCFO that user accounts meet USDA, OCIO, and cyber security standards, including password length and expiration.

Recommendation No. 4

Establish written procedures and controls to disable accounts that have not been accessed in over 90 days or that have passwords more than 90-days old, and delete those accounts no longer needed.

Agency Response. In its October 15, 2003, response, OCE stated,

Access to external entities on the system is protected by network restriction, intrusion detection, and passwords. These IDs do not enable access to files on the server other than e-mail. These IDs are used to automatically forward e-mail to specified user groups within OCE. An ID is required in the network tree to establish an e-mail account. Since no one logs into the tree to access these IDs directly, they appear to be inactive. All other IDs on the system which remain inactive for 90 days will be disabled or removed.

Written procedures and controls will be written to handle accounts over 90-days old.

Target date for completion: January 2004.

OIG Position. We accept management decision for this recommendation. For final action, provide documentation to OCFO that written procedures and controls have been established to disable accounts that have not been accessed in over 90 days or that have passwords more than 90 days old, and to delete those accounts no longer needed.

Recommendation No. 5

Implement an effective CM program for all OCE IT systems. Develop a policy establishing minimum security setting guidelines for OCE systems. Periodically, assess those settings and correct those that have been misapplied.

Agency Response. In its October 15, 2003, response, OCE stated, "Configuration management tasks are routinely performed by OCE's system analyst. In the future, these tasks will be documented. Target date for completion: Fiscal 2004."

OIG Position. We cannot accept management decision for this recommendation. OCE should specifically agree to develop a policy establishing minimum security guidelines for its systems, to include a provision that settings be periodically assessed and corrected as needed, and the date the action will be completed.

Section 2. Security Program Planning and Management Oversight

An entitywide program for security planning is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate, responsibilities may be unclear, misunderstood, and improperly implemented, and controls may be inconsistently applied.

Through the CSA, Congress provided a means for establishing minimally acceptable security practices related to Federal computer systems. CSA requires agencies to identify and protect systems containing "sensitive" information and requires a computer standards program and security training. OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, established a minimum set of controls for agencies' automated information security programs, including assigning responsibility for security, security planning, periodic review of security controls, and management authorization of systems to process information.

OCE has not established a security management structure that clearly assigns information security responsibilities and provides for a separation of duties, informs users of security policies, and implements an incident response capability. OCE also needs to improve its management of information systems security to ensure compliance with Federal regulations.

Finding 2

OCE Information System Security Program Management Needs Improvement

OCE needs to improve its management of IT resources and ensure compliance with existing Federal requirements for managing and securing IT resources. OCE has not (1) conducted the necessary risk assessments of their networks, (2) adequately planned for network security and contingencies, (3) performed background investigations of all personnel with computer security responsibilities, or (4) properly certified to the security of their major systems. OCE management has not placed a priority on OMB Circular A-130 requirements such as risk assessments, security plans, contingency planning, background investigations, and system certification. Since OCE relies on its IT infrastructure to advise the Secretary on economic prospects of agricultural markets and to establish agricultural estimates and projections, it is essential to have adequate security controls over IT resources.

Risk Assessments

OCE had not performed risk assessments, as defined by OMB, as a 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. OCE's GISRA report dated August 16, 2002, indicates that risk assessments of IT systems had been performed. However, OCE officials were unable to provide us with supporting documentation of those reviews. PDD 63⁷ requires agencies to proactively manage and protect its critical infrastructure. Specific requirements of PDD 63 include (1) identifying minimum essential infrastructure (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.

Contingency Plans

OCE does not have a contingency plan for its LAN. A contingency plan would ensure an adequate recovery of computer resources in the event of a disaster or other major disruption in service. OCE is in the process of developing a joint contingency plan with the National Agricultural Statistics Service for production of the monthly WASDE, which is housed on the LAN. Although we recognize this effort, we did not find a developed and tested contingency plan for OCE's LAN. We also did not find a contingency plan for OCE's NAWON and NAWIS. The purpose of NAWON/NAWIS is to provide for the collection of domestic meteorological data for use by Federal agencies and the private sector. OCE considers NAWON/NAWIS a separate computer system from the LAN.

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 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 the ability to recover in a timely manner.

⁷ The Clinton Administration's Policy on Critical Infrastructure Protection: PDD 63, dated May 22, 1998.

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 investigations. Not all of OCE's personnel with computer security responsibilities have undergone background investigations. A computer specialist along with a systems analyst makes up OCE's IT staff. Both individuals have the ability to bypass OCE computer security controls. We noted that a background investigation had not been completed for the computer specialist. Without proper background investigations on its system administrators, OCE 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

OCE has not performed system certifications and authorizations as required by OMB Circular A-130. Without adequate certification and authorization of OCE systems, it cannot be assured that adequate security controls have been established for those systems and that appropriate controls are operating effectively. OCE systems are used to provide important agricultural data as well as meteorological forecasts for agricultural planning.

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. Reauthorization 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. 6

Establish written procedures and controls to conduct 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 October 15, 2003, response, stated,

Risk assessments have been used to implement present network safeguard controls such as (scanning devices for vulnerabilities, patching units, networks address restriction, firewalls, and application security). OCE has followed OCIO guidelines to develop these security processes and controls. A

more comprehensive set of guidelines will be developed and documented.

Target date for completion: Fiscal 2004.

OIG Position. We accept management decision for this recommendation. For final action, provide documentation to OCFO showing that procedures and controls to conduct periodic risk assessments have been developed.

Recommendation No. 7

Establish written procedures and controls to prepare and continually update a disaster recovery/business resumption plan in preparation of a disaster or other significant network or system outage.

Agency Response. In its October 15, 2003, response, OCE stated,

OCE has a cooperative agreement with the National Information Technology Center [NITC] in Kansas City to store backup tapes which are FEDEXed to NITC weekly. OCE is actively working with the National Agricultural Statistics Service [NASS] to develop a disaster recovery/business resumption plan. A WAOB/NASS relocation site is presently under construction in Fairfax, Virginia. Written procedures and tools for recovery/resumption of business activities are being developed.

Target date for completion: Fiscal 2004-2005.

OIG Position. We cannot accept management decision for this recommendation. Since the target completion date is not specific and actions may take more than 12 months to implement, OCE should adopt interim measures to minimize the adverse condition noted during the corrective action period.

Recommendation No. 8

Establish written procedures and controls so that background investigations are periodically conducted on individuals with computer security responsibilities.

Agency Response. In its October 15, 2003, response, OCE stated, "OCE will develop procedures and guidelines governing background investigations on IT personnel with computer security responsibilities. Target date for completion: Fiscal 2004."

OIG Position. We accept management decision for this recommendation. For final action, provide documentation to OCFO that written procedures and controls have been established so that background investigations are periodically conducted on individuals with computer security responsibilities.

Recommendation No. 9

Establish written procedures and controls to ensure that systems are certified and authorized immediately and then on a 3-year schedule or when significant changes are made.

Agency Response. In its October 15, 2003, response, OCE stated, "OCE will develop guidelines for certification and authorization of its systems. Target date for completion: Fiscal 2004."

OIG Position. We cannot accept management decision for this recommendation. In our estimation, written procedures and controls, and not guidelines, are needed to provide the necessary level of assurance that the condition will be rectified.

Finding 3

OCE's Security Management Structure Has Insufficient Separation of Duties

OCE's security management structure does not provide for a separation of duties between oversight and administrative functions. The same individual is responsible for overseeing IT security and administering OCE's networks. Inadequate segregation of duties within the information security environment increases the risk that (1) erroneous or fraudulent data could be processed, (2) improper program changes could be implemented, and (3) computer resources could be damaged or destroyed. In OCE's case, a senior management official delegated responsibility for information systems management to the individual who was also responsible for ensuring network security. OCE has not developed and implemented a written procedure that provides for a separation of duties within the IT functional area. According to OCIO's Office of Cyber Security, separation of duties is an important element of access control. NIST SP 800-12 defines separation of duties as dividing roles and responsibilities so that a single individual cannot subvert a critical process. The General Accounting Office's (GAO) Federal Information System Controls Audit Manual (FISCAM)⁸ identifies

⁸ GAO FISCAM, Chapter 3, Section 3.5, "Segregation of Duties," dated January 1999.

information system management and network administration as incompatible duties, and should be performed by different individuals.

OCE security plan identifies the Chairperson of the World Agricultural Outlook Board (WAOB) (an OCE component) as the responsible official for developing and implementing an effective security plan. The WAOB chairperson appointed a WAOB systems analyst as the Senior Information Resources Management Official (SIRMO). The security plan defines the SIRMO's responsibilities as ensuring security over IT, market sensitive data, and working files. SIRMO also serves as the Information System Security Program Manager (ISSPM) with day-to-day operational responsibility for OCE's Information System Security Program (ISSP). In essence, the ISSPM is tasked with oversight responsibilities in ensuring the security of OCE's computer systems. However, the systems analyst serving as the SIRMO/ISSPM also serves as the network administrator. Network administration is defined as the function within an organization responsible for maintaining a secure and reliable online communications network and serves as liaison with user departments to resolve network needs and problems. We feel that IT security and network administration are incompatible duties that should be spread among senior management employees.

The IT staff within WAOB consists of two employees; one, a systems analyst (SIRMO) and the other a computer specialist. The two person IT staff is responsible for providing support to all elements of OCE.

According to FISCAM, the extent to which duties are segregated depends, in part, on the size of the organization. Smaller organizations and organizations with limited resources, like OCE, may rely more extensively on supervisory review to control activities. The information systems manager should not be in a position to manage the network administrator's work over network security and access because the same individual serves a dual role as both information system manager and network administrator. In effect, the information system manager would be reviewing his/her own work.

Recommendation No. 10

Develop and implement written procedures providing for a separation of duties within the IT functional area. Separate the functions performed by the individual responsible for network access and security. Ensure that these functions are not performed by the same individual. If separation of duties is not feasible, establish compensating controls such as supervisory review of transactions.

Agency Response. In its October 15, 2003, response, OCE stated, "Due to budget constraints, access and security functions are necessarily performed

by the same individual. As future budgets permit, these functions will be segregated among separate individuals. Target date for completion: Fiscal 2004.”

OIG Position. We cannot accept management decision for this recommendation. Since OCE feels that budget constraints may impede the implementation of separation of duties within the IT environment, OCE should provide evidence of compensating controls, such as a written policy on supervisory review of transactions related to the functions of network access and security, until funding is available for segregating duties.

Finding 4**OCE Has Not Formalized An Incident Response Capability**

OCE has not formalized a written policy for computer security incident response capability. Implementing such a policy would ensure that security incidents are properly tracked and that adequate corrective actions are taken to prevent recurrence. OCE's Computer Security Plan does not address incident response procedures. OCE told us that their policy was to follow procedures outlined in the USDA Computer Incident Response Procedures Manual. However, the procedures manual states that agencies are to develop their own internal procedures.

OCIO's Cyber Security Office issued the USDA Computer Incident Response Procedures Manual on October 25, 2001, which identifies policy and procedures for reporting intrusions into USDA IT systems. It requires all USDA agencies to establish and implement an internal incident handling/response capability, and to develop procedures that define the internal actions that must be taken in reporting and responding to intrusions and attempted intrusions. At a minimum, these internal policies are to include the reporting chain, the involvement of ISSPM, preservation of evidence, containment actions, documentation, and identification of corrective actions that will strengthen USDA security programs.

OCE should formulate their own written policies and procedures for responding to computer security incidents. Without adequate controls over the incident reporting process, OCE can have no assurance that incidents have been adequately addressed. Once formulated, OCE should communicate incident response capability/handling policies and procedures to all users.

Recommendation No. 11

OCE should establish written policies and procedures for responding to computer security incidents and distribute to all computer users.

Agency Response. In its October 15, 2003, response, OCE stated, "No security violations have been detected. Written policy and procedures for responding to computer security incidents will be developed and distributed to all computer users. Target date for completion: Fiscal 2004."

OIG Position. We accept management decision for this recommendation. For final action, provide documentation to OCFO indicating that written policies and procedures for responding to computer security incidents were established and distributed to all users.

Finding 5**OCE Computer System Users Not Informed of Security Policies**

Users of OCE's computer systems were not aware of security policies and requirements outlined in OCE's computer security plan because it had not been distributed to OCE staff. Our review disclosed that OCE staff had not received computer security-related training. For a computer security plan to be effective, those expected to comply with it should be aware of it. Without computer security training, users could be susceptible to revealing passwords or other sensitive information to unauthorized parties. Informing users of security policies could make them think twice about revealing sensitive data and make them more likely to notice and report suspicious activity.

CSA⁹ directs agencies to provide mandatory training in computer security awareness and accepted security practices for current and new employees who are involved with the management, use, or operation of each Federal computer system. OMB Circular A-130, appendix III¹⁰, requires training of individuals before granting access to computer systems. DR 3140-1¹¹, also requires agencies to (1) ensure that information systems security requirements, procedures, and practices are included in computer security training material; (2) provide new employees an orientation outlining security responsibilities; and (3) provide training to employees on a regular basis.

OCE computer users are informally made aware of password security and virus software updates. However, OCE does not meet the above requirements for notifying users of computer security policies because they do not have a formal written procedure informing users of their expectations in regards to computer security. GAO's FISCAM suggests that typical means for establishing and maintaining awareness include:

- informing users of the importance of the information they handle and the legal and business reasons for maintaining its integrity and confidentiality;
- distributing documentation describing security policies, procedures, and individual responsibilities, including their expected behavior;
- requiring users to periodically sign a statement acknowledging their awareness and acceptance of responsibility for security, including the consequences of security violations, and their responsibilities for following all organizational policies, including maintaining

⁹ CSA, Public Law 100-235, Section 2(b)(4), dated January 8, 1988.

¹⁰ OMB Circular A-130, appendix III, A.3.a.2 (b).

¹¹ DR 3140-1, USDA Information Systems Security Policy, Section 12 "Training," dated May 15, 1996.

confidentiality of passwords and physical security over their assigned areas; and

- requiring comprehensive security orientation, training, and periodic refresher programs to communicate security guidelines to both new and existing employees and contractors.

IT trends and their evolving security implications have become too complex to be successfully achieved by individuals lacking a comprehensive set of competencies. Without appropriate training OCE personnel are unable to fulfill their security responsibilities.

Recommendation No. 12

Provide user training and prepare and distribute formal written procedures for computer security to inform computer users of computer security policies and requirements.

Agency Response. In its October 15, 2003, response, OCE stated, “Formal materials will be prepared and distributed to employees to address this issue. Target date for completion: Fiscal 2004.”

OIG Position. We cannot accept management decision for this recommendation. OCE should address whether it intends to provide user training and by when.

Scope and Methodology

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

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

- Performed detailed testing of OCE'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 OCE, USDA, OMB, and other sources.
- Interviewed responsible agency and program officials managing the computer systems.
- Performed TCP/IP vulnerability scans on various network components.

We conducted this audit in accordance with generally accepted government auditing standards.



**United States
Department of
Agriculture**

Office of the Secretary

Office of the Chief Economist

14th & Independence Ave., SW
Washington, DC 20250

TO: Raymond G. Poland
Regional Inspector General

FROM: Keith Collins
Chief Economist

Keith Collins OCT 15 2003

SUBJECT: Response to OIG Security Audit

This memo responds to recommendations in OIG's security audit of the Office of the Chief Economist conducted from November 2002 through March 2003 in Washington, D.C.

Recommendation 1. OCE security officials should establish written procedures and controls to remove computer system access for separated employees within 24 hours of separation.

Current policy is to maintain separated employee files on the system to assure that necessary files are available for the successor. While the files remain on the server, the ID of the separated employee is disabled and cannot be accessed without the assistance of the system administrator. OCE will develop written procedures and controls to address this recommendation.

Target date for completion: December 2003.

Recommendation 2. OCE should document access authorizations on standard forms and maintain the access authorization forms on file. OCE should ensure that forms are approved by senior managers and securely transferred to security managers. OCE should review access authorizations periodically for appropriateness.

At present, management approves individual access authority on "needs access" basis. In addition, each OCE office is assigned segregated disk space. OCE will establish an authorization file and review this file periodically.

Target date for completion: June 2004

Recommendation 3. Ensure that all OCE user accounts meet USDA, OCIO, and cyber security standards, including password length and expiration.

This recommendation has been adopted.

Raymond G. Poland
Page 2

Recommendation 4. Establish written procedures and controls to disable accounts that have not been accessed in over 90 days or that have passwords more than 90-days old, and delete those accounts no longer needed.

Access to external entities on the system are protected by network restriction, intrusion detection, and passwords. These IDs do not enable access to files on the server other than e-mail. These IDs are used to automatically forward e-mail to specified user groups within OCE. An ID is required in the network tree to establish an e-mail account. Since no one logs into the tree to access these IDs directly, they appear to be inactive. All other IDs on the system which remain inactive for 90 days will be disabled or removed.

Written procedures and controls will be written to handle accounts over 90-days old.

Target date for completion: January 2004.

Recommendation 5. Implement an effective CM program for all OCE IT systems. Develop a policy establishing minimum security setting guidelines for OCE systems. Periodically, assess those settings and correct those that have been misapplied.

Configuration management tasks are routinely performed by OCE's system analyst. In the future, these tasks will be documented.

Target date for completion: Fiscal 2004

Recommendation 6. Establish written procedures and controls to conduct periodic risk assessments to determine the vulnerability of system assets and develop countermeasures to eliminate or reduce the threat of potential loss.

Risk assessments have been used to implement present network safeguard controls such as (scanning devices for vulnerabilities, patching units, networks address restriction, firewalls, and application security). OCE has followed OCIO guidelines to develop these security processes and controls. A more comprehensive set of guidelines will be developed and documented.

Target date for completion: Fiscal 2004

Recommendation 7. Establish written procedures and controls to prepare and continually update a disaster recovery/business resumption plan in preparation of a disaster or other significant network or system outage.

OCE has a cooperative agreement with the National Information Technology Center in Kansas City to store backup tapes which are FEDEXed to NITC weekly. OCE is actively working with the National Agricultural Statistics Service to develop a disaster recovery/business resumption plan. A WAOB/NASS relocation site is presently under construction in Fairfax, Virginia. Written procedures and tools for recovery/resumption of business activities are being developed.

Target date for completion: Fiscal 2004-2005.

Raymond G. Poland
Page 3

Recommendation 8. Establish written procedures and controls so that background investigations are periodically conducted on individuals with computer security responsibilities.

OCE will develop procedures and guidelines governing background investigations on IT personnel with computer security responsibilities.

Target date for completion: Fiscal 2004

Recommendation 9. Establish written procedures and controls to ensure that systems are certified and authorized immediately and then on a 3-year schedule or when significant changes are made.

OCE will develop guidelines for certification and authorization of its systems.

Target date for completion: Fiscal 2004

Recommendation 10. Develop and implement written procedures providing for a separation of duties within the IT functional area. Separate the functions performed by the individual responsible for network access and security. Ensure that these functions are not performed by the same individual. If separation of duties is not feasible, establish compensating controls such as supervisory review of transactions.

Due to budget constraints, access and security functions are necessarily performed by the same individual. As future budgets permit, these functions will be segregated among separate individuals.

Target date for completion: Fiscal 2004.

Recommendation 11. OCE should establish written policies and procedures for responding to computer security incidents and distribute to all computer users.

No security violations have been detected. Written policy and procedures for responding to computer security incidents will be developed and distributed to all computer users.

Target date for completion: Fiscal 2004

Recommendation 12. Provide user training and prepare and distribute formal written procedures for computer security to inform users of computer security policies and requirements.

Formal materials will be prepared and distributed to employees to address this issue.

Target date for completion: Fiscal 2004