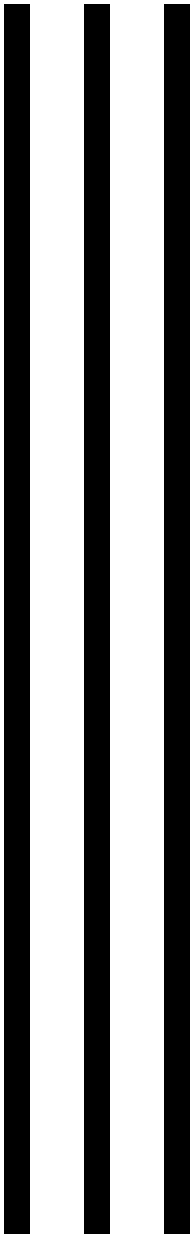

U.S. Department of Agriculture
Office of Inspector General
Financial and IT Operations
Audit Report

SECURITY OVER INFORMATION TECHNOLOGY RESOURCES AT THE NATIONAL AGRICULTURAL STATISTICS SERVICE

Report No.
26099-1-FM
May 2001

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: May 14, 2001

REPLY TO
ATTN OF: 26099-1-FM

SUBJECT: Security Over Information Technology Resources at the National Agricultural Statistics Service

TO: R. Ronald Bosecker
Administrator
National Agricultural Statistics Service

This report presents the results of our audit of the Security Over Information Technology Resources at the National Agricultural Statistics Service (NASS). The report identifies weaknesses in NASS' ability to protect its critical information technology resources. NASS has corrected a substantial number of the problems found, and has aggressively implemented plans to correct the remaining areas of concern.

Your response to our draft report is included 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 on all recommendations in the report. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer.

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

/s/

ROGER C. VIADERO
Inspector General

EXECUTIVE SUMMARY

RESULTS IN BRIEF

We identified weaknesses in National Agricultural Statistics Service's (NASS) ability to adequately protect sensitive information from inappropriate disclosure, and critical operations from disruption. Significant information security weaknesses were identified during our review including inadequately restricted access to sensitive data. Although this and other identified weaknesses placed critical NASS operations at risk of disruption of service and inappropriate disclosures, prompt action by NASS has mitigated a majority of the weaknesses identified. NASS relies on its information technology (IT) infrastructure to supply market-sensitive data on commodities to the agricultural community. NASS' ability to accomplish this mission would be jeopardized if its IT infrastructure were compromised.

To test the vulnerability of NASS to the threat of internal and external intrusions, we conducted an assessment of selected NASS networks, using a commercially available software product, which is designed to identify vulnerabilities associated with various operating systems. Our assessments, performed in November and December 2000, identified 71 high and medium risk IT security vulnerabilities[1] and numerous low risk vulnerabilities. These vulnerabilities could have allowed an attacker to gain complete administrative privileges of NASS' network. Once this administrative privilege is established, an attacker could obtain, modify or destroy critical NASS data. During our fieldwork, NASS 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. NASS also took immediate action to protect its internal network by ensuring the proper configuration of its firewall. Further, NASS began efforts to conduct its own scans of its systems on a periodic basis to identify and mitigate known vulnerabilities.

Additionally, we found that NASS had not developed a configuration program for its systems. A configuration program ensures that all systems are configured alike by routinely updating all systems with security patches and other software updates. We believe this corporate level approach to system

[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.

configuration, along with regularly scheduled vulnerability assessments and remediation of the risks discovered, would substantially enhance the security of NASS' computer systems.

We found that NASS needs to improve its management of IT resources, and ensure compliance with existing Federal requirements for managing and securing IT resources. NASS has not (1) identified their mission essential infrastructure (MEI) or conducted the necessary risks assessments of their networks as required by Presidential Decision Directive (PDD) – 63; (2) adequately documented network security in their security plan as required by the Office of Management and Budget (OMB) Circular A-130; (3) prepared for potential service disruptions by developing a comprehensive contingency plan; or (4) properly certified to the security of their major systems. We found that NASS' managers, who are responsible for ensuring adequate security, have not evaluated the adequacy of their computer-based controls, or fully identified risks to their systems.

Our audit disclosed that NASS had weak controls over access to its sensitive data and systems at both the SSO's and headquarters. Because SSO's were allowed to configure their systems, there was little oversight by headquarters personnel to ensure that access controls were functioning properly. Headquarters personnel stated that the access control weaknesses were overlooked in the daily operation of the computer system.

The types of weaknesses we found in our audit made it possible for persons to inappropriately modify or destroy sensitive data or computer programs or inappropriately obtain and disclose confidential information. In today's increasingly interconnected computing environment, inadequate access controls can expose agency information and operations to attacks from remote locations by individuals with minimal computer or telecommunications resources and expertise. NASS officials have begun to take corrective action to correct the weaknesses identified.

KEY RECOMMENDATIONS

We recommended that NASS:

- Ensure corrective actions are taken on the vulnerabilities we identified.
- Periodically scan its network for vulnerabilities and track corrective actions to assure remediation.

- Adopt a corporate level approach to include establishing minimum security guidelines for the various operating systems used by NASS. Periodically assess those settings and correct those that have been misapplied.
- Ensure NASS compliance with PDD-63 and OMB requirements by identifying NASS' MEI; performing a vulnerability assessment of the MEI; and establishing a remediation plan for correcting the vulnerabilities.

- Update the NASS Security Plan to include all areas required by OMB A-130, and provide more comprehensive information, as required.
- Document a comprehensive contingency plan and initiate procedures for periodic testing of the contingency plan.
- Correct identified access control weaknesses.

AGENCY RESPONSE

The NASS agreed with our recommendations and has initiated significant corrective actions.

OIG POSITION

We concurred with the NASS' proposed corrective actions and have reached management decision on all recommendations.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

Information security is critical for any organization that depends on information systems and computer networks to carry out its mission or business. Computer security risks are significant, and they are growing. The dramatic expansion in computer interconnectivity and the exponential increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. However, without proper safeguards, these developments pose enormous risks that make it easier for individuals and groups with malicious intentions to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other organizations' sites. Further, the number of individuals with computer skills is increasing, and intrusion, or "hacking" techniques are readily available and relatively easy to use. This environment poses a threat to the sensitive and critical operations of the National Agricultural Statistics Service (NASS) and puts it at high risk.

NASS administers the U.S. Department of Agriculture's (USDA) program of collecting, compiling, and disseminating current national and state agricultural statistics. NASS' primary activities are the collection, summarization, and analysis of data for publication of accurate and reliable agricultural forecasts and estimates. Statistical data developed by NASS on the nation's agriculture are essential for the orderly development of production and marketing decisions by farmers, ranchers, and agribusiness. This data is also used for defining and carrying out agricultural policy related to farm program legislation, commodity programs, agricultural research, rural development, and related activities.

NASS issues the official state and national agricultural production and marketing estimates relating to (1) the number of farms and land in farms, acreage, yield and production of grains, grain stocks, hay, oilseeds, cotton, some fruits and vegetables, floriculture and other specialty crops; (2) inventories and production of hogs, cattle, sheep and wool, catfish, trout, poultry, eggs, dairy products; (3) prices received by farmers; (4) prices paid by farmers for inputs and services, cold storage stocks, agricultural labor and wage rates; and (5) other agricultural subjects. Information for the official estimates is gathered from many sources, using a variety of means.

The information is entered through NASS' network of Local Area Networks (LAN), and uploaded through data communications to a mainframe computer

where data files are stored and processed. Data from the surveys are edited on the mainframe computer, or are edited and summarized on personal computers at the State Statistical Offices' (SSO). The SSO's also transmit computer data containing survey indicators and recommended estimates to Headquarters using data communications. Corn, cotton, soybeans, sweet oranges, winter wheat, and other spring wheat have been designated as "speculative" commodities. Data for these commodities are encrypted and handled under special security procedures in the "lockup" facility, where the official statistical estimates are generated, because of the sensitivity of the data and its potential impact on the futures market prices of the commodities involved.

For "non-speculative" commodities that have been classified as sensitive, data communications are not encrypted and the estimates are finalized before the "lockup."

OBJECTIVES

The objectives of this audit were to (1) assess the threat of penetration of NASS data systems by intruders; (2) determine the adequacy of security over the Local and Wide Area Networks; and (3) assess NASS management's role in ensuring compliance with the Office of Management and Budget (OMB) and Departmental requirements related to information technology (IT) security.

SCOPE

We tested the NASS computer network to identify vulnerabilities that could enable unauthorized users to access sensitive data stored on or transmitted over NASS' systems. We conducted our assessment at the NASS Headquarters in Washington, D.C., as well as conducting limited testing at 4 of 45 SSOs. The sample of SSOs was selected based on the type of connectivity used by the SSOs, and other considerations. We used commercial software applications to assist us in our security reviews of over 100 NASS network components.

The audit was conducted in accordance with Government Auditing Standards. Our testing was performed between October 2000 and January 2001.

METHODOLOGY

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

- We reviewed IT security policies and procedures issued by the Office

of the Chief Information Officer (OCIO) and NASS.

- We interviewed NASS officials responsible for managing the agency's computer systems.

- We conducted vulnerability scans of the systems at NASS' Headquarters and four SSOs.

- We performed detailed testing of NASS' entity-wide security program, both physical and logical access controls, segregation of duties, and service continuity at the NASS headquarters by analyzing records and controls established to ensure that the security of the NASS' computer systems was sufficient.

FINDINGS AND RECOMMENDATIONS

CHAPTER 1	VULNERABILITIES EXPOSE NASS SYSTEMS TO THE RISK OF MALICIOUS ATTACKS FROM INTERNAL AND EXTERNAL THREATS

FINDING NO. 1

Our vulnerability scans of selected NASS systems disclosed severe weaknesses in the system security administration. Specifically, we found that (1) scans of selected NASS systems disclosed a large number of vulnerabilities that could be exploited from both inside NASS' network, and externally; and (2) system settings did not provide for optimum security, nor were they uniform throughout NASS. OMB Circular A-130 requires agencies to assess the vulnerability of information system assets identify threats quantify the potential losses from threat realization; and develop countermeasures to eliminate or reduce the threat or amount of potential loss. NASS had not taken sufficient actions to identify and eliminate security vulnerabilities within its systems. As a result, NASS' systems and networks are vulnerable to cyber-related attacks, jeopardizing the integrity and confidentiality of NASS' critical economic data.

We conducted our assessment of selected NASS networks between November and December 2000. We utilized two commercial off-the-shelf software products, one designed to identify over 800 vulnerabilities associated with various operating systems that use Transmission Control Protocol/Internet Protocol (TCP/IP)[2], and the other, which tests system settings in Novell networks.

TCP/IP System Vulnerabilities

We conducted our vulnerability scans at five NASS locations. These scans included 104 NASS network components. We also tested the firewall established by NASS as protection between NASS' systems and the departmental telecommunications network. Our assessments revealed 71 high and medium-risk vulnerabilities.[3] In addition, we identified 209 low-risk vulnerabilities. The high and medium vulnerabilities, if left uncorrected, could allow unauthorized users access to critical and sensitive NASS data. Additionally, the large number of low vulnerabilities identified, indicates the need to strengthen system administration.

[2] The TCP/IP is a series of protocols originally developed for use by the US Military and now used on the Internet as the primary standard for the movement of data on multiple, diverse platforms, such as Windows NT and UNIX.

[3] 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.

Detailed below are examples of the high-risk vulnerabilities revealed during our scans of the NASS systems:

- A commonly used program to transfer electronic mail contains a vulnerability that could allow an attacker to gain complete administrative privileges of the system. Once this administrative privilege is established, an attacker could obtain, modify or destroy critical NASS data.

- Programs used on web servers to provide enhanced functionality could allow an attacker to execute commands on the server that could provide them with such critical information as the server's password file. The attacker could use this password file to obtain or destroy other data on the server.

- We scanned NASS' systems from outside the firewall to assess the level of protection the firewall was providing. Our tests showed that the firewall was not properly configured to protect the NASS internal network.

Based upon our tests, a management alert dated November 21, 2000, was issued to NASS officials describing the vulnerabilities detected and the severity of each. The management alert also reported the incorrect configuration of NASS' firewall. On December 6, 2000, NASS advised us that they had implemented the changes and enhancements necessary to resolve each of the high and medium-risk vulnerabilities reported in the management alert. Additionally, NASS took immediate action to correct the problems with their firewall configuration. On February 26, 2001, NASS informed us that they will evaluate commercially available tools for performing vulnerability assessments for the UNIX, Novell, and NT operating systems during fiscal year (FY) 2001. NASS plans to review licensing opportunities with other departmental agencies. NASS plans to acquire the recommended packages after October 1, 2001, either independently or as part of a larger USDA group. Once the recommended tools for performing vulnerability assessments is obtained, NASS will conduct vulnerability assessments on a quarterly basis beginning in January 2002

We found that NASS had not developed a configuration management program for its systems. A configuration management program ensures that all systems are configured alike by routinely updating all systems with recent security patches and other software updates. We believe this corporate level approach to system configuration, along with regularly scheduled vulnerability assessments and remediation of the risks discovered, would substantially enhance the security of NASS' computer systems.

Novell System Policies

We conducted a detailed assessment of the security of the Novell networks at five sites. Our assessment software allowed us to compare NASS' established security practices to

the actual settings on the Novell systems. We also compared the system's security settings to the software product's "best practices settings," which are based on standard practices from a wide variety of government and private institutions. The software product reports weaknesses that may leave the system open to potential threats in the following areas (1) account restrictions; (2) password strength; (3) access control; (4) system monitoring; (5) data integrity; and (6) data confidentiality.

Our assessments disclosed significant weaknesses in account restrictions, password strength, and access controls; the areas that define a user's ability to access the system. Our tests also showed the need for a configuration management program, as discussed above. We found that the Novell security settings were not consistently applied throughout the agency, varying from one site to another. For example, six grace logins[4] were allowed at two sites tested, while at two other sites, only one grace login was allowed. Some additional weaknesses we found included:

- User accounts were hidden from the system administrator. This raises concern because hidden accounts are often used as a means to set up a "back door" to the server. These accounts hold administrator access privileges, which are the most trusted users on a Novell system and allow complete control of the system. Additionally, because of these privileges, unauthorized users can modify system logs to hide their activities from the system administrator. This condition was noted at three of the five sites we visited.

- An excessive number of persons with administrator authorities were found at three of the five locations tested. We found 8 of 102 users, 5 of 97 users, and 36 of 729 users were admin equivalent at three NASS sites tested. Additionally, at one NASS field office, we noted that NASS had failed to remove user accounts belonging to another agency, including some accounts with administrator privileges.

- A large number of inactive accounts that had not been disabled were noted on all five networks tested. For example, almost 80 percent of all accounts on one network were inactive, while 24 percent of 625 user accounts were inactive at another site tested. User accounts that become inactive, but not disabled, provide opportunities for unauthorized users to gain access to the network. An attacker can try different passwords on these inactive accounts and attempt to gain access to the network. Once that access is gained, unauthorized activity cannot be traced to the responsible person.

In addition to the vulnerabilities identified by our scans, our audit work identified other vulnerabilities affecting the security of the NASS networks:

- Our review of 127 login IDs showed the use of alphanumeric characters for passwords was not required, and a minimum password length less than 6

[4] Grace logins refer to the number of times the user can log into a system without changing their password after it has expired.

characters was found for 16 of the 127 login IDs. A password made up of a combination of letters and numbers make passwords more difficult for unauthorized users to guess. Additionally, when only alpha characters are allowed in a password, users are more likely to assign common words or names as passwords making them easier for an unauthorized user to guess. Finally, passwords less than six characters in length are easier for an unauthorized user to guess.

- The feature to lockup a computer after failed login attempts was not enabled. Our testing showed that the system allowed unlimited attempts to guess the correct password. With this feature disabled, unauthorized persons could use a password cracker to attempt to access the system. At the completion of our audit, NASS personnel enabled the lockout feature so the system would lock after three unsuccessful login attempts.

RECOMMENDATION NO. 1

Ensure corrective actions are taken on all high and medium vulnerabilities identified on the assessment reports provided to NASS officials.

Agency Response

NASS has implemented solutions to resolve all of the high-risk vulnerabilities, and has mitigated all medium-risk vulnerabilities.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 2

Assess low vulnerabilities to identify trends and initiate action on those areas that together or in aggregate could lead to more serious vulnerabilities.

Agency Response

NASS has resolved over 50 percent of the 209 vulnerabilities through both direct and indirect action. NASS continues to evaluate solutions for the

low-risk vulnerabilities that have not been resolved. There are some low-risk vulnerabilities that NASS acknowledges and accepts the risks.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 3

Obtain software to enable NASS to scan its entire network, develop procedures to assure periodic assessments are performed; and methodology is developed to track and assure correction of disclosed vulnerabilities.

Agency Response

The OCIO has solicited interest from agencies regarding the acquisition of software for vulnerability testing. NASS has agreed to participate in this acquisition and has money available for an October 1, 2001, acquisition. NASS will begin vulnerability testing of our network within 90 days of product acquisition, therefore about January 1, 2002. Once the initial testing is complete, NASS will continue to conduct the tests on a quarterly basis. NASS will strive to resolve all high vulnerabilities within a week and medium vulnerabilities within three weeks. NASS will report high and medium risk vulnerabilities that are not resolved within 30 days to the OCIO.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 4

Adopt a corporate level approach to configuration management. Develop a policy establishing minimum security setting guidelines for the various operating systems used by NASS. Periodically assess those settings and correct those that have been misapplied.

Agency Response

NASS has just completed a merging process that enables our implementation of centralized configuration management. NASS has standardized some security setting guidelines and will continue to review and standardize configuration parameters during May. NASS is adopting the “Best Practices” for most of the configurable security settings. NASS will continue with this review and implementation during May.

NASS is in the process of reviewing the roles that may allow us to define a

specific role for specific responsibilities. This should allow better management and more flexibility in identifying and monitoring the various groups' activities because they would only be capable of performing required functions. NASS plans to implement roles by July 1, 2001.

OIG Position

Management decision has been reached on this recommendation.

CHAPTER 2	NASS INFORMATION SECURITY PROGRAM MANAGEMENT NEEDS IMPROVEMENT

FINDING NO. 2

NASS needs to improve its management of IT resources, and ensure compliance with existing Federal requirements for managing and securing IT resources. NASS has not (1) conducted the necessary risks assessments of their networks; (2) adequately planned for network security and contingencies; or (3) properly certified to the security of their major systems. This occurred because NASS has not placed a priority on OMB Circular A-130 requirements such as risk assessments, security plans, contingency planning, and system certifications. NASS relies on its IT infrastructure to supply market-sensitive data on commodities to the agricultural economy. NASS' ability to accomplish its mission may be jeopardized if it cannot properly secure its IT infrastructure.

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

Risk Assessments

Risk assessments, as defined by OMB, are a formal, systematic approach to assessing the vulnerability of information system assets identifying threats quantifying the potential losses from threat realization; and developing countermeasures to eliminate or reduce the threat or amount of potential loss. Additionally, PDD 63 requires agencies to proactively manage and protect its MEI. According to PDD 63, MEI is defined as the systems, the hardware the systems runs on, the personnel who operate the systems, the buildings where the systems reside, and users of the systems. Specific requirements of PDD 63 include (1) identifying MEI; (2) assessing the vulnerability of the MEI; (3) establishing a remediation plan for correcting vulnerabilities; and (4) creating a system for responding to significant infrastructure attack.

We found that NASS had not identified threats to network security by performing the required risk assessments of its networks. Our testing revealed that NASS submitted a list of its sensitive systems to OCIO as part of the Department's efforts to identify its infrastructure, but no further action was taken by NASS. We found that a

comprehensive security assessment has not been performed of the NASS infrastructure and network since 1997. Additionally, we found that an assessment of NASS' critical systems has not been performed.

Until updated risk assessments are completed, NASS cannot be assured that all of the risks attributable to its mission critical systems are identified and that appropriate steps are taken to mitigate these risks.

Security Plans

Our review disclosed that NASS had not prepared security plans that adequately addressed the requirements of OMB Circular A-130. OMB requires agencies to prepare a security plan to provide an overview of the security requirements of their systems.[5] Security plans should define who has responsibility for system security, who has authority to access the system, appropriate limits on interconnectivity with other systems, and security training of individuals authorized to use the system. In addition, USDA Departmental Manual 3140[6] requires each agency to submit an automated data processing security plan or an annual update to an existing plan to the OCIO.

The current NASS Security Plan does not include a designation of the agency official responsible for security over NASS' major applications. Some requirements were clearly missing from the plan, such as the Incident Response Capability and System Interconnection. Additionally, in discussing NASS' major applications, the plan did not address (1) application rules; (2) specialized training; (3) personnel security; (4) contingency planning; (5) technical controls; (6) information sharing; and (7) public access controls, all of which are required by OMB Circular A-130. As a result, NASS cannot be assured it has adequately addressed its security needs and that security policies and practices have become an integral part of its operations.

Contingency Plans and Backup/Recovery Plans

Although NASS had a contingency plan in place, it was not sufficiently comprehensive to ensure an adequate recovery in the event of a disaster or other major disruption in service. We also found that NASS did not regularly backup its system files, and had not adequately tested its contingency plan. As a result, NASS cannot be assured that its network can be quickly and effectively recovered to accomplish its mission 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 information technology and the push toward e-government makes the return to manual processing an unrealistic option to disaster recovery. For this reason, an agency

[5] The Computer Security Act of 1987 also requires that security plans be developed for all Federal computer systems that contain sensitive information.
[6] DM 3140-1.1, Part 9.

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 natural disasters. Further, OMB 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.

NASS uses the Business Continuity Plan prepared during its Year 2000 (Y2K) conversion effort as its contingency plan. However, the Y2K plan was not comprehensive, as it focused entirely on the preparation of monthly activity reports, and did not address potential service disruptions beyond Y2K. For example, the plan did not identify resources that would be needed to perform critical, time sensitive operations in the event of a disaster. Also, NASS operations were not prioritized for reestablishing the most critical operations first in the event of an emergency. Without this detail, the contingency plan cannot be adequately tested and therefore would be of little use in minimizing the disruption of system failure.

While NASS has back-up and off-site storage procedures in place; due to problems with its tape archival system, the off-site storage procedures have not been in effect since June 2000. If faced with an emergency, NASS would not have access to up-to-date information and would lose months worth of data. Management officials were aware of the problem, but did not address it until our audit. NASS is currently working to reload old tapes and reconcile them to the database. NASS was unable to provide a date when this process will be completed.

System Certification/Authorization

NASS has never performed system certifications and authorizations as required by OMB Circular A-130. Without adequate certification and authorization of the 26 NASS critical systems, it cannot be assured that adequate security controls have been established for those systems and that appropriate controls are operating effectively. NASS systems are used to collect, compile and analyze data for agricultural forecasts and estimates which are critical to its operations and to the agricultural economy.

OMB 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[7], risk assessment, contingency plan, and signed

[7] The technical evaluation may also be referred to as a certification review.

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.

In summary, the lack of risk assessments, adequate security and contingency plans, and system certifications for such key operations as the compilation and analysis of data for agricultural forecasts and estimates places NASS operations at high risk. NASS management needs to take an active role in IT security to ensure that the security vulnerabilities disclosed by our audit are timely and effectively corrected.

Our review of the Department's FY 2000 Federal Managers' Financial Integrity Act (FMFIA) Report showed that NASS and the Office of the Chief Financial Officer did not report the lack of an adequate IT security management program. This material weakness should have been reported under Section 2 of the FMFIA Report.

RECOMMENDATION NO. 5

Develop a time-phased corrective action plan to address the weaknesses noted in this report. Provide quarterly updates to the OCIO on the status of corrective actions until all material problems are remediated.

Agency Response

NASS plans to have centralized configuration management for security implemented by October 1, 2001. We believe this will lead to a significant reduction in the number of security concerns currently identified. NASS will provide quarterly updates to the OCIO on June 30 and September 30, 2001 detailing the current implementation status for each of the recommendations presented in the OIG audit report.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 6

Take actions to comply with PDD-63 and OMB requirements by identifying NASS' MEI; performing a vulnerability assessment of the MEI; and establishing a remediation plan for correcting the vulnerabilities.

Agency Response

NASS will identify its mission essential infrastructure (MEI), assess the vulnerabilities associated with the MEI and establish a remediation plan for correcting vulnerabilities. NASS plans to be in full compliance with PDD-63

and OMB Circular A-130 by August 1, 2001.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 7

Perform risk assessments of NASS critical systems, and update the NASS Security Plan to include all areas required by OMB A-130 and the Department.

Agency Response

NASS will update the NASS Security Plan so that it includes all areas required by OMB Circular A-130 and the Department by August 1, 2001. NASS will perform a risk assessment of critical systems by September 1, 2001.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 8

Resolve the archival tape problems and resume off-site storage practices.

Agency Response

A backup system has been operational since October 1999. The system performs backups on a daily basis. In June 2000, we experienced a hardware failure that resulted in restoring the database back to March 2000. Some data was inaccessible following this failure. During this time period, the tapes normally retained off-site were kept in-house to aid the file restoration process. Steps were taken and the backup process was modified to retain a backup copy of the database. Since NASS recovered from this failure backups have been completed according to the established routine. This routine includes the system files. A review of the logs is completed daily to ensure that tape backups have occurred as scheduled. Off-site storage activities have returned to the normal.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 9

Prepare a comprehensive contingency plan and initiate procedures for annual testing of the plan.

Agency Response

NASS has prepared a contingency plan for the lockup area. The hardware and software required for implementing the lockup contingency plan have been acquired. The plan is scheduled to be tested during the next lockup.

There is a team currently working on a contingency plan for the state offices and headquarters LAN environment. They held their first meeting in Washington during the week of April 2. Draft recommendations should be available for review by May 1. NASS plans to begin implementing a contingency plan for the states and headquarters during the summer of 2001. There will be aspects of this implementation that will be budget dependent and will be implemented as budget is available. The initial implementation of this plan will be tested in February 2002. The plan will be tested annually in February thereafter.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 10

Establish a program to perform system certification/authorizations of all NASS critical systems in compliance with OMB A-130.

Agency Response

NASS feels that we evaluate current systems on an annual basis to ensure that adequate security controls are in place. NASS has reviewed OMB Circular A-130 and will perform the system certifications and authorizations required. NASS plans to be in full compliance with A-130 by August 1, 2001.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 11

Until appropriate corrective action is completed, report the lack of an effective IT security management program as a material weakness in the NASS FMFIA report.

Agency Response

NASS plans to have an effective IT security management program implemented and operational by September 30, 2001. However, if there are any portions of the program that have not been implemented at that time, or are questionable, NASS will report them under Section 2 of the Federal Managers' Financial Integrity Act (FMFIA) Report.

OIG Position

Management decision has been reached on this recommendation.

CHAPTER 3	NASS LOGICAL ACCESS CONTROLS NEED IMPROVEMENT.

FINDING NO. 3

NASS did not sufficiently ensure that only authorized users had access to its networks; that users were properly authorized to access network resources; and that users' access authority was not excessive as it relates to the performance of their job functions. Because SSO's were allowed to configure their individual systems, there was little oversight by headquarters personnel to ensure that access controls were functioning properly. Headquarters personnel stated that the access control weaknesses were overlooked in the daily operation of the computer system. In today's increasingly interconnected computing environment, inadequate access controls can expose NASS' critical data and operations to attacks of unauthorized disclosure, modification, or deletion of data by individuals with minimal computer or telecommunications resources and expertise.

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. During our review, we noted sufficient controls over the physical access to NASS' systems; however, we identified weaknesses in the logical controls over the systems. The lack of logical access controls exposes the agency's systems and data to unauthorized use, modification or deletion.

We found NASS systems contained accounts that belonged to users who were no longer employed. Further, we noted instances of user accounts and passwords being shared by numerous employees. These vulnerabilities occurred in some of NASS' most sensitive systems.

Our review of NASS' user accounts found two accounts still active for users no longer employed by NASS. We found one active account with system administrator[8] privileges that belonged to an employee who retired from NASS in May 2000. NASS subsequently contracted with this employee to work on a test database, but had not removed the user's administrative access, which included the ability to modify NASS' critical Estimates Database. Another NASS account, used to access its data at the National Information Technology Center, belonged to another retired NASS employee. We found that this account has been accessed after the retirement date of this employee. On investigating, NASS officials found that a current employee was using the account for routine NASS

[8] System Administrator privileges provide complete control and modification ability to the system.

business. They took immediate steps to ensure the account was properly converted for use by the current user.

We also identified 150 generic user accounts on the NASS LAN. Of the 150 generic accounts, 44 had access to NASS' critical Estimates Database. NASS allows the use of these accounts to avoid having to reestablish user-specific accounts for every statistical estimate reporting period. Generic accounts make it impossible for system administrators to track the actions of users in the event that inappropriate or malicious action is taken. NASS established procedures to require that the accounts be disabled when not in use and that they be assigned to an individual user; however, we found that NASS had not followed these procedures and allowed the accounts and the passwords to be shared by several users. Of the 150 generic accounts, NASS had only disabled 2 of them, even though our tests showed that 85 of the 150 accounts had expired passwords. Over half of the expired passwords were more than a year old, with 31 of them dating back as far as 1992. Further, these accounts were routinely established with global access privileges, which included the ability to create, modify, and erase files, and were not changed according to users' access requirements. Finally, one of these generic user accounts had the ability to grant rights to other users. The user of this account could circumvent the system administrator's ability to limit the access controls of these generic accounts.

RECOMMENDATION NO. 12

Immediately delete all accounts and access authorities, including application, program, and remote access for all separated employees.

Agency Response

NASS reviewed all user accounts on the Headquarters servers in Washington, D.C. and is in the process of reviewing the servers located in other offices. NASS deactivated 54 of the 150 generic accounts that had not been used since early 2000. These accounts will remain deactivated until September 2001 at which time they will be reviewed. If there is not a request for one of these accounts to be reactivated prior to September 2001, the account will be deleted from the server. The generic accounts that remained active are used on a frequent basis. We will document who has access to each generic account and change the password whenever someone no longer requires rights.

NASS evaluated all user IDs on the system and found a number of them that had become dormant over time. NASS disabled 21 of these accounts. These accounts will be deleted in September if there is no activity. NASS prefers to initially disable accounts because there may be files that will be required by the replacement as part of their job function. NASS will establish a policy, by June 1, requiring that accounts be disabled for 90 days and then deleted.

Only current NASS employees have accounts on the NASS Access Server that provides remote access to the NASS environment.

The ability for any non-supervisory user to grant rights to other users will be removed by May 1, 2000. NASS is in the process of removing the ability that certain NASS user IDs had that enabled them to grant rights to specific areas. As of May 1, 2001, only a centralized group will be able to grant rights. The requests for the modification of rights will need to be sent from a supervisor to the Technical Services Branch's official mailbox. This will centralize and coordinate the granting of rights and will provide a paper trail of the requests.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 13

Reduce the number of shared accounts to those needed and used on a regular basis. In addition, disable accounts not in use, and adjust the rights assigned to those accounts to each user's needs. Where shared accounts are needed, set expiration periods to a short timeframe to guard against misuse.

Agency Response

NASS is reviewing all shared accounts. A balance needs to be reached which provides flexibility for the usage of these accounts while simultaneously maintaining a high level of security. The Agency will begin disabling these accounts, in June, when they are not in use. NASS will limit the number of concurrent logins to one for these accounts during May.

OIG Position

Management decision has been reached on this recommendation.

RECOMMENDATION NO. 14

Review user privileges to ensure they are restricted to access required in the performance of the users job.

Agency Response

NASS has reviewed user privileges as part of the merging process. NASS is trying to implement containers (groups) representing the required activities. Privileges, or rights, are now being assigned to the container and staffs are included in the container. This makes it much easier to see what privileges are available and who has them. Staff are simply added or deleted from the container as assignment rotations occur and the privileges associated with the container remain unchanged.

NASS is in the process of evaluating and modifying the methodology currently used for rights. This activity will take time. Current access requirements must be reviewed and decisions made on the proper implementation so that users are not inadvertently denied access to information required for task completion. There are currently over 16,000 rights assigned. While this may imply a high level of security it is nearly unmanageable and very difficult to find exactly who has which rights to what. NASS is implementing numerous activities that will ensure that privileges are granted correctly. These activities are being implemented as part of the centralized configuration management.

OIG Position

Management decision has been reached on this recommendation.

EXHIBIT A – NASS Response To Draft Report

USDA

United States Department of Agriculture

National Agricultural Statistics Service

1400 Independence Avenue, SW
Washington, DC
20250-2000

April 30, 2001

TO: Richard J. Davis
Director
Administration Financial Division
Office of the Inspector General

FROM: R. Ronald Bosecker
Administrator

SUBJECT: Security Over Information Technology Resource at NASS

Attached are NASS's written comments pertaining to the discussion draft report, as requested.

The security at NASS is stronger today because of the findings that you pointed out. NASS appreciates the opportunities and benefits achieved through participation in these audits.

If you have any questions or concerns, please contact Rod DeSmet at (202) 690-2273.

NOTE: Portions of this response have been redacted due to inclusion of sensitive information.

FINDING NO. 1

TCP/IP System Vulnerabilities

NASS agrees with the number of high, medium and low vulnerabilities that were discovered during the OIG audit. NASS prioritized the seriousness of each and immediately began implementing changes which resulted in corrections of most of the vulnerabilities.

The largest risk that NASS faced was the incorrect configuration of a parameter on our firewall. This allowed users once on the USDA network access to the NASS Wide Area Network(WAN). However, this did not allow these users access to any NASS system. Users would have been required to provide a valid userid and password to access a NASS system. The incorrect configuration was researched and a fix was implemented. OIG was asked to rerun the tests, which they did, and they were unsuccessful in accessing the NASS WAN.

There were 71 high and medium risk vulnerabilities discovered through the testing of 104 NASS systems. Of these, there were numerous occurrences of the same vulnerability on multiple systems. For example, there were four (4) [ ], each with the same two (2) medium vulnerabilities which caused a total of 8 medium vulnerabilities. NASS has four (4) [ ], three (3) used for [ ] and a [ ]. There were 26 medium vulnerabilities found [ ], of which 11 were unique. Three of them occurred on all four (4) systems, one (1) occurred on three (3) systems, five (5) occurred on two (2) systems and one occurred on a single system. The three (3) [ ] were in the process of being implemented. All patches would have been implemented prior to moving these systems to production. The three (3) medium vulnerabilities found on the [ ] are similar in that NASS was in the process of updating the patches. There are patches released weekly [ ] and NASS implements the patches [ ]. The minimum password length was found to be insufficient because the parameter was not configured. There was a password associated with that system that passed the password length requirement.

The statement was made that "... the large number of low vulnerabilities identified, indicates the need to strengthen system administration." NASS understands the implications of this statement and is in the process of trying to strengthen our system administration. However, NASS also thinks that the 209 low risk vulnerabilities may lead to the wrong interpretation. NASS has corrected numerous low risk vulnerabilities. A number of them were corrected by correcting high and medium vulnerabilities. NASS wishes to point out that 66 of the low risk vulnerabilities were 27 unique occurrences. Also, there were 50 low risk vulnerabilities associated with the [ ] which were 6 unique occurrences.

In summary, NASS feels that we have fixed all of the high risk vulnerabilities and all but one (1) of the medium vulnerabilities. NASS has not found a satisfactory fix to the [ ] vulnerability [ ]. NASS has fixed numerous low risk vulnerabilities both directly and indirectly. NASS feels that the wording of the audit portrays a bad image based on the number of vulnerabilities and NASS does not agree with this. NASS feels that we had vulnerabilities and that we have and continue to take appropriate action to mitigate them.

NASS is in the process of creating a system that will allow centralized configuration management. NASS has been limited in its ability to do this in the past because of the decentralized environment [ ]. NASS specified policies and [ ] offices implemented them accordingly. However, something [ ] would change and someone would forget to reset the configuration parameter correctly. NASS has recently completed implementing a merged [ ] environment where [ ] security can be administered from a centralized point. [ ]. NASS will be able to centrally set and review configuration settings to ensure comparability across all NASS [ ].

Novell System Policies

NASS understands there were weaknesses in account restrictions, password strength and access controls. Again, it is pointed out that NASS needs to implement a configuration management system. A centralized configuration management system will allow NASS to ensure conformity across [ ].

There were 12 objects hidden from the system administrator. These objects have been removed as part of the merging process. These accounts did not have administrator access rights.

There were 49 accounts with administrator equivalences found in three (3) of the five locations tested. NASS is eliminating administrative equivalences with the merging process. NASS will be controlling administrative access through the use of groups. [

].

NASS is in the process of disabling dormant accounts. This has been a trade-off in the past due to the large number of phone enumerators who collect data for NASS. This group works on an infrequent basis and there has been a problem with them remembering their passwords since they may not work for months at a time. This group has very limited system rights with access only to the application that they use.

NASS has begun standardizing account information [ ] through the merging process. NASS was going to wait until the merging process was complete but decided with the vulnerabilities listed to go ahead for the merged [ ]. The standardization of account information was completed for all NASS locations during April. NASS has standardized the following: [

]. These changes have been implemented and are in agreement with 'Best Practices' [ ]. NASS is not able to require an [

]. NASS is still evaluating this option.

RECOMMENDATION NO. 1

NASS has implemented solutions to resolve all of the high vulnerabilities. NASS has resolved all of the medium vulnerabilities with the exception of [
].

RECOMMENDATION NO. 2

NASS has resolved over 50% of the 209 low vulnerabilities through both direct and indirect action. NASS continues to evaluate solutions for the low risk vulnerabilities which have not been resolved. There are some low risk vulnerabilities that NASS acknowledges and accepts the risks associated with using the product. NASS has mitigated the risks to an acceptable level through proper configuration [ ] (i.e., requiring a userid and password).

RECOMMENDATION NO. 3

NASS has discussed with the Department at the Chief Information Officer's staff meeting options for acquiring products to complete these scans. NASS is hesitant to go off and acquire a product that may be different than the direction that the Department might go. NASS believes that the Associate CIO for Cyber Security should be tasked with recommending products for vulnerability testing. At that point, Agencies may do what they like but if they choose the recommended product there would be some benefits such as expertise across Agencies, pricing efficiencies, etc. NASS understands the usefulness of these types of products and has allocated money in [ ] for these types of products. The OCIO has solicited interest from Agencies regarding the acquisition of [ ]. NASS has agreed to participate in this acquisition and has the money available for an October 1, 2001 acquisition. NASS will begin vulnerability testing of our network within 90 days of product acquisition, therefore about January 1, 2002. Once the initial testing is complete, NASS will be continue to conduct the tests on a quarterly basis. NASS will strive to resolve all high vulnerabilities within a week and medium vulnerabilities within three weeks. NASS will report high and medium risk vulnerabilities that are not resolved within 30 days to the OCIO.

RECOMMENDATION NO. 4

NASS is in the process of establishing configuration management. Configuration management is possible now with the NASS LAN appearing as a single entity through the merging process. NASS has just completed the merging process which enables our implementation of centralized configuration management. [

]. NASS will continue to review and standardize configuration parameters during May.

NASS is able to elevate several of the security settings to a level that [ ] will no longer

be able to modify. This should eliminate most of the current inconsistencies between [ ] in the future. NASS is adopting the 'Best Practices' thresholds [ ] for most of the configurable security settings. NASS will continue with this review and implementation during May.

NASS is in the process of reviewing roles which may allow us to define a specific role for specific responsibilities. This should allow better management and more flexibility in identifying and monitoring the various groups' activities because they would only be capable of performing required functions. For example, currently the [ ] for the LAN because part of their responsibility is to change passwords, but they require only the subset of supervisory rights necessary to change passwords. NASS plans to implement [ ] roles by July 1, 2001.

FINDING NO. 2

Finding 2, NASS Information Security Program Management Needs Improvement, contained seven of the 14 audit recommendations. NASS believed that we were in compliance with the numerous assessments and plans required since we had not been told by anyone that we were not. NASS followed Departmental guidance and responded to each of the various information requests. NASS only partially complied with some of the security requirements since we only responded to those areas that we knew about. NASS did not realize that we were in noncompliance and has begun working on those areas where additional requirements need to be satisfied.

RECOMMENDATION NO. 5

NASS plans to have centralized a configuration management program for security implemented by October 1, 2001. We believe this will lead to a significant reduction in the number of security concerns currently identified. NASS will provide quarterly updates to the OCIO on June 30 and September 30, 2001 detailing the current implementation status for each of the recommendations presented in the OIG audit report.

NASS has elevated [ ] as part of the merging process. [ ].

NASS has reduced the number of supervisory accounts by over 50%. Above the states will be the limited supervisory role for the [ ]. At a level just above the [ ] will be the [ ] and above the [ ] will be the security staff.

In terms of the security staff, NASS is forming a security team. There will be a team leader at the same level as the section heads for the sections supporting the LAN, WAN, UNIX and telecommunications environments. Team members will be the security staff and technical representatives [ ]. There will also be a staff resource identified for each of the major applications used in NASS. The people with application responsibilities will participate during activities such as system certification and assessment. This team will be defined during May and June.

RECOMMENDATION NO. 6

NASS will identify its mission essential infrastructure (MEI), assess the vulnerabilities associated with the MEI and establish a remediation plan for correcting the vulnerabilities. NASS plans to be in full compliance with PDD-63 and OBM Circular A-130 by August 1, 2001.

RECOMMENDATION NO. 7

NASS will update the NASS Security Plan so that it includes all areas required by OMB Circular A-130 and the Department by August 1, 2001. NASS will perform a risk assessment of critical systems by September 1, 2001.

RECOMMENDATION NO. 8

An [ ] backup system has been operational since October 1999. The system performs backups on a daily basis. In June 2000, we experienced a hardware failure that resulted in restoring [ ] back to March 2000. Some data was inaccessible following this failure. During this time period, the tapes normally retained off-site were kept in-house to aid the file restoration process. Steps were taken and the backup process was modified to retain a backup copy of the [ ]. Since NASS recovered from this failure backups have been completed according to the established routine. This routine includes the system files. A review of the logs is completed daily to ensure that tape backups have occurred as scheduled. Off-site storage activities have returned to the normal schedule.

RECOMMENDATION NO. 9

NASS has prepared a contingency plan for the lockup area. The hardware and software required for implementing the lockup contingency plan have been acquired. The plan is scheduled to be tested during the [ ].

There is a team currently working on a contingency plan for the state offices and headquarters LAN environment. They held their first meeting in Washington during the week of April 2. Draft recommendations should be available for review by May 1. NASS plans to begin implementing a contingency plan for the states and headquarters during the summer of 2001. There will be aspects of this implementation that will be budget dependent and will be implemented as budget is available. The initial implementation of this plan will be tested in February 2002. The plan will be tested annually in February thereafter.

RECOMMENDATION NO. 10

NASS feels that we evaluate current systems on an annual basis to ensure that adequate security controls are in place. NASS has reviewed OMB Circular A-130 and will perform the system certifications and authorizations required. NASS plans to be in full compliance with A-130 by August 1, 2001.

RECOMMENDATION NO. 11

NASS plans to have an effective IT security management program implemented and operational by September 30, 2001. However, if there are any portions of the program that have not been implemented at that time, or are questionable, NASS will report them under Section 2 of the Federal Managers' Financial Integrity Act (FMFIA) Report.

RECOMMENDATION NO. 12

NASS reviewed all user accounts on the Headquarters servers in Washington, D.C. and is in the process of reviewing the servers located in the states. NASS deactivated 54 of the 150 generic accounts that had not been used since early 2000. These accounts will remain deactivated until September, 2001 at which time they will be reviewed. If there is not a request for one of these accounts to be reactivated prior to September, 2001, the account will be deleted from the server. The generic accounts that remained active are used on a frequent basis. We will document who has access to each generic account and change the password whenever someone no longer requires rights.

NASS evaluated all userids on the system and found a number of them that had become dormant over time. NASS disabled 21 of these accounts. These accounts will be deleted in September if there is no activity. NASS prefers to initially disable accounts because there may be files that will be required by the replacement as part of their job function. NASS will establish a policy, by June 1, requiring that accounts be disabled for 90 days and then deleted.

Only current NASS employees have accounts on the NASS Access Server which provides remote access to the NASS environment.

The ability for any non-supervisory user to grant rights to other users will be removed by May 1, 2001. NASS is in the process of removing the ability that certain NASS userids had that enabled them to grant rights to specific areas. As of May 1, 2001 only a centralized group will be able to grant rights. The requests for the modification of rights will need to be sent from a supervisor to the Technical Services Branch's official mailbox. This will centralize and coordinate the granting of rights and will provide a paper trail of the requests.

RECOMMENDATION NO. 13

NASS is reviewing all shared accounts. A balance needs to be reached which provides flexibility for the usage of these accounts while simultaneously maintaining a high level of security. The Agency will begin disabling these accounts, in June, when they are not in use. NASS will limit the number of concurrent logins to one for these accounts during May.

RECOMMENDATION NO. 14

NASS has reviewed user privileges as part of the merging process. NASS is trying to implement containers (groups) representing the required activities. Privileges, or rights, are now being assigned to the container and staff are included in the container. This makes it much easier to see what privileges are available and who has them. Staff are simply added or deleted from the container as assignment rotations occur and the privileges associated with the container remain unchanged.

NASS is in the process of evaluating and modifying the methodology currently used for rights. This activity will take time. Current access requirements must be reviewed and decisions made on the proper implementation so that users are not inadvertently denied access to information required for task completion. There are currently over 16,000 rights assigned. While this may imply a high level of security it is nearly unmanageable and very difficult to find exactly who has which rights to what. The following activities will ensure that privileges are granted correctly and are being implemented as part of the centralized configuration management:

1. All [ ] will be removed for all non-TSB staff.
2. Create a [ ] role (password changes, intruder lockout, etc.).
3. Clean up trustee rights at the container level.
4. Remove individual file level access rights except where an actual requirement exists.
5. Remove all rights granted to supervisors because they are redundant.
6. Remove groups that duplicate containers and use the containers to assign rights.
7. Replace individual rights by granting rights to the section/branch container.
8. All requests for privileges will come from a supervisor to an official mailbox.

SUMMARY:

The security in NASS is better today because of the vulnerabilities pointed out in the OIG audit. However, security is a process requiring continuous monitoring and improvement. NASS finished the merging process during April 2001, at which time centralized configuration management began. NASS requests that OIG perform the same tests that were completed as part of the audit in [ ]. NASS would like to have these tests performed during May. The tests would validate the changes implemented for the various vulnerabilities and would provide a beginning point for centralized configuration management.

NASS has nominated staff to the OCIO to be included in the development and training activities currently underway for Risk Assessment Tools by the Department. NASS has also offered our telecommunications and UNIX environments for the pilot assessment program that will be conducted.

ABBREVIATIONS

FMFIA	Federal Managers' Financial Integrity Act
FY	Fiscal Year
IT	Information Technology
LAN	Local Area Networks
MEI	Mission Essential Infrastructure
NASS	National Agricultural Statistics Service
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PDD	Presidential Decision Directive
SSO	State Statistical Offices
TCP/IP	Transmission Control Protocol/Internet Protocol
USDA	United States Department of Agriculture
Y2K	Year 2000