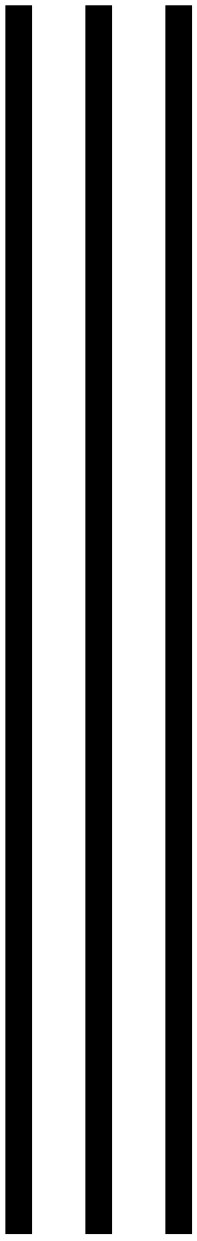


# U.S. Department of Agriculture
# Office of Inspector General
# Financial and IT Operations
# Audit Report

## INFORMATION SECURITY AT THE NATIONAL AGRICULTURAL STATISTICS SERVICE


**Report No.**
**26099-2-FM**
**March 2002**

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: March 25, 2002

REPLY TO
ATTN OF: 26099-2-FM

SUBJECT: Information Security at the National Agricultural Statistics Service

TO: R. Ronald Bosecker
Administrator
National Agricultural Statistics Service

This report presents the results of our audit of Information Security at the National Agricultural Statistics Service (NASS). You requested that we conduct this review to ascertain whether security breaches, alleged in paper e-mail messages brought to your attention in November 2001, actually existed. Nothing came to our attention during our review that indicated that the alleged security breaches had occurred or NASS data had been misused. While we did identify material weaknesses in the NASS network, nothing came to our attention during our review that indicated that NASS or its employees used those weaknesses for personal gain. 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 accepted management decisions on all recommendations. 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.

RICHARD D. LONG
Assistant Inspector General
for Audit

# EXECUTIVE SUMMARY

**INFORMATION SECURITY AT THE NATIONAL AGRICULTURAL STASTICS SERVICE**

**AUDIT REPORT NO. 26099-2-FM**

## RESULTS IN BRIEF

We initiated our review at the request of the National Agricultural Statistics Service (NASS) management to verify whether (1) its employees had used its electronic mail (e-mail) system to prepare and send three sets of e-mails, which contained racially derogatory language and alleged security breaches within NASS' network; and (2) security breaches alleged in those e-mails actually occurred. The e-mails were brought to the attention of NASS management after two current NASS employees said they received them in hard copy through the U.S. Postal Service. NASS management immediately requested that we conduct a review to determine whether the e-mails and the security breaches alleged in those e-mails were legitimate. We conducted our review in January and February 2002. Nothing came to our attention during our review that indicated that the e-mails had been initiated using the NASS e-mail system, and that the security breaches alleged in those e-mails had occurred, or that any NASS data had been misused. Further, while we did identify material weaknesses in the administration of NASS' network as discussed below, nothing came to our attention during our review that indicated that NASS or its employees used those weaknesses for personal gain.

Our vulnerability scans of selected NASS network devices disclosed vulnerabilities that could be exploited from within NASS' network, and some that can be exploited externally. NASS had taken action on our prior audit recommendation by acquiring one of the vulnerability assessment tools that we used during our audit; however, NASS just began to use the tool and had not fully implemented the use of the tool in its efforts to identify and eliminate security vulnerabilities within its network.

We found that NASS needs to strengthen its firewall administration and increase security over remote access to its network resources. Due to other priorities placed on its security staff, NASS does not have controls in place to keep its firewall configuration current by periodically reviewing and modifying its firewall rules, and has not ensured that the firewall

administrator receives proper training in its configuration. In addition, NASS' current remote access policy reduces the effectiveness of its firewall by allowing users unauthenticated access through it.

We also found that NASS did not ensure that only authorized users had access to its network. NASS had not implemented adequate written procedures to ensure that it timely removed user accounts for those persons that left NASS employment, and had accepted the risk of using generic user accounts on its network. As a result, persons no longer employed at NASS or anyone with knowledge of the generic user accounts could inappropriately access and potentially destroy critical NASS data.

Finally, NASS needs to report the material internal control weaknesses we have identified in its Federal Manager's Financial Integrity Act (FMFIA) report. It also needs to establish goals and performance measures in its Government Performance and Results Act (GPRA) report that relate to securing its information technology resources and data.

## KEY RECOMMENDATIONS

We recommended that NASS:

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

- Develop and implement a policy to periodically review the firewall configuration and remove or modify firewall rules as necessary.

- Implement a virtual private network solution with smart card or token authentication and strong encryption for remote access to the internal NASS network.

- Ensure that NASS' security staff is properly trained to configure and maintain the firewall rule base to ensure the appropriateness of firewall rules.

- Establish and implement procedures to periodically reconcile user accounts on the NASS networks to current employee listings, and take immediate action to remove those accounts no longer needed.

- Discontinue the use of all generic user accounts on the NASS network. Establish accounts on an as-needed basis and assign individual responsibility to those accounts.

- Report the material control weaknesses identified in this report, including the noncompliance with Office of Management and Budget Circular A-130 and Presidential Decision Directive 63 in its FMFIA report.

- Establish performance goals and measures relating to information technology security in its GPRA report.

## AGENCY RESPONSE

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

## OIG POSITION

We concurred with NASS' proposed corrective actions.

# 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. This environment poses a threat to the sensitive and critical operations of the National Agricultural Statistics Service (NASS).

NASS administers the U.S. Department of Agriculture's (USDA) program of collecting, compiling, and disseminating current national, State, and county 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 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, 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."

In May 2001, we issued our report on the security over NASS' information technology (IT) resources.[1] That audit was initiated as a part of a nationwide audit of IT security within the Department. We reported that NASS' network was vulnerable to the threat of internal and external intrusion, was not in compliance with federally mandated requirements for managing its IT resources, and had not ensured that only authorized users had access to its network resources. We recommended that NASS periodically scan its network for vulnerabilities, ensure compliance with federally mandated security requirements, and ensure that only authorized users had access to its network. NASS agreed with our recommendations and immediately took action toward correcting the identified weaknesses.

Toward the end of that review, two NASS employees contacted the Office of Inspector General (OIG) whistleblower hotline and reported the existence of weaknesses in the NASS network. We contacted the two employees to determine the nature of the weaknesses; however, at that time they refused to discuss the specifics surrounding their concerns at the advice of their legal council.

Since that review, the two NASS employees said they received, through the U.S. Postal Service mail, a series of e-mails containing racially derogatory statements and citing backdoors in the NASS' firewall configuration, and the existence of 'special user' accounts and 'corporate friends.' In November 2001, NASS officials requested that OIG conduct a review to ascertain whether the alleged security breaches existed.

## OBJECTIVES

The objectives of this audit were to (1) verify whether e-mails that contained racially derogatory comments and allegations of

[1] Audit Report No. 26099-1-FM, "Security Over Information Technology Resources at the National Agricultural Statistics Service," dated May 14, 2001.

security weaknesses in the NASS network had been prepared by NASS employees using the agency's e-mail system; (2) whether the security breaches alleged by those e-mails actually occurred; (3) follow up on the agency's progress in correcting the audit findings from our prior NASS IT audit; (4) determine the adequacy of security over the Local and Wide Area Networks; (5) determine if adequate logical and physical access controls exist to protect computer resources against unauthorized modification, disclosure, loss, or impairment; and (6) address any NASS management concerns.

## SCOPE

We restored and reviewed the contents of selected NASS network server backup tapes within the October 1998 through December 1999 timeframe containing e-mail databases and user e-mail archives. We reviewed NASS' progress in implementing the recommendations made in our prior report. We also 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. We used commercial software applications to assist us in our security reviews of numerous NASS network components.

The audit was conducted in accordance with "Government Auditing Standards." Our testing was performed during January and February 2002.

## METHODOLOGY

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

- We restored and reviewed e-mail databases and user archives from NASS backup tapes to ascertain whether NASS employees prepared and sent certain e-mails using its e-mail system.

- We reviewed the firewall and router configurations to determine whether adequate security measures had been implemented by NASS to protect its IT resources.

- We interviewed the two NASS employees that had called the OIG whistleblower hotline to obtain an understanding of their concerns regarding the security over NASS' IT network environment.

- We interviewed the current NASS employees named in the e-mails to determine whether they prepared or received those e-mails, or if they had any information relating to the allegations cited in those e-mails

regarding security breaches within the NASS network.

- We reviewed IT security policies and procedures issued by Office of Management and Budget (OMB), the Department, and NASS, to ensure NASS' compliance with existing IT security requirements.

- We performed detailed testing of NASS' entity-wide security program, analyzed logical access controls at the NASS headquarters, and by analyzing records and controls established to ensure that the security of the NASS' computer systems were sufficient and that controls were functioning as intended.

- We interviewed NASS officials responsible for managing the agency's computer systems to obtain an understanding of the management of its IT resources.

- We conducted vulnerability scans of the systems located in the NASS headquarters' network to assess the threat of network penetration.

# FINDINGS AND RECOMMENDATIONS

| CHAPTER 1 | MISUSE OF NASS IT RESOURCES COULD NOT BE SUBSTANTIATED |
|---|---|

## FINDING NO. 1

We initiated our review at the request of NASS management to (1) verify whether its employees had used its e-mail system to prepare and send three sets of e-mails, which contained racially derogatory language and alleged security breaches within NASS' network; and (2) verify whether the security breaches alleged in those e-mails actually occurred. Those e-mails were brought to the attention of NASS management after two current NASS employees said they received them in hard copy through the U.S. Postal Service. NASS management immediately requested that we conduct a review to determine whether the e-mails and the security breaches alleged in those e-mails were legitimate.

With the assistance of NASS staff, we restored selected backup tapes dated October 30, 1998; November 27, 1998; April 30, 1999; May 28, 1999; and one set containing December 2000 archives. However, not all the backup tapes from the time period of the e-mails existed and were not available for our review. NASS had only a 13-month retention policy for backup tapes; therefore, NASS employees took older tapes and reused them as needed. Those tapes we chose to restore contained NASS' e-mail database or user-archived e-mails that should have provided us the ability to determine whether the e-mails, dated October 1998, April 1999, and December 1999, were present in the existing NASS backup tapes. We also conducted a review of the e-mail archives of a former NASS employee that were provided to us by the two current NASS employees who said that they received the questioned e-mails. Our review efforts consisted not only of searching for the exact e-mails, but also searching for the existence of approximately 20 key words and phrases. Searching for these words and phrases would indicate the additional use of racially derogatory language, or the existence of additional security breaches similar to those alleged in the e-mails such as 'back doors' in the firewall, 'special user' accounts, or the existence of 'corporate friends.'

We also interviewed the two NASS employees who said they received the hard copy e-mails through the U.S. Postal Service. They discussed with

us their concerns over the security of NASS network resources, which we have addressed elsewhere in this report; however, they informed us that they had no knowledge of the specific security breaches alleged in the e-mails. We contacted these two employees prior to the issuance of our previous audit after they had contacted our whistleblower hotline. At that time, and at the advice of their legal council, they refused to provide us specifics of their concerns over the security of NASS' network.

We also interviewed the current NASS employees that were named in the e-mails. Each of the employees individually stated that they had not seen, received, or written the e-mails. Further, the employees had no knowledge of any 'back door' in the NASS firewall, 'special user' accounts, or 'corporate friends,' as alleged in the e-mails.

In conclusion, the backup tapes we reviewed did not contain the questioned e-mails. Because only a limited number of backup tapes existed, we cannot say with certainty whether or not the e-mails actually originated from the NASS e-mail system. However, nothing came to our attention during our review that indicated that the e-mails had been initiated using the NASS e-mail system, that additional e-mails containing racially derogatory comments existed, that the security breaches alleged in those e-mails had occurred, or that any NASS data had been misused. Finally, while we did identify material weaknesses in the administration of NASS network, nothing came to our attention during our review that indicated that NASS or its employees used those weaknesses for personal gain.

| CHAPTER 2 | VULNERABILITIES COULD EXPOSE NASS SYSTEMS TO THE RISK OF MALICIOUS ATTACKS FROM INTERNAL AND EXTERNAL THREATS |
|---|---|

## FINDING NO. 2

Our vulnerability scans of selected NASS network devices disclosed vulnerabilities that could be exploited from within NASS' network, and some that can be exploited externally. NASS had taken actions to implement the recommendations we made in our prior audit report by acquiring one of the vulnerability assessment tools that was used during our audit; however, NASS just began to use the tool prior to our audit and had not fully implemented the use of the tool in its efforts to identify and eliminate security vulnerabilities within its systems. NASS has begun to correct the vulnerabilities we identified; however, until it completes its own scanning process, NASS' systems and networks could be vulnerable to cyber-related attacks.

The 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.

We conducted our assessment of selected NASS network components in January and February 2002. We utilized two commercial off-the-shelf software products, one designed to identify over 1,000 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 NASS' Washington, D.C. offices. These scans included 46 NASS network components. Our assessments revealed 92 high and medium-risk vulnerabilities.[3] In addition, we identified 139 low-risk vulnerabilities. The high and medium vulnerabilities, if left uncorrected, could allow unauthorized users access to NASS data. While NASS took corrective action to eliminate the

[2] The TCP/IP is a series of protocols originally developed for use by the U.S. 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.

vulnerabilities we identified in our last review, many of the high and medium-risk vulnerabilities we identified in this review were on systems that we had not previously scanned or on systems that NASS had placed into production since our prior review. Further, since our prior review, the software tool we used had been updated to identify an additional 200 vulnerabilities that had not been known to exist during our prior review. NASS recently purchased the same vulnerability scanning tool that we used and had just begun to integrate it into its overall security management process at the time of our review. To fully benefit from this tool, NASS needs to implement written policies to scan and mitigate the identified vulnerabilities.

In addition to our review, NASS contracted with a private-sector firm to review its network security and its remote access policy. That contractor was able to successfully compromise NASS' network using a well-known vulnerability that existed on one of its systems. The contractor made several recommendations to strengthen NASS' network security and remote access policies. NASS agreed with those recommendations and has begun to address them.

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 NASS data.

- Two commonly used programs used to transfer files and perform remote administration were configured with default passwords. An attacker could use these programs to install and execute malicious software on this system that could affect other systems within the network.

We also conducted our scans through the firewall established by NASS as protection between NASS' systems and the departmental telecommunications network. Through the firewall, we identified 16 high and medium-risk vulnerabilities and 8 low vulnerabilities. These vulnerabilities may be exploitable by malicious users outside the NASS network, including the global Internet. Finally, in addition to the vulnerabilities identified by our scans, we found weak user passwords on several of NASS' systems.

Novell System Policies

We conducted a detailed assessment of the security of NASS' Novell network at its headquarters office. 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 that NASS had corrected several vulnerable areas in its Novell network since our prior audit, including removing administrative authorities of those users that no longer needed them, and increasing user account password strength requirements. However, weaknesses in account restrictions and access controls still exist because NASS was still in the process of fully implementing our prior audit recommendations. These two areas define a user's ability to access the system. NASS does not have a vulnerability assessment tool for its Novell networks, but officials expressed the need to obtain an assessment tool similar to the one we used. Some of the weaknesses we found included:

- User accounts were hidden from the system administrator. Because they are hidden, these accounts may not be subject to the same type of review as other accounts and may not be timely removed when no longer needed. Hidden accounts should not be used as they provide an additional means for unauthorized and potentially unmonitored access to the network. This vulnerability is nearly impossible to identify without the assistance of an analysis tool similar to the one we used.

- An excessive number of accounts had not been accessed within 90 days. We identified 168 of these accounts, 97 of which had not been disabled by the systems administrator. 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.

We provided NASS officials with the vulnerability assessment reports. NASS officials informed us that they had begun addressing the vulnerabilities.

## RECOMMENDATION NO. 1

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

**Agency Response**

NASS agreed that the vulnerabilities found during the audit pose a potential threat to its network. NASS prioritized the vulnerabilities and concentrated on those that were present outside, or external, to its network. NASS had already mitigated nearly all of the vulnerabilities exploitable from outside its network and many of those that were exploitable from within its network. NASS will make every attempt to mitigate the remaining high and medium-risk vulnerabilities by April 19, 2002, and low-risk vulnerabilities by May 10, 2002. NASS will provide follow up notification to the Chief Financial Officer and Office of the Chief Information Officer if it fails to successfully mitigate all high and medium-risk vulnerabilities by April 19, 2002.

**OIG Position**

We accept the management decision on this recommendation.

## RECOMMENDATION NO. 2

Implement a written policy to periodically conduct vulnerability scans on all network resources, and ensure that the vulnerabilities identified are timely mitigated.

**Agency Response**

NASS understand the importance of conducting periodic vulnerability assessments. NASS participated in the Department's acquisition of vulnerability assessment software in October 2001. NASS plans to complete training in this software's usage as soon as possible with the intention of beginning network scans during the spring of 2002. NASS has prepared a Security Policy Directive requiring scans of the NASS network on a monthly basis and directs staff to mitigate all high and medium-risk vulnerabilities within two weeks.

**OIG Position**

We accept the management decision on this recommendation.

## RECOMMENDATION NO. 3

Ensure corrective action is taken on all the vulnerabilities identified in NASS' Novell operating system, especially those pertaining to account restrictions and access controls.

**Agency Response**

NASS has reviewed the user accounts which have not been accessed for 90 days or more. NASS has deleted 32 of these accounts and disabled an additional 61 totaling 93 of the 97 accounts that had not been accessed for 90 days or more. The remaining four accounts are tied to application software systems and need to be present when problems are encountered. The disabled accounts will be evaluated during April 2002, to determine if they can be permanently deleted from the system.

**OIG Position**

We accept the management decision on this recommendation.

## RECOMMENDATION NO. 4

Obtain the software and implement a policy to periodically scan its Novell systems to identify configuration weaknesses in that operating system.

**Agency Response**

NASS is currently obtaining prices for a software tool that will allow the agency to perform assessments of our Novell servers. The assessment software will be acquired by NASS in April 2002.

**OIG Position**

We accept the management decision on this recommendation.

| CHAPTER 3 | NASS NEEDS TO STRENGTHEN ADMINISTRATION OF ITS FIREWALL AND IMPROVE REMOTE ACCESS PROCEDURES |
|---|---|

## FINDING NO. 3

NASS needs to strengthen its firewall administration and increase security over remote access to its network resources. Due to other priorities placed on its security staff, NASS does not have controls in place to keep its firewall configuration current by periodically reviewing and modifying its firewall rules, and has not ensured that the firewall administrator receives proper training in its configuration. In addition, NASS' current remote access policy reduces the effectiveness of its firewall and its other security measures by allowing unauthenticated access through its firewall. This and the effects of the weak logical access controls we identified in Finding No. 4, places NASS' network at risk of compromise.

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. Agencies are required to establish controls to assure adequate security for all information processed, transmitted, or stored.

Firewall Configuration

Our review found that NASS has not established controls to periodically review its firewall configurations to ensure that they are kept current and that user accounts on the firewall system are kept to a minimum and are properly disabled or removed when not needed. On one of its firewalls, we found that the NASS security staff overlooked generic system user accounts that had not been properly disabled. Further, we found that a former employee responsible for administering the firewall, who resigned in December 2001, still had a user account on the firewall system. We later confirmed that this former employee's account had been disabled; however, it should have been removed. In addition, we identified firewall rules that allowed specific Internet Protocol (IP) addresses access to the firewall. These IP addresses were needed when one of NASS' employees, located in a remote office, was assisting in the configuration of the firewall over two years ago. That employee is no longer with NASS; therefore, those IP addresses should have been removed from those rules. We consider this a material weakness.

We also found that NASS had provided its security staff with only limited training on the proper configuration of its firewalls. While the security staff were the only ones allowed to enter or change firewall rules, they relied heavily on the NASS technical staff for guidance on what rules should be entered and how to enter them. Without proper training, the security staff was not sufficiently knowledgeable about firewall configurations to question the legitimacy or appropriateness of the rules being entered.

Remote Access

NASS has adopted a flexible workplace policy that allows its employees to work from their homes on a limited basis. Some of the employees have acquired high-speed Internet access for their homes providing them with faster and more efficient access to the NASS network than the older dial-up connections. To facilitate this, NASS configured its firewall to allow its employees to gain access to its network using two commercially available remote access software packages. This configuration circumvents one additional layer of authentication normally required of remote users that connect to NASS' network using its dial-in access server. NASS users still need to provide user identification and a password for the remote access software, along with an additional password for their network login. However this configuration allows anyone with these two programs to scan NASS' network attempting to connect to its systems, providing an opportunity to try guessing user names and passwords to gain entry. While NASS has provided its users with remote access software setup instructions that require passwords and the encryption of the data transmitted, NASS does not have any control over how the users ultimately decide to establish their connections. We consider this a material weakness.

NASS should implement a virtual private network (VPN) solution and require smart card or token authentication for those sessions. Users would have to provide a user name, password, and an un-shareable token before access through the firewall could be granted. Further, through the use of a VPN, NASS could be assured that the data transmitted over the Internet would be encrypted, preventing unauthorized disclosure of any sensitive data transmitted. Finally, NASS would have more control over how this environment is configured and could control who has the authority to use the remote access software to gain entry into the NASS network.

We discussed these issues with NASS management. They have agreed with our position and have begun procuring a smart card or token authorization system to implement with a VPN solution.

## RECOMMENDATION NO. 5

Develop and implement a policy to periodically review the firewall configuration and remove or modify firewall rules as necessary.

**Agency Response**

NASS has acquired new enterprise firewalls which are compatible with the Department's firewall solution. NASS has taken steps to reduce the number of individual firewall rules which directly reduces the work associated with firewall management. NASS will be reviewing all firewall rules as the implementation of the new firewalls proceeds and will eliminate unnecessary rules at that time. NASS plans to have the new firewalls operational in May 2002.

A Security Policy Directive has been approved which documents firewall configuration and management. This directive discusses the process for adding, deleting and modifying firewall rules. It also addresses the issue of periodically reviewing the firewall rules which have been implemented.

**OIG Position**

We accept the management decision on this recommendation.

## RECOMMENDATION NO. 6

Implement a VPN solution with smart card or token authentication and strong encryption for remote access to the internal NASS network.

**Agency Response**

NASS contracted with a private-sector firm, who along with OIG, recommended NASS implement advanced authentication measures for remote access. NASS has taken the first step in this process with the acquisition and implementation of modern firewall technology. NASS plans to implement a system providing advanced authentication for remote access following the implementation and testing of the new firewalls. The implementation of an advanced authentication system is expected to begin in July 2002.

**OIG Position**

We accept the management decision on this recommendation.

## RECOMMENDATION NO. 7

Ensure that NASS' security staff is properly trained to configure and maintain the firewall rule base to ensure the appropriateness of firewall rules.

**Agency Response**

NASS included a training requirement, as well as assistance with configuration and implementation of the new firewalls, as part of the recent firewall acquisition. This training will ensure that the security staff is well versed in firewall management and the generation and modification of rules. As stated in its response to Recommendation No. 5, NASS plans to have the new firewalls operational in May 2002.

**OIG Position**

We accept the management decision on this recommendation.

| CHAPTER 4 | NASS NEEDS TO STRENGTHEN ITS LOGICAL ACCESS CONTROLS |
|---|---|

## FINDING NO. 4

NASS did not ensure that only authorized users had access to its network. NASS had not implemented adequate written procedures to ensure that it timely removed user accounts for those persons that left NASS employment, and had accepted the risk posed by the use of generic user accounts on its network. As a result, persons no longer employed at NASS or anyone with knowledge of the generic user identifications (ID) could inappropriately access and potentially destroy critical NASS data.

Department Manual 3140-1.6, ADP Security Manual, (part 6 of 8), Appendix D, Section 4a, requires agencies to use individual user IDs and passwords to control access to systems processing personnel, financial, market-related, or other sensitive data. Section 6c, specifically prohibits issuance of group logon IDs and passwords and prohibits the sharing of the same. Section 6c also requires security staff to remove employee user ids and passwords when the employee is no longer with the agency.

In our prior report of IT security at NASS,[4] we found that NASS had 3 user accounts on its network that belonged to persons no longer employed by NASS, and 150 generic user accounts that could have been used by several persons. We recommended that NASS reduce the number of generic user accounts, disable those that are not in use, and ensure that the privileges of those accounts are not excessive. While NASS disabled 54 of the 150 generic user accounts we identified, NASS chose to accept the risk that these generic user accounts pose in order to provide its staff easier administration of accounts that are used only temporarily by any one person.

Generic accounts do not provide for individual responsibility and make it impossible for system administrators to track the actions of the users of those accounts in the event that inappropriate or malicious actions are taken. Further, the existence of generic user accounts provides additional accounts that a malicious user could use to gain unauthorized access to network resources and data.

In our current review, we found that NASS had not removed the user accounts for six persons no longer employed by NASS, five of which had

[4] Audit Report No. 26099-1-FM, "Security Over Information Technology Resources at the National Agricultural Statistics Service," dated May 14, 2001.

not been disabled. NASS needs to establish a formal reconciliation process to ensure that separated employees are timely removed from its network. In addition, we found 228 generic user accounts, which represented over 38 percent of the total number of user accounts on NASS' headquarters network. We consider this a material weakness.

NASS officials informed us that they use a majority of these generic accounts for people needing access to the network on a rotating basis, eliminating the need for NASS network administrators to delete and recreate a user account every time one is needed. However, due to the sensitive nature of the data that NASS maintains, we believe that it should discontinue the use of shared, generic user accounts, and create user accounts when needed that provide for individual responsibility.

## RECOMMENDATION NO. 8

Establish and implement procedures to ensure that separated employee's user accounts are timely removed from the NASS network.

**Agency Response**

NASS attempts to disable separated user accounts in a timely manner. There are occasions when user accounts are left active, for example, managers may need to move files to a new employee now responsible for a recently separated employee's activities. NASS distributes personnel summaries which provide information concerning employees that are recently hired, separated, and transferred. The security staff will be added to the distribution list for this summary in April 2002. Additionally, the security staff will ask NASS' personnel office for a listing of all separated and transferred employees on a quarterly basis beginning in April 2002. This should ensure that NASS remains current in disabling accounts for those employees who no longer require access to the network.

**OIG Position**

We agree with NASS' proposed actions.

## RECOMMENDATION NO. 9

Establish and implement procedures to periodically reconcile user accounts on the NASS networks to current employee listings, and take immediate action to remove those accounts no longer needed.

**Agency Response**

NASS security staff will ask the personnel office for a listing of current employees on a quarterly basis beginning in April 2002. This listing will be used to reconcile current employees with current network user accounts.

**OIG Position**

We agree with NASS' proposed actions.

## RECOMMENDATION NO. 10

Discontinue the use of all generic user accounts on the NASS network. Establish accounts on an as-needed basis and assign individual responsibility to those accounts.

**Agency Response**

NASS agrees there is a degree of risk associated with allowing generic user accounts. NASS has disabled an additional 32 of these generic user accounts and deleted another 20. NASS is in the process of switching from generic user accounts to specific individual accounts for infrequent users. NASS plans to be totally switched from generic user accounts to individual accounts by September 30, 2002.

**OIG Position**

We accept the management decision on this recommendation.

| CHAPTER 5 | FURTHER ACTIONS NEEDED TO COMPLY WITH FEDERALLY MANDATED SECURITY REQUIREMENTS |
|---|---|

## FINDING NO. 5

As reported in our prior audit, NASS has not completed all the necessary risk assessments of its systems, adequately planned for network and system contingencies, or properly certified to the security of its major systems. NASS has begun and continues to take the necessary actions toward compliance. Since NASS relies on its IT infrastructure to supply market-sensitive data on commodities to the agricultural economy, it needs to promptly complete its planned actions to ensure compliance with these federally mandated requirements.

OMB Circular A-130, Appendix III, "Security of Federally 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, Presidential Decision Directive (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. Finally, the Government Performance and Results Act (GPRA) of 1993 requires agencies to establish annual performance plans and measurable performance goals relating to its operations.

In our prior audit, we reported that NASS' security plan did not include all the required elements outlined in OMB Circular A-130, that it had not completed risk assessments for all of its major systems, had not properly planned for contingencies by establishing a comprehensive disaster recovery plan, or properly certified to the security controls in its major systems. We recommended that NASS take actions to ensure compliance with these requirements including implementing a time-phased plan to correct the deficiencies. NASS agreed with our recommendations and agreed to complete its compliance with these requirements by August 2001. While NASS missed that timeframe, our review showed that it continues to take the necessary steps toward compliance. At the time of our review, NASS had updated its security plan; completed risk assessments for 2 of its systems, its network and 1 of the 10 systems

identified in its security plan; and designed disaster recovery procedures for its field and headquarters offices.

Since NASS is in the process of complying with these federally mandated requirements and the recommendations we made in our prior report, we are making no further recommendations on these issues in this report. However, until such time that NASS has completed compliance with these requirements, NASS needs to include this material weakness, and those addressed elsewhere in this report, in its Federal Manager's Financial Integrity Act (FMFIA) report. Further, we believe that these weaknesses require NASS to establish measurable performance goals relating to securing its IT resources in its GPRA report.

## RECOMMENDATION NO. 11

Report the material control weaknesses identified in this report, including the noncompliance with OMB Circular A-130 and PDD 63 in its FMFIA report.

**Agency Response**

NASS is attempting to comply with the requirements of OMB Circular A-130. NASS spent a great deal of time during fiscal year 2001 trying to get the security plan in compliance with OMB Circular A-130 and PDD 63. Until compliant, NASS will report this material control weakness in it annual FMFIA report.

**OIG Position**

We accept the management decision on this recommendation.

## RECOMMENDATION NO. 12

Establish performance goals and measures relating to IT security in its GPRA report.

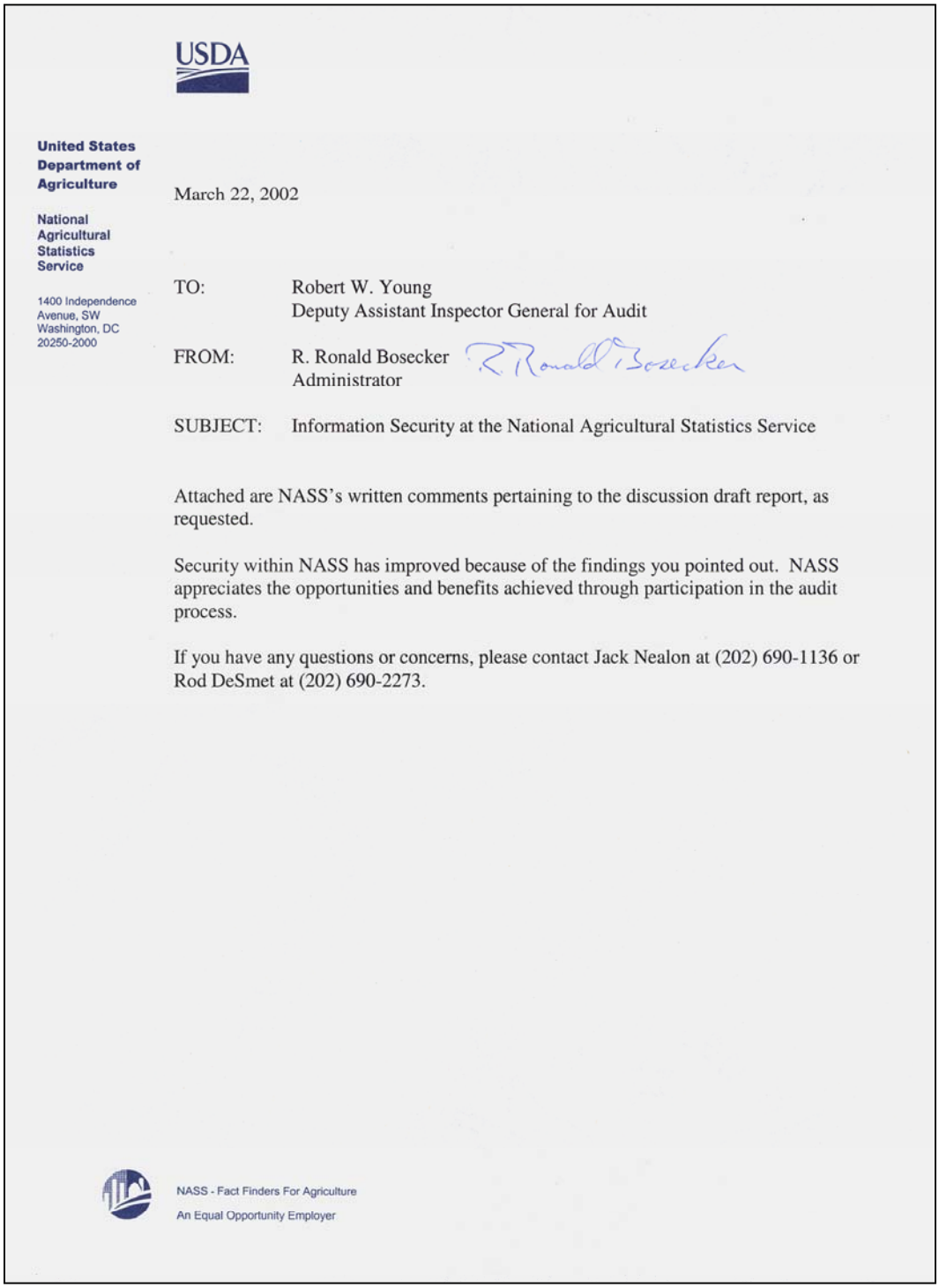
**Agency Response**

NASS is in the process of developing the agency's fiscal year 2003 Annual Performance Plans as required under GPRA. NASS is defining a performance goal and associated measures to be included in this report. NASS will establish it goals and begin to measure its performance in July 2002.

**OIG Position**

We agree with NASS' actions on this recommendation.

## EXHIBIT A – NASS RESPONSE TO THE DRAFT REPORT



USDA

United States Department of Agriculture

National Agricultural Statistics Service

1400 Independence Avenue, SW
Washington, DC
20250-2000

March 22, 2002

TO: Robert W. Young
Deputy Assistant Inspector General for Audit

FROM: R. Ronald Bosecker
Administrator

SUBJECT: Information Security at the National Agricultural Statistics Service

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

Security within NASS has improved because of the findings you pointed out. NASS appreciates the opportunities and benefits achieved through participation in the audit process.

If you have any questions or concerns, please contact Jack Nealon at (202) 690-1136 or Rod DeSmet at (202) 690-2273.

NASS - Fact Finders For Agriculture
An Equal Opportunity Employer

Recommendation No. 1

NASS agrees that the vulnerabilities found during the audit pose a potential threat to our network. NASS prioritized the vulnerabilities and concentrated on those that were present outside, or external, to our network. NASS feels that these vulnerabilities pose the greatest threat to the Agency. There were 16 high and medium-risk vulnerabilities and 8 low-risk vulnerabilities discovered. NASS has eliminated 15 of the 16 high and medium vulnerabilities and one of the 8 low-risk vulnerabilities. Five of the remaining 7 low-risk vulnerabilities that have not been mitigated are associated with the remote access software being loaded on systems internal to NASS. NASS understands the risk associated with remote access and plans are underway to augment remote access with advanced authentication. NASS continues to work on the single unresolved medium-risk and two low-risk external vulnerabilities.

NASS is also progressing with remedies to the vulnerabilities discovered which are internal to the NASS network. There were 92 high and medium-risk vulnerabilities discovered on the NASS internal network. The exploitation of these vulnerabilities require internal access to the NASS network either by physically gaining access to a NASS facility or via remote access. NASS has eliminated 26 of the 92 high and medium-risk vulnerabilities. NASS will make every attempt to mitigate the remaining high and medium-risk vulnerabilities by April 19, 2002. There were 139 low-risk vulnerabilities found internal to the NASS network. NASS has eliminated 35 of these vulnerabilities and is attempting to mitigate the remaining low-risk vulnerabilities by May 10, 2002.

NASS will notify the USDA Chief Financial Officer and Chief Information Officer of our progress on April 4. NASS will provide a followup notification to these individuals if we fail to mitigate all high and medium-risk vulnerabilities by the April 19 completion date.

Recommendation No. 2

NASS understands the importance of conducting periodic vulnerability assessments. It is very easy to introduce vulnerabilities into the network with operating system and application software changes. In addition, the assessment software is continually enhanced to discover new types of vulnerabilities. NASS participated in the Department's acquisition of vulnerability assessment software in October, 2001. NASS is currently reviewing training options for our security staff regarding the configuration and use of this software to enable them to begin performing the network scans. NASS plans to complete training in this software's usage as soon as possible with the intention of beginning network scans during the spring of 2002. Performing the actual scans is just one part of a sound vulnerability assessment program. A documented plan must exist which defines both the execution of the scans and resulting actions. A Security Policy Directive has been prepared and approved. This Directive requires scans of the NASS network be executed on a monthly basis. It further directs the security staff, upon completion of the scan, to mitigate all high and medium-risk vulnerabilities within two weeks.

Recommendation No. 3

NASS has reviewed the user accounts which have not been accessed for 90 days or more. NASS has deleted 32 of these accounts and disabled an additional 61 totaling 93 of the 97 accounts that had not been accessed for 90 days or more. The remaining four accounts are tied to application software systems and need to be present when problems are encountered. The disabled accounts will be evaluated during April to determine if they can be permanently deleted from the system.

Recommendation No. 4

NASS is currently obtaining prices for a software tool that will allow the Agency to perform assessments of our Novell servers. The assessment software will be acquired by NASS in April.

Recommendation No. 5

NASS has acquired new enterprise firewalls which are compatible with the Department's firewall solution. In addition, NASS recently began utilizing the Department's virus checking system for e-mails. The utilization of the virus checking system allows NASS to remove Simple Network Management Protocol (SNMP) firewall access that had been granted to other USDA Agencies with whom NASS has entered into telecommunications optimization and consolidation agreements. The removal of this e-mail access will greatly reduce the number of individual firewall rules which directly reduces the work associated with firewall management. NASS will be reviewing all firewall rules as the implementation of the new firewalls proceeds and will eliminate unnecessary rules at that time. NASS plans to have the new firewalls operational in May, 2002.

A Security Policy Directive has been approved which documents firewall configuration and management. This Directive discusses the process for adding, deleting and modifying firewall rules. It also addresses the issue of periodically reviewing the firewall rules which have been implemented.

Recommendation No. 6

NASS contracted with a private-sector firm, who along with OIG, recommended NASS implement advanced authentication measures for remote access. NASS has taken the first step in this process with the acquisition and implementation of modern firewall technology. NASS has obtained price quotes for a system which provides advanced authentication. NASS plans to implement a system providing advanced authentication for remote access following the implementation and testing of the new firewalls. The implementation of an advanced authentication system is expected to begin in July, 2002.

Recommendation No. 7

NASS included a training requirement, as well as assistance with configuration and implementation of the new firewalls, as part of the recent firewall acquisition. This training will ensure that the security staff is well versed in firewall management and the generation and modification of rules. The greatest benefit may be the fact that the staff responsible for managing the firewalls will be working directly with the vendor during the configuration and implementation. This opportunity to learn from the experts the 'hows and whys' of the firewall implementation in the NASS environment will be invaluable.

Recommendation No. 8

NASS attempts to disable separated user accounts in a timely manner. There are occasions when user accounts are left active, for example, managers may need to move files to a new employee now responsible for a recently separated employee's activities. Some of these accounts may also have remained on the system longer than necessary because we limited user account activity in November, 2001 in anticipation of this followup review by OIG. NASS distributes personnel summaries which provide information concerning employees that are recently hired, separated, and transferred. The security staff will be added to the distribution list for this summary. Additionally, the security staff will ask NASS's personnel office for a listing of all separated and transferred employees on a quarterly basis. This should ensure that NASS remains current in disabling accounts for those employees who no longer require access to the network.

Recommendation No. 9

The NASS security staff will ask the personnel office for a listing of current employees on a quarterly basis. This listing will be used to reconcile current employees with current network user accounts.

Recommendation No. 10

NASS agrees there is a degree of risk associated with allowing generic user accounts. NASS has disabled an additional 32 of these generic user accounts and deleted another 20. NASS is in the process of switching from generic user accounts to specific individual accounts for infrequent users. The first test of replacing generic accounts with individual user accounts will be for the March 'Hogs and Pigs Board' on March 25, 2002. NASS will continue the process of phasing out generic user accounts and replacing them with individual accounts over the next few months. NASS plans to be totally switched from generic user accounts to individual accounts by September 30, 2002.

Recommendation No. 11

NASS is attempting to comply with the requirements of OMB Circular A-130. NASS spent a great deal of time during FY2001 trying to get our security plan in compliance with OMB Circular A-130 and PDD-63. NASS satisfied the reporting requirements through the submission of an enhanced annual security plan and the request from the OCIO and OIG for OMB by completing the 'USDA Information Systems Assessment Guide'. NASS completed this analysis for a single system as required. The OCIO is currently scheduling visits with USDA Agencies to discuss each Agency's submission. NASS is waiting for this discussion to occur so we can make the submission for our remaining systems consistent with the Department's standards.

Recommendation No. 12

NASS is in the process of developing the Agency's FY2003 Annual Performance Plans as required under GPRA. NASS is defining a performance goal and associated measures to be included in this report.

# ABBREVIATIONS

| | |
|---|---|
| FMFIA | Federal Managers' Financial Integrity Act |
| GPRA | Government Performance and Results Act |
| ID | identification |
| IP | Internet Protocol |
| IT | Information Technology |
| NASS | National Agricultural Statistics Service |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PDD | Presidential Decision Directive |
| SSO | State Statistical Office |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| USDA | U.S. Department of Agriculture |
| VPN | Virtual Private Network |

USDA/OIG-A/26099-2-FM Page 26
USDA/OIG-A/26099-2-FM Page 26
USDA/OIG-A/26099-2-FM Page 26
USDA/OIG-A/26099-2-FM Page 26
USDA/OIG-A/26099-2-FM Page 26
USDA/OIG-A/26099-2-FM Page 26
USDA/OIG-A/26099-2-FM Page 26
USDA/OIG-A/26099-2-FM Page 26
USDA/OIG-A/26099-2-FM Page 26
USDA/OIG-A/26099-2-FM Page 26
USDA/OIG-A/26099-2-FM Page 26