U.S. Department of Agriculture

Office of Inspector General
Western Region

Audit Report

Grain Inspection, Packers And Stockyards Administration Management And Security Of Information Technology

Report No. 30099-1-SF
November 2003

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: NOV 7 2003

REPLY
ATTN OF: 30099-1-SF

SUBJECT: Management and Security of Information Technology,
Grain Inspection, Packers and Stockyards Administration

TO: Donna Reifschneider
Administrator
Grain Inspection, Packers and Stockyards Administration

ATTN: Carol Remmers
Manager
Information Systems and Security Program

This report presents the results of our review of the management and security of information technology at the Grain Inspection, Packers and Stockyards Administration. The agency's written response to the draft report is included as exhibit A with excerpts and the Office of Inspector General's position incorporated into the relevant sections of the report. Based on the written response, we have accepted your management decision for audit recommendations Nos. 1, 4 through 11, 13, 15, 16, 18 through 21, and 24. The Office of the Chief Financial Officer (OCFO) has responsibility for monitoring and tracking final action on the subject audit. Please follow your agency's internal procedures in forwarding final action correspondence to OCFO.

In order to reach management decision on the recommendations Nos. 2, 3, 12, 14, 17, 22, and 23, please provide us a written response with your estimated timeframes for completing corrective actions within 60 days. Departmental Regulation 1720-1 requires that all corrective action be completed within 12 months of report issuance.

We appreciate the assistance your staff provided to our auditors during the review.

Richard D. Long

RICHARD D. LONG
Assistant Inspector General
for Audit

Executive Summary

Grain Inspection, Packers and Stockyards Administration, Management And Security Of Information Technology (Audit Report No. 30099-1-SF)

Results in Brief

This report presents the results of our audit of management and security over information technology (IT) resources within the Grain Inspection, Packers and Stockyards Administration (GIPSA). Our overall objective was to assess GIPSA's information system security program. Specifically, we reviewed the adequacy of GIPSA's security over its systems and network, its logical and physical access controls, and its controls over the modification of application software programs.

GIPSA's information systems contain confidential and proprietary data obtained from private companies relating to transactions involving grains and livestock. GIPSA also monitors the shipments of these commodities within the United States and maintains a centralized repository of this data.

Our audit, which involved electronic vulnerability scans of GIPSA's systems, identified control weaknesses that, if not corrected, could expose GIPSA's network to internal and external intrusions. Our scans of GIPSA's network revealed 200 high and medium-risk vulnerabilities that could allow unauthorized access to that network. The likelihood that such access could occur and go undetected was increased by an inadequate system of firewalls and intrusion detection devices between GIPSA and the rest of the USDA network. GIPSA's logical and physical controls also needed strengthening to eliminate unsecured dial-in access and unrestricted entry to the computer room. For the convenience of its users, GIPSA had maintained the unsecured dial-in access. Due to a lack of guidance on how vulnerability scans were to be conducted, GIPSA's IT staff had conducted scans at a level too low to identify all vulnerabilities

We concluded GIPSA needs to improve its system security administration and ensure compliance with Federal requirements for managing and securing IT resources. Specifically, GIPSA administrators should have (1) conducted the necessary risk assessments of the GIPSA network; (2) properly certified the agency's mission-critical systems; (3) updated and approved GIPSA's security plans; (4) developed, implemented, and tested the IT contingency plan; and (5) ensured proper security clearances were obtained for IT staff. These actions were not done because of insufficient oversight by GIPSA's IT management.

Finally, our review disclosed that GIPSA's IT staff needed to improve its management over mission-critical applications. GIPSA's IT staff did not follow proper application change control procedures and did not build in logical controls in a major application. This occurred because GIPSA's CIO

had not established the needed controls. The lack of controls could leave the agency's mission-critical applications vulnerable to misuse and could directly affect key operations such as inspection, billing and trading information.

Recommendations in Brief

In the area of system vulnerabilities and access controls, we recommend GIPSA take immediate action on the high and medium vulnerabilities identified by the Office of Inspector General (OIG) scans and run all future vulnerability scans at the appropriate levels. Also, GIPSA should immediately remove the unsecured method of dial-in access; develop secure procedures for remote dial-in access and the handling and reporting of security incidents; and establish an intrusion detection system between the GIPSA network and the USDA Backbone.

In the area of system security administration, we recommend GIPSA establish risk assessment procedures and perform risk assessments of its mission-critical systems. GIPSA should establish and implement procedures requiring security plans to be reviewed, tested, and updated on an annual basis. GIPSA should develop a comprehensive contingency plan and ensure the contingency plan is tested and updated at least on an annual basis. Also, GIPSA should obtain security clearances for 12 IT employees. In addition, GIPSA needs to strengthen its physical access control to its computer room.

In the area of application life cycle controls, we recommend GIPSA develop proper application change control procedures. GIPSA should also ensure application changes are authorized and approved by management and it should implement logical access controls at grain export elevator workstations.

Agency Response

In its written response to the audit report, GIPSA concurs with all the audit findings and accepts 23 of the 24 recommendations. For recommendation number 7, GIPSA believes the iron bars on the server room windows are unnecessary because the server room is three stories up and faces the inside of a courtyard. An armed guard protects the courtyard when open and secured with an iron gate when the area is closed. The complete written response is shown in Exhibit A of the audit report.

OIG Position

Based on GIPSA's written response, OIG accepts GIPSA's management decision for 17 of the 24 audit recommendations.

Abbreviations Used in This Report

APHIS	Animal and Plant Health Inspection Service
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
GAO	General Accounting Office
DAA	Designated Approval Authority
DM	Departmental Manual
DR	Departmental Regulation
FGIS	Federal Grain Inspection Service
GIPSA	Grain Inspection, Packers and Stockyards Administration
ISSPM	Information System Security Program Manager
IT	Information Technology
JFMIP	Joint Financial Management Improvement Program
LAN	Local Area Network
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
P&S	Packers and Stockyards
TCP/IP	Transmission Control Protocol / Internet Protocol
VPN	Virtual Private Network
USDA	U. S. Department of Agriculture

Table of Contents

Background and Objectives

Background

The mission of the Grain Inspection, Packers and Stockyards Administration (GIPSA) is to administer uniform, national grain inspection and weighing programs and promote the integrity of livestock, meat, and poultry markets to ensure a productive and competitive global marketplace for U.S. agriculture products. This includes establishing and maintaining official U.S. grain standards and promoting the uniform procedures for official inspections; and fostering fair and open competition to guard against deceptive and fraudulent practices that affect the demand and price of meat and their products.

In September 1998, the General Accounting Office released a report to the Committee on Government Affairs, U.S. Senate, entitled, "Serious Weaknesses Place Critical Federal Operations and Assets at Risk." The report states widespread and serious weaknesses in the Federal Government's ability to adequately protect Federal assets from fraud and misuse, sensitive information from inappropriate disclosure, and critical operations from disruption. The report notes that individual agencies have not yet done enough to effectively address these problems, including instituting procedures for ensuring that risks are fully understood and implementing controls to mitigate these risks.

Presidential Decision Directive 63, Policy on Critical Infrastructure Protection, issued May 22, 1998, states that critical infrastructures are those systems essential to the minimum operation of the economy and Government and includes telecommunications, banking and finance, energy, transportation, and other essential government services. The Directive states that the Government will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, with particular emphasis on information technology (IT) systems.

Information security, improving the overall management of IT resources, and the transition to electronic business (e-Government), has emerged as a top priority within the U.S. Department of Agriculture (USDA). Prior Office of Inspector General (OIG) reviews have identified noncompliance with federally mandated laws, regulations, and guidance relating to the management and security of information technology resources. As technology has enhanced the ability to share information instantaneously among computers and networks, it has also made organizations more vulnerable to unlawful and destructive penetration and disruptions. Threats range from those posed by insiders, and recreational and institutional hackers to attacks by intelligence organizations of other countries.

The kinds of cyber-assets that USDA must protect include:

- Billions of dollars in Federal payroll, thrift savings, and other accounts at the National Finance Center for USDA, and other Federal agencies;
- Market-sensitive data on commodities and the agricultural economy;
- Personal information for both employees and customers, including social security numbers, health, business and financial data;
- Sign-up and participation information, and other information critical to the delivery of USDA's programs;
- Geological Information Systems, ecological, environmental, soil and other scientific data; and
- Research data.

Protecting these critical assets must be a top priority for USDA's program managers as well as information technology staffs, especially as the Department makes more programs and information available over the Internet. The Internet was designed to be an open system with no regard for security. While new security standards are continually being developed, safeguards such as encryption, data backup procedures and controls, network intrusion detection systems, disaster recovery and contingency planning can be employed to afford some degree of security. However, the Department will only be as secure as its weakest link.

The USDA OIG, Financial and Information Technology Operations (FITO), conducted nationwide audits of selected USDA agencies to assess the overall management and security of major USDA computer systems. GIPSA was one of several agencies selected for review as part of the nationwide audit of USDA mission-critical systems. A nationwide audit report will be issued to the OCIO by FITO.

GIPSA has identified 10 mission-critical systems. The GIPSA computer systems are operated to provide general computing resources including data communications, software, and hardware for approximately 800 GIPSA employees nationwide.

Objectives

Our audit objectives were to (1) assess the overall management of GIPSA's Information System Security Program, (2) determine the adequacy of the security over the local and wide area networks, and identify vulnerabilities in Departmental payment/data systems, (3) determine if adequate logical and physical access controls exist to protect computer resources against unauthorized modification, disclosure, loss, or impairment, (4) evaluate the controls over the modification of application software programs to ensure that only authorized modifications are implemented, and (5) determine the adequacy of controls over access to and modification of system software and data transmission.

Findings and Recommendations

Section 1. System Vulnerabilities

Our audit identified control weaknesses, which, if not corrected, could expose GIPSA's network to internal and external attacks. First, our assessment of GIPSA's network revealed 200 high and medium-risk vulnerabilities, which could allow unauthorized access to GIPSA's network. GIPSA IT staff had conducted vulnerability scans but ran their scans at a level that did not allow them to identify all vulnerabilities. Second, we found security weaknesses in GIPSA's logical and physical access controls. Finally, we noted that GIPSA's network was not adequately protected by a system of firewalls and intrusion detection devices. Unless these conditions are corrected, GIPSA's network is not only vulnerable to internal and external attacks, but the agency will be unable to detect such violations when they occur.

Finding 1 — GIPSA Vulnerability Scans Did Not Detect Vulnerabilities Within Its Own Network

GIPSA did not properly conduct vulnerability scans that would allow it to identify vulnerabilities within its network. This occurred because there were inadequate procedures or guidelines from the Office of Chief Information Officer (OCIO) on how the vulnerability scans were to be conducted. Therefore, GIPSA personnel did not use all the functionality of the scanning software tool and ran their scans at levels that did not allow them to identify all vulnerabilities. As a result, GIPSA officials were not aware that their systems and networks were vulnerable to cyber-related attacks that could jeopardize the integrity and confidentiality of GIPSA's mission-critical systems.

OMB A-130, Appendix III[1] 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. In addition, USDA Departmental Regulation 3140[2] establishes policies to ensure comprehensive security programs are in place to safeguard all information technology resources. USDA managers must ensure security is in place to protect against accidental or deliberate alteration, destruction, delay, theft, or access to systems, data, applications, equipment and telecommunications.

We conducted an assessment of GIPSA's networks during the week of

[1] OMB A-130, Appendix III, Section B, dated November 30, 2000
[2] USDA Departmental Regulation 3140, dated May 15, 1996

December 2, 2002. We used two commercially available software products – one designed to identify security vulnerabilities associated with various operating systems that use Transmission Control Protocol/Internet Protocol (TCP/IP), and the other designed to test system policy setting in the networks. The software products perform tests on an agency's computer systems, identify vulnerabilities, and prioritize them into high, medium and low risks. The software also generates a report that suggests corrective actions.

TCP/IP System Vulnerabilities

GIPSA's computer system consists of numerous computers and routers connected together into the agency's network. The Department's CIO maintains the backbone telecommunication lines, router, and equipment to run the Departments "backbone network". Agencies such as GIPSA obtain their connection to National Information Technology Center, National Finance Center, and the Internet by connecting to this backbone.

We conducted our tests of the TCP/IP systems in coordination with GIPSA's IT staff. Our tests of 66 network operating systems identified 21 high-risk vulnerabilities, 179 medium-risk vulnerabilities, and 523 low-risk vulnerabilities. High-risk vulnerabilities are those that could allow access to the computer and possibly to the network of computers. Medium-risk vulnerabilities are those that could allow access to sensitive network data that may lead to exploitation of other vulnerabilities. Low-risk vulnerabilities are those that allow access to data that might be sensitive, but are less likely to lead to higher-risk vulnerability.

We provided our test results to the CIO describing the vulnerabilities detected and the severity of each vulnerability on them. Because of the security issues involved, details of the vulnerabilities are not provided in this report.

Although GIPSA acquired similar scanning tools, GIPSA's IT staff was not scanning at levels that would detect all known vulnerabilities. According to GIPSA's IT staff, they were advised during a training course on using the scanning software that performing vulnerability scans at level 3 would be sufficient to catch all known vulnerabilities. There were no Departmental procedures or guidelines on how the vulnerability scans should be conducted. The scanning software has five levels, 1 through 5, and the higher the level, the more in-depth the scan. Level 1, the lowest setting, only identifies operating systems running on the network with no check for weaknesses; on the other hand, level 5 would check for compromises by highly skilled attackers and identify weaknesses in a system's configuration. GIPSA's staff only performed their vulnerability scans at levels 1 through 3 while OIG's vulnerability scans were performed at levels 4 and 5. As a result, GIPSA's scanning results did not identify the high-risk and medium-risk vulnerabilities

disclosed by OIG's scans.

OCIO procedures[3] state that scans are supposed to be performed on a monthly basis for all networks, systems, and servers by duly authorized users**.** However, we found GIPSA's vulnerability scans were not performed on a monthly basis. According to Information System Security Program Manager (ISSPM), the vulnerability scans were not conducted on a monthly basis due to a lack of staff with the knowledge to operate the scanning software tool.

Network Operating System Vulnerabilities

We also conducted a detailed assessment of the security over GIPSA's network operating systems. Our assessment software provided comprehensive scans covering logical access controls; such as, user account characteristics, password controls, and many other security features. Our review of the scanning results disclosed the following weaknesses in account restrictions and access control, the areas that define a user's ability to access the system:

- Five users had nonexpiring passwords. These users were not forced to change their password at normal intervals like the rest of the users on the network and there were no justification for this privilege.

- Seven users had privileges on their user profile to dial-in to the GIPSA network, which were unnecessary. GIPSA users do not need these privileges on their user profile active in order to dial-in to the GIPSA network.

We discussed the findings on TCP/IP System Vulnerabilities and Network Operating System Vulnerabilities with GIPSA's IT staff. The GIPSA IT staff promptly took corrective measures on the high-risk vulnerabilities identified and provided us with the documented support. At the time of our review, GIPSA's staff was still resolving the medium-risk vulnerabilities. We did not follow up on the low-risk vulnerabilities because they did not relate to a direct threat to the computer system. GIPSA staff also took immediate action on the non-expiring passwords and dial-in privileges on users accounts. The issue relating to the lack of Departmental guidance on scanning will be covered in the nationwide audit report to the OCIO by FITO.

Recommendation No. 1

Take immediate action to correct the all medium vulnerabilities identified by OIG's vulnerability scans and conduct a rescan to ensure that the vulnerabilities identified by OIG have actually been corrected.

[3] CS-07, Security Vulnerability Scan Procedures, dated September 5, 2001

Agency Response.

GIPSA accepts the recommendation. GIPSA's Network and Telecommunications Branch took immediate action and corrected all high and medium vulnerabilities identified. A rescan was conducted to insure the vulnerabilities identified were corrected.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO of the rescan showing that all high and medium vulnerabilities were corrected.

Recommendation No. 2

Run all future vulnerability scans of the GIPSA network at a maximum level to detect vulnerabilities and perform scans on a monthly basis.

Agency Response.

GIPSA accepts the recommendation. GIPSA's ISSPM will insure all future scans are run at the maximum level to detect vulnerabilities and that scans are run on a monthly basis.

OIG Position.

In order to reach management decision please provide the timeframes when procedures will be in place to run all future monthly scans at the maximum level.

Recommendation No. 3

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

Agency Response.

GIPSA accepts the recommendation. GIPSA's ISSPM will monitor low-level vulnerabilities to identify trends and advise network personnel on those areas that could lead to more serious vulnerabilities.

OIG Position.

In order to reach management decision please provide the timeframes when GIPSA's ISSPM will be monitoring low-level vulnerabilities to identify trends and advise network personnel on those areas that could lead to more serious vulnerabilities.

Finding 2 Access Controls Need to be Strengthened

Our review disclosed serious vulnerabilities over access to GIPSA's network. Specifically, we found that GIPSA's management has allowed some of its users to access its network via an unsecured method of dialing in. We also observed that physical access controls to GIPSA's new computer room need to be improved. GIPSA's IT staff was aware of the vulnerabilities posed by the unsecured dial-in access and had drafted procedures requiring its removal. GIPSA's Deputy Administrator, however, did not approve the procedures and wanted to keep the unsecured method of access available for the convenience of its staff. GIPSA's CIO was also unaware of the physical security weaknesses we observed in the new computer room. These deficiencies leave GIPSA's network vulnerable to unauthorized access, potentially jeopardizing the integrity of GIPSA's mission-critical systems.

Logical Access Controls

Logical access controls protect network applications and data against theft or unauthorized modification. Logical access controls such as user names, passwords, and access permissions, ensure that only authorized users have access to network resources from their workstations, and that users are granted only the access that is needed to conduct their job responsibilities. Without strong logical access controls, privacy and financial data is subject to loss and unauthorized modification[4].

GIPSA's logical access controls were weakened by an unsecured dial-in access that allowed access to the network without proper security and/or firewall protection. GIPSA's IT staff was aware of the vulnerabilities posed by the unsecured dial-in access and developed a draft policy requiring all users to use only one secure method of remote dial-in. However, management wanted to keep the unsecured dial-in access in place because certain users, accustomed to the unsecured access, complained about the connection speed and cumbersome authentication process of the secure dial-in access method. As a result, USDA and GIPSA's networks are vulnerable because the unsecured dial-in access provides an unprotected backdoor gateway to GIPSA's network.

[4] NIST SP800-12, Introduction to Computer Security; March 16, 1995

OMB[5] defines adequate security as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. For each system, an individual should be the focal point for assuring there is adequate security within the system, including ways to prevent, detect, and recover from security problems."

Also, Departmental Regulations[6] state, "USDA agencies which access the Internet must develop and implement an Internet security policy which meets the minimum requirements…. The most practical method of securing access to systems from the Internet is to use a secure Gateway or a firewall system."

There are two methods of remote dial-up access to the GIPSA network. We determined that one method was secured by the Department's firewall protection, Virtual Private Network (VPN) software, and a Public Access Network[7] that required three levels of authentication before allowing access to the GIPSA network. In contrast, the second method of access, via unsecured dial-in, was unprotected and did not have a firewall or an authentication process. A user could gain access to the GIPSA network without going through proper security checks. This could result in an unsecured backdoor entrance into the USDA Backbone and GIPSA networks. If a hacker discovered this unsecured dial-in access, the hacker could gain unlimited access to the networks.

We concluded the draft remote dial-in procedures should be implemented immediately to ensure all users connect to the network only using a secure remote dial-in access with proper security and/or firewall protection. Adequate security must be a top priority in assuring the integrity of the Department and GIPSA's critical systems. Proper security checks and controls should take precedence over individual preference and convenience.

Physical Access Controls

The physical access controls to GIPSA's new computer room need to be strengthened to minimize the risk of unauthorized access. We determined the glass window on the door of the computer room and windows facing the outside inner courtyard of the building could be broken and entry could be forced. According to GIPSA, no modification can be made until the agency has completely moved into the new office site and building management has given proper approval. Anyone who gains access to the USDA agriculture-building complex could easily break these windows and enter. As a result, the computer servers and related equipment were subject to the risk of theft, damage, or other disruptions.

[5] OMB A-130, Appendix III, dated November 30, 2000
[6] DR 3140-2, "USDA Internet Security Policy", dated March 7, 1995
[7] Public Access Network is neutral zone between the Department's Backbone and Agency access where the web servers reside.

According to regulations,[8] an agency's physical access controls are to restrict the entry and exit of personnel from the area, such as the office building, suite, data center, or room containing a local area network (LAN) server. In addition, management controls must provide reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation.

GIPSA currently has two computer rooms, one for the Federal Grain Inspection Service (FGIS) and the other for the Packers and Stockyards (P&S) Administration. GIPSA stated it is in the process of moving its offices to a new location in the Agriculture building. One computer room will be used to house the network system for both the FGIS and the P&S Administration. This computer room has windows with no protective bars to prevent access from the outside courtyard, and a door with a glass window that provides little protection within.

According to GIPSA, no modifications to the computer room can be made until the agency had moved into the new location and proper approval has been given. The Network Branch Chief stated the Agricultural building is a historic building, any modifications, such as installing protective bars on the windows should be made in consultation with building management.

Recommendation No. 4

Immediately remove the unsecured method of dial-in access from the GIPSA network.

Agency Response.

GIPSA accepts the recommendation. GIPSA has adopted OIG's suggestion of removing the unsecured dial-in access to the GIPSA network. GIPSA will use the more secure VPN method.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO that GIPSA is now using the more secure VPN method.

Recommendation No. 5

Implement remote dial-in procedure to ensure that only the secure method of network access is used.

[8] OMB A-123, dated June 21, 1995; and NIST SP 800-18 (5.MA.2.1), dated December 1998

Agency Response.

GIPSA accepts the recommendation. GIPSA now only allows VPN, a secure method of access to its network.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO that the procedures had been implemented.

Recommendation No. 6

Replace the glass window on the new computer room door with a wooden panel.

Agency Response.

GIPSA accepts the recommendation. GIPSA has placed a wooden panel on the inside of its server room door. This keeps the historic look of the building from the hallway view but precludes entry into the room by breaking a glass window.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO that a wooden panel has been placed on the inside of its server room door.

Recommendation No. 7

Add protective bars to the inside or outside of GIPSA's computer room windows to mitigate any potential unauthorized entry.

Agency Response.

GIPSA rejects the recommendation. Bars on the outside windows are not necessary because the server room is three stories up and faces the inside of a courtyard. The courtyard is protected by an armed guard when open and secured with an iron gate when the area is closed.

OIG Position.

OIG accepts GIPSA's management decision. GIPSA is now aware of and is accepting the risk of not adding protective bars to its computer room windows. No further action needs to be taken.

Finding 3 — Intrusion Detection Controls Were Inadequate

GIPSA did not have an internal firewall with an intrusion detection system to detect network security violations. GIPSA also did not have its own procedures for responding to and reporting security incidents. GIPSA managers said they relied on the Department's intrusion detection system to protect their network and used the Department's incident response procedures manual as their own policy. As a result, there was no assurance that external and internal intrusions to the network would be detected and prevented and security incidents would be properly addressed and reported to the Office of Chief Information Officer (OCIO). At the time of our review there had been no known penetrations into the GIPSA computer system.

OMB A-130[9] states that, "an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident…. Agencies should establish formal incident response mechanisms…. To be fully effective, incident handling must also include sharing information concerning common vulnerabilities and threat with those in other systems and other agencies." According to guidance provided by the National Institute of Standards and Technology (NIST),[10] "attention to external threats to the exclusion of internal threats leaves the network open to attack from the inside…important systems such as internal web and email servers or financial systems should be placed behind internal firewalls."

The OCIO at Ft. Collins, Colorado, monitors data traffic over the USDA Intranet backbone to identify any alleged intrusions against the Department's IT systems. This information is forwarded to the Department's IT security officer who in turn notifies the appropriate agency ISSPM that an intrusion was attempted against their systems. The agency's ISSPM then notifies the local security officer where the incident occurred.[11] It is the agency's responsibility to address and mitigate the security incident and complete a security incident report for the OCIO.

[ ]
[ ]
[ ]
[ ]
[ ]
[ ]

[9] OMB A-130, Appendix III, dated November 30, 2000
[10] NIST SP 800-41, Guidelines on Firewall and Firewall Policy, dated January 2002
[11] OIG Audit Report No. 10099-1-TE, Security Over NRCS IT Resources, dated January 2002

[ ]
[ ]
[ ]
[ ]

[ ]
[ ]
[ ]
[ ]
[ ]
[ ]

[ ]
[ ]
[ ]
[ ]
[ ]

Recommendation No. 8

[ ]
[ ]

Agency Response.

GIPSA accepts the recommendation. GIPSA [ ]
[ ]
[ ]

OIG Position.

OIG accepts GIPSA's management decision. [ ]
[ ]
[ ]

Recommendation No. 9

Establish internal procedures for handling and reporting security incidents to ensure quick mitigation and proper processing of security violations.

Agency Response.

GIPSA accepts the recommendation. GIPSA has established internal incident handling procedures. All incidents are immediately reported to the ISSPM or GIPSA Help Desk. The ISSPM or GIPSA Help Desk contacts the appropriate personnel to assist in responding to the incident. Together, the incident is worked to mitigate security breaches and violations. An incident report is filed and kept open until the incident is resolved.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO that GIPSA has established internal incident handling and reporting procedures.

Finding 4 Chief Information Officer had Administrative Privilege

Our scans identified that the Chief Information Officer (CIO) had full administrative privileges over the network operating system. The CIO informed us that he needed this access to fulfill his oversight responsibilities over his staff and contractors. However, this level of access gave the CIO complete control to configure and modify any system on the network, a far greater control than was required for mere oversight responsibilities. As a result, there was no clear separation of duties between the day-to-day network maintenance and oversight function.

NIST 800-14[12] states that once a position is defined two general security rules should be assigned to a user's access privilege—separation of duties and least privilege. Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties.

We determined that the CIO should not have full administrative privileges because there is no adequate separation of duties between the administration and oversight function. Applying the least privilege concept, we determined that the CIO should have only that access needed to fulfill his oversight responsibilities. This may require read-only access to system log files, but should not include the ability to fully administer the systems on the network.

The CIO was responsible for overseeing his staff, but unlike the network administrators, the CIO did not need to administer the network on a daily

[12] NIST 800-14, Principles and Practices for Securing IT Systems, dated September 1996

basis. If the CIO needs the ability to monitor his staff, then the read-only option would give him the ability to check on his staff, but not the ability to make any major changes to the network without a secondary review. Such ability could be detrimental to system operations.

Adequate internal controls mandating separation of duties would require that the CIO's access be modified to provide only the access level needed to fulfill his oversight responsibilities.

Recommendation No. 10

Remove the CIO's administrative privilege and establish only the access levels needed to fulfill his oversight responsibilities.

Agency Response.

GIPSA accepts the recommendation. Full system administrative privileges have been removed from the CIO.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO that the CIO no longer has full system administrative privileges.

Section 2. Security Program Management of Information Technology Resources

We concluded GIPSA needs to improve its management of Information Technology (IT) resources, and ensure compliance with Federal requirements for managing and securing IT resources. Specifically, we found GIPSA had not (1) conducted the necessary risk assessments of its network, (2) properly certified its mission-critical systems, (3) updated and approved its security plans, (4) developed and implemented an adequate contingency plan, and (5) obtained proper security clearances for its employees. Also, GIPSA did not establish procedures to ensure the security controls were properly tested for applicability and effectiveness. This resulted from insufficient oversight by past and current IT management.

Finding 5 No Risk Assessments Were Performed

GIPSA did not perform risk assessments, required by OMB A-130, of its 10 mission-critical systems. GIPSA's CIO could not provide us the reason why a risk assessment had not been done in the past but he stated that GIPSA planned to do a risk assessment during the current fiscal year. However, GIPSA had not yet completed any at the time of our audit. As a result, there was limited assurance GIPSA was aware of potential vulnerabilities or threats to its systems, of the value of its information if lost, and of the effectiveness of its countermeasures to eliminate or reduce the threats to its mission-critical system.

Office of Management and Budget (OMB) A-130[13] states, "the need to determine adequate security will require that a risk-based approach be used. This risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards." According to the NIST's Risk Management Guide for IT Systems[14], "risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. In addition, the risk assessment is usually repeated at least every 3 years."

GIPSA did not perform risk assessments of its mission-critical systems. However, GIPSA stated a risk assessment is one of the items to be completed by the Information Systems Security Program Manager, and the risk assessment was included in the agency's Plan of Action and Milestone to be performed in FY 2003. However, at the time of our review, GIPSA still had not conducted the risk assessment and had no plans to conduct risk

[13] OMB A-130, Appendix III, dated November 30, 2000
[14] NIST SP 800-30, dated October 2001

assessments on a routine basis.

GIPSA's managers were not aware of the importance of performing a comprehensive risk assessment. They stated that they had conducted scans to determine potential vulnerabilities to their system. However our review noted that not only were the scans that they conducted not adequate (see Finding No. 1) but the scanning alone did not constitute a comprehensive risk assessment review. For example, the scans did not identify all potential threats and vulnerabilities to the system, nor did it measure the effectiveness of current or proposed safeguards to mitigate or eliminate the potential threats or vulnerabilities, areas that are covered under a comprehensive risk assessment. Without a comprehensive risk assessment, GIPSA's management did not have the complete information needed to protect its mission-critical system.

Recommendation No. 11

Perform risk assessments of its general support systems and mission-critical systems.

Agency Response.

GIPSA accepts the recommendation. GIPSA, with the assistance of a contractor, anticipates completing the risk assessment of its General Support System (WAN) by the end of the second quarter of fiscal year 2004. This is the only risk assessment remaining. GIPSA had completed a program risk assessment in June 2003.

OIG Position.

OIG accepts GIPSA's management decision based on the completion of all risk assessments by March 30, 2004 (end of the second quarter of fiscal year 2004). For final action, please provide documentation to OCFO that the risk assessments as recommended has been completed.

Recommendation No. 12

Establish a policy requiring that risk assessments be performed at least every 3 years.

Agency Response.

GIPSA accepts the recommendation. GIPSA will follow Departmental policy requiring risk assessments be completed at least every three years.

OIG Position.

In order to reach management decision please provide timeframes when GIPSA will establish a policy requiring risk assessments be completed at least every three years.

Finding 6 Mission-Critical Systems Were Not Certified

GIPSA had not certified and authorized 10 mission-critical systems. According to GIPSA's CIO, the program sections failed to establish certification-testing teams for certifying the mission-critical systems and applications and there was no followup by management. As a result, there was no assurance that GIPSA had properly established adequate security controls to protect these 10 systems.

OMB A-130[15] requires that a management official authorize in writing the use of each general support system based on implementation of its security plan. Management authorization is based on the managerial, operational, and technical controls being in place to ensure that the system can be operated securely. The technical evaluations are the basis for a management accreditation, or "authorization to process."

GIPSA has 10 mission-critical systems, none of which were formally tested and certified. According to GIPSA's security plan, each major application and general support system is to undergo appropriate technical certification evaluations to ensure that all installed security safeguards are adequate. The certification of the system is based on the documented results of a system security control tests and the recommendations of the certification team/individual. Certification tests are technical evaluations that indicate how well a design/implementation meets a specified set of automated information system security requirements.

According to the CIO, each program section was asked to establish a certification testing team, called the Designated Approval Authority (DAA). It was the responsibility of each program section to establish its own DAA to conduct system certification testing. However, the program sections failed to establish DAAs and there was no follow up or oversight by management to ensure that certification-testing teams were established. GIPSA needs to also make sure that IT staff is included in the system testing.

Recommendation No. 13

Establish certification-testing teams (DAA), which should include members

[15] OMB A-130, Appendix III, dated November 30, 2000

of the IT staff, for system testing.

Agency Response.

GIPSA accepts the recommendation. GIPSA will be forming teams to include members of the IT Staff as well as DAA's in September 2003 to begin the certification and accreditation process. GIPSA's ISSPM will establish certification-testing teams in October 2003.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO that GIPSA's ISSPM has established certification-testing teams to include members of IT staff.

Recommendation No. 14

Ensure that all current and future mission-critical systems are properly tested, certified, and authorized.

Agency Response.

GIPSA accepts the recommendation. All current and future systems will be properly tested, certified, and authorized.

OIG Position.

In order to reach management decision please provide timeframes when procedures will be in place to properly test, certify and authorize all current and future systems.

Finding 7 Security Plans Were Not Properly Updated and Approved

GIPSA did not have documentation to support that security plans were properly updated and approved. In addition, GIPSA did not have policies or procedures in place requiring the production, update, and periodic review of security plans. GIPSA had not established a formal certification and approval process for security plans. As a result, there was no assurance the security plans were being properly updated, certified, and approved or whether the existing plans were proper.

OMB A-130[16] requires agencies to prepare a security plan to provide an

[16] OMB A-130, Appendix III, dated November 30, 2000

overview of the security requirements of their systems. According to NIST,[17] by authorizing a system, a manager accepts the risk associated with it. In the security plan, the manager should include the date of authorization, name, title, and title of the management official who approved the plan. Also, USDA Departmental Manual 3140[18] requires each agency to submit an automated data processing security plan and an annual update to an existing plan to the OCIO. In addition, NIST[19] states there should be a policy that requires the production, update, and review of system security plans on a periodic basis or when major applications or general support systems are implemented or significantly changed.

GIPSA has one overall general security plan for its network and 10 system-specific security plans, one for each mission-critical system. Our review indicated that none of the security plans were properly updated and approved by management. According to the Acting Information System Security Program Manager, the security plans are "living documents," meaning that updates and changes are made continuously. However, there was no documentation that indicated when the changes were made or who approved them. We informed management of the requirement to document any updates and changes to the security plans. Specifically, the management official who approves the security plans should document his/her name, title, and the date on the approved plan. The CIO stated he was not aware the security plans needed formal written certification and approval whenever updates and changes were made.

We noted two of the system-specific security plans were not updated to reflect the current system owner and security officer for those mission-critical systems. According to Information System Security Program Manager (ISSPM), for 2002 only, the OCIO waived the requirement for agencies to submit their annual security plans. Although, GIPSA was not required to submit their security plans to the OCIO in 2002; GIPSA was still required to review, update, and document any changes to their security plans. According to regulations,[20] agencies are required to have a policy that requires the production, update, and review of system security plans on a periodic basis or when a major applications or general support system is implemented or significantly changed.

Our review disclosed GIPSA did not have a policy that required updates and review of system security plans on a periodic basis. The security plans are revised and updated on an as-needed basis. In addition, GIPSA did not have any evidence to indicate security plans were being reviewed periodically, at a minimum on an annual basis. As a result, there was no assurance the security

[17] NIST SP 800-18, Guide for Developing Security Plans for IT Systems, dated December 1998
[18] USDA Departmental Regulation 3140-1, dated March 15, 1996
[19] NIST SP 800-18, Guide for Developing Security Plans for IT Systems, dated December 1998
[20] OMB A-130, Appendix III, dated November 30, 2000 and NIST SP 800-18, dated December 1998

plans were current or effective.

Recommendation No. 15

Develop and implement procedures requiring that the security plan be updated, certified, and reviewed on an annual basis.

Agency Response.

GIPSA accepts the recommendation. GIPSA's ISSPM has given each DAA and application programmer a copy of OCIO's CS-025 to assist them in understanding the importance of up-to-date security plans. GIPSA has established policy that directs annual security plans to be reviewed and completed.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO that procedures are in place to update, certify and review the annual security plan.

Recommendation No. 16

Establish a formal approval process for security plans that documents the name, date, and title of the approving management official.

Agency Response.

GIPSA accepts the recommendation. GIPSA has established a formal approval process for security plans that documents the name, date, and title of the approving management official. The approving management officials include the ISSPM, CIO, Deputy Administrators, and Administrators. The plans are then sent to the Chief of Cyber Security, OCIO.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO that GIPSA has established a formal approval process for security plans that documents the name, date, and title of the approving management officials.

Finding 8 GIPSA Did Not Have an IT Contingency Plan

GIPSA did not have a contingency plan to ensure that it could recover its IT operations in event of a disaster or major disruption in service. GIPSA's CIO did not think a separate IT contingency plan was needed, since GIPSA used the Department's Continuity of Operations Plan (COOP). However, an IT contingency plan is a separate document from the Department's COOP since it provides for a detailed plan for restoring and recovering critical components of GIPSA's mission-critical systems. Without an adequate IT contingency plan, GIPSA cannot be assured that its network and operations can recover quickly and effectively to accomplish its mission in the event of an emergency.

OMB A-130[21] requires agencies to 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. NIST[22] states general support systems require emergency, backup, and contingency plans. Furthermore, OMB A-130 states that contingency plans should be tested insofar as untested or outdated contingency plans create the false sense of the ability to recover in a timely manner.

GIPSA used the Department's COOP, which was the boilerplate emergency plan approved and used by the Department. The Department's COOP plan contained information on the GIPSA relocation site, the telephone contact number for key GIPSA personnel, and the delegation of authority to the deputy administrators and directors. However, it did not show the assignment of responsibilities for recovery or give detail instructions for restoring operations, and it did not identify the critical computers, equipment, software, and telecommunications hardware needed in GIPSA or the data files critical to GIPSA operations.

GIPSA's COOP plan also did not show the current condition of system security, and it did not include procedures to follow when the data/service center was unable to receive or transmit data. In addition, the plan had not been tested and was not approved by key GIPSA groups, including senior management, data center management, and program managers. Therefore, there was no assurance that the COOP plan would be effective in the event of an emergency. If GIPSA's mission-critical systems were inoperative, there would be severe disruptions to GIPSA's program operations.

[21] OMB A-130, Appendix III, dated November 30, 2000
[22] NIST SP 800-18, Guide for Developing Security Plans for IT Systems, dated December 1998

Recommendation No. 17

Establish procedures to implement a contingency plan, which complies with NIST and OCIO requirements.

Agency Response.

GIPSA accepts the recommendation. GIPSA's ISSPM, along with the DAA's, and application developers are working on completing the plans. The estimated time for completion is December 2003.

OIG Position.

In order to reach management decision please provide the timeframes when procedures are established to implement a contingency plan.

Finding 9 Required Security Clearances For IT Staff Were Not Obtained

GIPSA had not obtained security clearances for the 12 employees with access to sensitive data in its IT staff. Of the 12 employees identified, GIPSA had initiated security clearances for 7. GIPSA's CIO was not aware of the Federal requirements for obtaining security clearances for employees in positions classified as "public trust positions." As a result, GIPSA has allowed employees to access critical systems and sensitive agency data when those employees maybe unsuitable for such a position of trust.

Federal regulations[23] state that to establish a person's suitability for employment, appointments to positions in the competitive service require the person to undergo an investigation by Office of Personal Management (OPM) or by an agency with delegated authority from OPM to conduct investigations. Positions at the high or moderate risk levels would normally be designated as "public trust" positions. Such positions may involve policy making, major program responsibility...fiduciary responsibilities, and other duties involving access to sensitive operation or data.[24]

Officials from GIPSA, Animal and Plant Health Inspection Service (APHIS), and Agriculture Marketing Service all met to determine if security clearances were needed for employees in public trust positions. GIPSA worked with APHIS since GIPSA relied on APHIS for all its personnel functions. Under a Memorandum of Understanding (MOU) between APHIS and GIPSA, APHIS would process the paperwork for all new hires, which would include determining if an employee needed a background investigation. OPM would

[23] 5 CFR 731.104 and 106, dated January 1, 2002
[24] NIST 800-12, An Introduction to Computer Security, March 16, 1995

conduct the actual background investigations for all security clearance applicants.

GIPSA's CIO stated APHIS was supposed to initiate background investigation and security clearances for the agencies. However, APHIS advised GIPSA that they would not continue their joint effort because of other priorities in Homeland Security. GIPSA was forced to take the initiative in obtaining proper security clearances for those employees deemed priorities.

GIPSA has approximately 34 employees in its IT staff. We identified 12 employees on the IT staff who have access to sensitive data and need security clearances. These include the CIO, Information Systems Security Program Manager, system security officers, network administrators, and programmers. We determined these positions were defined by regulations as "public trust" positions. GIPSA had initiated security clearances for 7 of the 12 employees in July 2002 but had not yet received clearances from OPM at that time of our review. GIPSA did not initiate security clearances for the remaining five employees due to an oversight by management.

Recommendation No. 18

Initiate security clearances for five employees that have not submitted security clearance applications to OPM.

Agency Response.

GIPSA accepts the recommendation. Security clearances will be submitted for all IT personnel by the end of 2003.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO that OPM has received security clearance applications for all of it's IT personnel.

Recommendation No. 19

Formally request OPM to expedite the security clearances for employees in "public trust positions."

Agency Response.

GIPSA accepts the recommendation. GIPSA will formally request that OPM expedite the security clearances for employees in IT positions by the end of September 2003.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO that GIPSA has formally requested OPM to expedite the security clearances for employees in IT positions.

Our review disclosed that GIPSA's IT staff needed to improve its controls over mission-critical applications. GIPSA's IT staff did not follow proper application change control procedures, did not build in logical controls in a major application, and did not properly link applications to prevent redundant manual entries and to eliminate data entry errors. This occurred because GIPSA's CIO had not established the needed controls. The lack of controls could leave the agency's mission-critical applications vulnerable to misuse and could directly affect key operations such as inspection, billing and trading information.

Finding 10 Proper Application Change Controls Were Not Established

Application changes were made in a manner not consistent with Departmental requirements and OMB guidelines. GIPSA did not have written and standardized change control procedures in place for making and testing application changes. These procedures should have provided for the process of documenting all changes made to an application and a separation of duties between programming and placing the application changes into production during the life of the application. The lack of proper application change controls resulted in a higher risk of having program failure when a new version of an application was put into operation. Such failure could affect the billing of exporters for GIPSA administrative tonnage fees, and the accuracy of the weekly grain export report for the commodity trading financial market.

USDA DM 3200-002[25] states that, "all major application systems must use a change control process." The manual requires that the process and the changes made by it should be properly documented. In addition, it states that, "a procedure must exist for approval and acceptance of changes. The process may include a change control board or an individual who is responsible for ensuring that all changes have been properly evaluated."

OMB A-130[26] emphasizes that "separation of duties is the practice of dividing the steps in a critical function among individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such a control keeps a single individual from subverting a critical process."

We interviewed three programmers responsible for the modification of 3 of 10 major applications to obtain an understanding of the change control

[25] USDA Departmental Manual 3200-002, dated March 3, 1988
[26] OMB A-130, Appendix III, dated November 30, 2000

procedure in place. They informed us that each programmer was assigned to program specific application(s). For each application, the programmer was responsible to design, develop, program, modify, test the application(s), and to install the application changes on to the system. We determined that each programmer was responsible for making all of the necessary changes to the application without any oversight by management. As a result, there was no separation of duties between the programming and the placing of the application changes into production.

We also learned from the programmers that there was no documentation in place to show: 1) the request for changes; 2) who approved the modifications; 3) the testing done on the modifications; 4) and who authorized the implementation of the changes.

Lack of proper controls in (1) making software changes, (2) testing the results, and (3) obtaining written approval for the changes made, could allow unauthorized changes to be made on the applications. It also could result in a higher risk of having program failure when a new version of the application is put into operation.

Recommendation No. 20

Develop standardized procedures to track all changes made to major software applications within GIPSA.

Agency Response.

GIPSA accepts the recommendation. GIPSA's new Policies and Procedures Guide takes into account the OCIO Policy CS-009 that addresses standardized procedures for tracking changes made to major software applications in GIPSA.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO that GIPSA's new Policies and Procedures Guide takes into account the OCIO Policy CS-009 that addresses standardized procedures for tracking changes made to major software applications.

Recommendation No. 21

Develop a process to have a second programmer review and verify the program modification prior to implementation.

Agency Response.

GIPSA accepts the recommendation. A second programmer will verify and review the changes prior to implementation. This function will be addressed as part of the release management function in GIPSA's Policies and Procedures guide.

OIG Position.

OIG accepts GIPSA's management decision. We have received a copy of this procedure and verified that this change has been implemented. For final action, please provide documentation to OCFO that GIPSA's Policies and Procedures guide requires a second programmer to verify and to review application changes prior to implementation.

Recommendation No. 22

Ensure application changes are authorized and approved by system development management other than the programmer.

Agency Response.

GIPSA accepts the recommendation. The DAA, application programmer, and the CIO will authorize all major program changes.

OIG Position.

In order to reach management decision please provide the timeframes when procedures will be established to require the DAA, application programmer, and the CIO to authorize all major program changes.

Finding 11 Password Controls Not Established To Secure Access to a Major Application

One of the grain inspection applications did not have logical controls in place to ensure authorized users were verified prior to gaining access to the application. This occurred because GIPSA had not established logical access controls to secure access to the application. As a result, there is a greater potential for unauthorized access to the software applications. Fraudulent transactions such as a fake shipment or a fictitious ship log could be generated from the unauthorized access. This could also result in generating a wrong administrative tonnage fee billing to exporters and misrepresenting the weekly grain export data to commodity traders.

NIST[27] states that there should be controls in place to authorize and restrict activities of users within the application.

Computers are located at grain export elevators throughout the country. Users enter inspection information into the software application, without being forced to use a password, in order to calculate the grain's grade. The software application then generates a log to document the export information to feed into another software application responsible for billing exporters for inspection services based on tonnage handled by the facility, and for reporting the shipment weekly to the public for the commodity trading financial market. The lack of password controls increases the risk of potential unauthorized intrusions to the national database without detection. Unauthorized users can vandalize the system by entering false or inaccurate data, which could affect the inspection, billing, and trading information.

When we pointed out the absence of password controls to the CIO he agreed with us that password controls were needed and would be establishing the password controls to access the software application as soon as possible. At the exit conference, GIPSA's CIO mentioned that the risk of intrusion would be extremely remote because there were compensating controls to detect any unauthorized entry. Nevertheless, he plans to install the password controls.

Recommendation No. 23

Establish formal procedures to require logical access controls to secure access to the application.

Agency Response.

GIPSA accepts the recommendation. The ISSPM has sent a formal request to the application developer requiring logical access controls be put in place to secure the grain inspection application.

OIG Position.

In order to reach management decision, please provide the timeframes when the procedures will be implemented.

Recommendation No. 24

Implement logical access controls requiring users to log in with a password at grain export elevator workstations.

[27] NIST SP 800-18, dated December 1998

Agency Response.

GIPSA accepts the recommendation. The recommended logical access controls will be included in the next deployment that is currently under way and scheduled to be completed by the end of December 2003.

OIG Position.

OIG accepts GIPSA's management decision. For final action, please provide documentation to OCFO that logical access controls are in place.

General Comment

During our review, we noted that the two applications were not electronically linked to reduce the occasional data errors in manually transferring the data between the two applications. The two applications were developed separately. Inspection data is entered into the grain inspection application to generate a ship log. The field office then manually enters the ship logs into the billing application to generate invoices for billing. Per GIPSA management the field offices did have controls in place, such as reconciliation procedures, to ensure that all the ship logs had been entered completely and accurately into the billing application for processing. However, occasional data entry errors do occur, but are corrected within a billing cycle of 30 days; therefore not affecting the financial statements. GIPSA agrees that the benefit of linking the two applications would reduce the redundant efforts of entering support grain inspection information. It would also help to eliminate occasional data errors transferring information from one application to another.

The Joint Financial Management Improvement Program (JFMIP)[28] requires that "financial management systems be designed with effective and efficient interrelationships between software, hardware, personnel, procedures, controls and data contained within the systems." To be integrated, financial management systems must have "a design that eliminates unnecessary duplication of transaction entry." In addition, JFMIP emphasizes:

> *Having a single, integrated financial management system does not necessarily mean that each agency must have only one software application covering all financial management systems needs. Rather, a single integrated financial management system is a unified set of financial systems and the financial portions of mixed systems encompassing the software, hardware, personnel, processes (manual and automated), procedures, controls, and data necessary to carry out financial management functions, manage financial operations of the agency, and report on agency's financial status to central agencies, Congress, and the public.*

GIPSA's IT staff stated that they are developing a new application architecture that will in effect combine the two current applications into one application. Due to the corrective actions planned by GIPSA, we are not recommending any further actions.

[28] JFMPIR-SR-02-01, dated November 2001

Scope and Methodology

Our audit was part of a nationwide audit of selected USDA agencies. We reviewed the adequacy of security over the entire GIPSA computer system and network, the logical and physical access controls, and the controls over the modification of application software.

We identified internal controls related to system vulnerabilities, security of information technology resources, and application life cycle controls. We reviewed these internal controls to ensure the proper management and security of information technology within GIPSA. This audit did not cover the actual testing of the data going through the computer programs. This review only looked at the controls established for writing software applications and for making modifications to those applications.

This review was done at the GIPSA Headquarters office located in Washington, D.C., administered by the IT staff. Fieldwork was performed from November 4, 2002 through December 15, 2002.

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

- We reviewed IT security policies and procedures from OCIO, NIST, GIPSA, and the General Accounting Office (GAO).
- We interviewed responsible GIPSA officials managing the IT computer systems.
- We performed an Internet Security software scan on the GIPSA computer system.
- We analyzed records and controls established to ensure the integrity of the IT security over the GIPSA computer system.

This audit was performed in accordance with generally accepted government auditing standards.

USDA

United States Department of Agriculture

Grain Inspection, Packers and Stockyards Administration

Stop 3601
1400 Independence Ave., SW
Washington, DC 20250-3601

DATE: September 23, 2003

TO: Richard D. Long
Assistant Inspection General
for Audit

ATTN: 30099-1-SF

FROM: Donna Reifschneider
Administrator
Grain Inspection, Packers and Stockyards Administration

SUBJECT: GIPSA Response to Official Draft - Grain Inspection, Packers and Stockyards Administration, Management and Security of Information Technology

Please find attached to this correspondence, the GIPSA response to your official draft report dated August 11, 2003. The attachment includes a response and proposed completion date for each finding and recommended actions. While we have already addressed the hallway glass window in our new computer room, we take exception to adding bars to the windows in that room. The windows are three floors up and in a secured courtyard.

Should questions arise about this response please contact Carol Remmers, Information Systems Security Program Manager at 202-690-0044.

Attachment

GIPSA Response to
USDA/OIG-Audit/30099-1-SF

Senior management and the Chief Information Officer of the Grain Inspection, Packers and Stockyards Administration (GIPSA) would like to thank the OIG staff for the thoroughness and professionalism they exhibited in their review of the Management and Security of our Information Technology Resources. While GIPSA was aware of many of the issues identified in the 30099-1-SF audit and was in the process of addressing them prior to the review, several new issues were raised and brought to a high level of visibility.

GIPSA is currently involved in a top down approach to redesigning and reengineering our Agency's Information Technology. We are involved in developing and documenting an Agency Enterprise Architecture (EA). This includes a Technical Architecture which will address our agency-wide Information Technology security. Each identified module in the new structure will have its own security plan. As part of the new EA, GIPSA has developed a new Policies and Procedures Guide that will insure proper revision management and control.

GIPSA has made major security changes to the management of its Information Technology resources and continues to plan others as detailed in the following responses to the individual OIG findings.

Grain Inspection, Packers and Stockyards Administration
Status on
OIG's Findings and Recommendations

Finding #1:

GIPSA Vulnerability Scans Did Not Detect Vulnerabilities Within Its Own Network

In this finding, the OIG ran IP address scans to detect vulnerabilities on the GIPSA network. GIPSA had been running regular scans prior to the OIG audit; however GIPSA had not been running scans at the Level 5 (most thorough scan). GIPSA had only one employee trained in using the scanning tool.

1) Scans will be run monthly on all GIPSA devices.
2) Scans will be done at the highest level (5).
3) All high and medium vulnerabilities must be addressed within 24 hours and a report of the action taken must be made.
4) Records of all scans and reports on actions taken for all scans must be maintained.
5) Two employees are trained in conducting vulnerability scans.

Recommendation No. 1

GIPSA's Network and Telecommunications Branch took immediate action and corrected all high and medium vulnerabilities identified. A rescan was conducted to insure the vulnerabilities identified were corrected.

A copy of the original scan reports with notes on actions taken was forwarded to Gary Morin of the OIG.

Recommendation No. 2

GIPSA's ISSPM will insure all future scans are run at the maximum level to detect vulnerabilities and that scans are run on a monthly basis.

Recommendation No. 3

GIPSA's ISSPM will monitor low-level vulnerabilities to identify trends and advise network personnel on those areas that could lead to more serious vulnerabilities.

Finding #2:

Access Controls Need To Be Strengthened

In this section, two areas were identified, logical and physical.

1) Logical Access Control:

[ ]
[ ]
[ ]

[ ]
[ ]
[ ]
[

[
[
[

[
[
[
[
[ ]

Currently, these remote users are in the process of transferring from the 5200 to the secure method. This transfer process will be completed by the end of September 2003 at which time the 5200 no longer be used.

2) Physical Access Control:

GIPSA has adopted the OIG's suggestion to install a solid wood panel behind the glass panel of the door to the server room. This was installed in March of 2003.

Although the windows of the server room face out onto a courtyard, the courtyard is three stories up from a secured parking area. The courtyard is protected by an armed guard when open, and only permitted cars are allowed into the parking area. The parking area is secured with a locked iron gate after business hours. Therefore, the iron bars on the windows are unnecessary.

Recommendation No. 4

GIPSA has adopted OIG's suggestion of removing the unsecured dial-in access to the GIPSA network. GIPSA will use the more secure VPN method.

Recommendation No. 5

GIPSA now only allows VPN (secure method) access to its network.

Recommendation No. 6

GIPSA has placed a wooden panel on the inside of its server room door. This keeps the historic look of the building from the hallway view but precludes entry into the room by breaking a glass window.

Recommendation No. 7

Bars on the outside windows are not necessary because the server room is three stories up and faces the inside of a courtyard. The courtyard is protected by an armed guard when open and secured with an iron gate when the area is closed.

Finding #3:

Intrusion Detection Controls Were Inadequate

GIPSA is in full agreement with this finding and is currently in the process of researching an intrusion detection solution for the Agency. We are examining the following options.

Option 1 - IDS run by Office of the Chief Information Officer, USDA (OCIO)

on GIPSA purchased equipment

Minimal …….. $ 46,237.00
Maximum ……..... $207,908.00 (recommended)

Option 2 – IDS run by GIPSA

This option will require equipment plus a dedicated employee to monitor the IDS. GIPSA's ISSPM is still researching.

Recommendation No. 8

[ ]
[ ]

Recommendation No. 9

GIPSA has established internal incident handing procedures. All incidents are immediately reported to the ISSPM or GIPSA Help Desk. The ISSPM or GIPSA Help Desk contacts the appropriate personnel to assist in responding to the incident.

Together, the incident is worked to mitigate security breaches and violations. An incident report is filed and kept open until the incident is resolved.

Finding #4:

Chief Information Officer Had Administrative Privilege

Full system administrative privileges have been removed from the CIO.

Recommendation No. 10

GIPSA has removed the CIO's administrative privileges and has limited the CIO's access to those levels needed to fulfill his oversight responsibilities.

Finding #5:

No Risk Assessments Were Performed

The IT Staff at GIPSA understands the importance of completing thorough risk assessments. In May of 2003, each application developer and Designated Approving Authority (DAA) worked together to complete a risk assessment on each GIPSA system. DAA's were given an information valuation matrix to rate their particular system. The matrix was based on the C-I-A (confidentiality, integrity and availability) model and each DAA assigned a high, medium and low value to each system. After the information valuation was complete, each DAA was given a series of "risk" questions based on high, medium and low risks. The DAA was then asked to sign an "accreditation" form accepting residual risk.

A Program Risk Assessment was completed in June 2003 by a contractor (BackBone Security). GIPSA's ISSPM reviewed a draft report of their findings, made recommendations and is currently waiting for the contractor's reply.

Recommendation No. 11

GIPSA, with the assistance of a contractor, anticipate completing the risk assessment of its General Support System (GIPSA WAN) the end of the second quarter of fiscal year 2004. This is the only risk assessment remaining.

Recommendation No. 12

GIPSA will follow Departmental policy requiring risk assessments be completed at least every three years.

Finding #6:

Mission-Critical Systems Were Not Certified

OCIO, Cyber Security has published a "Certification and Accreditation" (C&A) guide. The primary purpose of this guide is to support the Office of Management and Budget

(OMB) Circular A-130, Appendix III requirement for agencies to "ensure that a management official authorizes in writing the use of each system/application . . . before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every three years."

Ideally, the C&A process should be integrated into the system development life cycle (SDLC) during the capital planning and investment control (CPIC) process. During development, the system security plan (SSP) should be written and the initial risk assessment completed in order to provide an assessment of the possible risks to the system. However, many legacy systems already in place have not gone through the C&A process as part of the SDLC. The requirement for system approval applies to these systems as well. New regulations state that every USDA general support system or major application must have official approval to operate. This approval can consist of an unconditional approval, which is good for three years, or an Interim Approval to Operate (IATO), which is only valid for up to 12 months and is not renewable. An IATO can be granted if risks have been identified and a mitigation plan with a specific timetable for addressing those risks has been approved. If systems have not obtained official approval to operate prior to deployment, they must complete the C&A process and obtain approval to operate.

GIPSA will be forming teams to include members of the IT Staff as well as DAA's in September 2003 to begin the C&A process.

The USDA OCIO will provide training for all agency DAA's in C&A.

Recommendation No. 13

GIPSA's ISSPM will establish certification testing teams in October 2003.

Recommendation No. 14

All current and future systems will be properly tested, certified and authorized.

Finding #7:

Security Plans Were Not Properly Updated And Approved

OCIO has provided guidance to all USDA agencies to assist in completing security plans. This policy is CS-025. GIPSA will use this policy to more effectively complete the required plans.

Recommendation No. 15

GIPSA's ISSPM has given each DAA and application programmer a copy of OCIO's CS-025 to assist them in understanding the importance of up-to-date security plans.

GIPSA has established policy that directs annual security plans to be reviewed and completed.

Recommendation No. 16

GIPSA has established the following formal approval process for security plans that documents the name, date and title of the approving management official.

1) ISSPM
2) CIO
3) Deputy Administrators
4) Administrator

The plans are then sent to Chief of Cyber Security, OCIO.

Finding #8:

GIPSA Did Not Have An IT Contingency Plan

Currently, GIPSA's ISSPM is working with the DAA's and application developers to complete contingency plans. The plans are split into two groups: The WAN and those applications which run on the WAN and GIPSA's stand alone applications.
Systems cannot be certified and accredited unless a contingency plan has been written and tested. C&A methodology outlined by the Department will guide GIPSA system owners and program managers with uniform guidance on how to certify and accredit their IT systems and complete the required contingency plans.

Recommendation No. 17

GIPSA's ISSPM, along with the DAA's and application developers are working on completing the plans. The estimated time for completion is December 2003.

Finding #9:

Required Security Clearances For IT Staff Were Not Obtained

Recommendation No. 18

Security clearances will be submitted for all IT personnel by the end of 2003.

Recommendation No. 19

GIPSA will formally request that OPM expedite the security clearances for employees in IT positions by the end of September 2003.

Finding #10:

Proper Application Change Controls Were Not Established

OCIO, Cyber Security has created policy that will assist GIPSA in setting up a successful configuration management program (CM). The CM program is part of the overall Policies and Procedures Guide that has been developed to manage all new IT development within GIPSA. CM ensures that the hardware, software, communications services and documentation for a system can be accurately determined at any time.

The objectives of CM are to:

- Provide controls to ensure the system operates correctly throughout its life;
- Ensure that the configuration of all system components is available and accurate at all times;
- Ensure the pertinent functional and physical interfaces between systems, equipment, and software are correctly and adequately documented;
- Provide maintenance efficiency by ensuring that change proposals are adequately acted upon; and
- Ensure that the impact of any change to system functionality, security, performance, and cost is known at the time the change is approved.

Recommendation No. 20

GIPSA's new Policies and Procedures Guide takes into account the OCIO Policy CS-009 that addresses standardized procedures for tracking changes made to major software applications in GIPSA.

Recommendation No. 21

A second programmer will verify and review the change prior to implementation. This function will be addressed as part of the release management function in GIPSA's Polices and Procedures guide.

Recommendation No. 22

All major changes will be authorized by the DAA, application programmer and the CIO.

Finding #11

Password Controls Not Established To Secure Access To A Major Application

The major application (CUSUM) did not have password controls in place because the PC's are located in a secure room in the grain elevator. Only authorized employees are permitted to enter the grain elevators alone because all visitors are escorted and never left alone. The risk of an intrusion is low. The risks will be further reduced by requiring user passwords in the next deployment.

Recommendation No. 23

The ISSPM has sent a formal request to the application developer requiring logical access controls be put in place to secure the CUSUM application.

Recommendation No. 24

The recommended logical access controls will be included in the next deployment that is currently under way and scheduled to be completed by the end of December 2003.

Glossary of Terms

Continuity Of Operations Plan (Coop) - This is a plan that will be implemented if a situation occurs that requires the immediate and unexpected relocation of the GIPSA network from Washington, D.C., because of a national emergency or declaration of a disaster.

Local Area Network (LAN) – a local area network is a group of computers and associated devices that share a common communications line and typically share the resources of a single process or server with a small geographic area). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may server as few as two or three users or many as thousands of users.

Public Access Network – In computer networks, a public access network is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.

In a typical public access network configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to WEB sites or other companies accessible on the public network. The public access network host then initiates sessions for these requests on the public network. It can only forward packets that have already been requested.

Users of the public network outside the company can access only the public access network host. The public access network may typically also have the company's Web pages so these could be served to the outside world. However, the public access network provides Web pages might be corrupted but no other company information would be exposed. Cisco, the leader maker of routers, is one company that sells products designed for setting up a public access network.

Transmission Control Protocol/Internet Protocol (TCP/IP) - TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.

Virtual Private Network (VPN) – A virtual private network is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

Informational copies of this report have been distributed to:

Agency Liaison Officer (4)
General Accounting Office (1)
Office of Management and Budget (1)
Office of the Chief Financial Officer
  Director, Planning and Accountability Division (1)