INFORMATION SECURITY PROGRAM

National Transportation Safety Board

Report Number: FI-2004-097
Date Issued: September 28, 2004

U.S. Department of Transportation
Office of the Secretary of Transportation

Office of Inspector General
Washington, D.C. 20590

September 28, 2004

The Honorable Ellen Engleman Conners
Chairman
National Transportation Safety Board
490 L'Enfant Plaza, SW
Washington, DC 20594

Dear Chairman Engleman Conners:

This report presents the results of our audit of the information security program at the National Transportation Safety Board (NTSB). The Federal Information Security Management Act (FISMA) of 2002 requires each agency to develop, document, and implement an agencywide information security program to protect the information and information systems that support the operations and assets of the agency. FISMA also requires 24 large Federal agencies to report annually to the Congress on their information security programs. This year the Office of Management and Budget (OMB) expanded FISMA reporting requirements to all departments and agencies that are subject to the Paperwork Reduction Act of 1995, including NTSB.

NTSB is responsible for investigating accidents in all transportation modes to determine the cause and recommend changes to improve safety and reduce the likelihood and consequences of future accidents. NTSB plays a critical role in ensuring a safe transportation system. To support its investigation operations nationwide, NTSB has implemented an information technology (IT) infrastructure, including communication networks, computer laboratories, and various software application systems, to support NTSB's Headquarters, 10 regional offices, and the NTSB Academy. This IT infrastructure enables NTSB's investigators to gather accident evidence, analyze information from voice and data recorders, assist victims' family members, and provide accident investigation results to the American public. NTSB invests about $2 million to $3 million annually in IT system operations.

Responding to requirements of FISMA, the Department of Transportation Office of Inspector General performed an audit of the NTSB's information security program. Our objectives were to (1) evaluate the effectiveness of NTSB's information security program, and (2) provide input to NTSB's annual FISMA report by answering questions specified by OMB.

Since this is the first year that NTSB has been asked to implement the FISMA requirements, we focused our audit on the overall adequacy of the information security program and network security. The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States. We plan to do a more detailed evaluation during fiscal year (FY) 2005. Our input to NTSB's annual FISMA report is in Enclosure 1. Our scope and methodology are described in Enclosure 2.

Results in Brief

NTSB has installed firewall security to protect its IT infrastructure against cyber attacks from the Internet and is using a swipe card system to control physical access at the Headquarters. However, we found that NTSB's network computers are vulnerable to unauthorized access by insiders as a result of a lack of an agencywide information security program.

FISMA requires each agency, through the Chief Information Officer (CIO), to implement an agencywide information security program to protect the information and information systems that support the operations and assets of the agency. To effectively implement this program, agencies need to develop and implement security plans and maintain a system inventory. As part of its responsibilities under FISMA, OMB also requires agencies perform security certification review on their information systems. However, we found that none of the following requirements had been implemented at NTSB:

- Designating an agency CIO, or equivalent, responsible for the implementation of an agencywide information security program;
- Establishing a system inventory of major information systems;
- Developing security plans in accordance with the National Institute of Standards and Technology guidance;
- Requiring information systems be certified as adequately secured commensurate with operational risks before accreditation for business use; and

- Documenting security weaknesses and corrective actions in the Plan of Action and Milestones, as required by OMB.

Using commercial scanning software, we performed a vulnerability assessment on NTSB private networks and the firewall server. Our assessment showed that the firewall is reasonably configured to prevent unauthorized access from the Internet. Due to time constraints, we did not perform a complete review of the firewall security capabilities. We plan to perform a more detailed review of NTSB's firewall security in FY 2005. However, we found NTSB systems and data are vulnerable to insiders—we identified over 250 high-risk, 460 medium-risk, and 4,500 low-risk vulnerabilities on NTSB network computers.[1] All the high-risk vulnerabilities we identified were on the "Top Twenty Vulnerabilities List" jointly developed by the SANS Institute and Department of Homeland Security. These vulnerabilities could allow insiders—NTSB employees, contractors, and business associates—to gain unauthorized access to NTSB business information stored on these computers.

For example, with these vulnerabilities, we were able to gain total (root-level) control of 28 NTSB computers, including a computer in the Chairman's Office. We could have changed computer configurations, installed virus software, or deleted all files on the computers. In fact, we did obtain substantial sensitive information from these computers, such as:

- NTSB payroll data that list the annual salaries and social security numbers of NTSB employees, including the Chairman and Board members;

- Internal documents on preliminary investigation issues; and

- Personal information including employee's birth dates, home addresses, and credit card numbers.

Our network activities went undetected because NTSB has no intrusion detection and monitoring capabilities.

The lack of an agencywide information security program puts the integrity, confidentiality, and availability of NTSB business operations at risk, as we demonstrated. In our opinion, this constitutes a significant deficiency and should be reported as a material internal control weakness to OMB and Congress under the Federal Managers' Financial Integrity Act of 1982.

[1] High-risk vulnerabilities may provide an attacker with immediate access into a computer system, such as allowing execution of remote commands. Medium-risk and low-risk vulnerabilities may provide an attacker with useful information, such as password files, they can then use to compromise a computer system.

NTSB has demonstrated a strong commitment to strengthen its information security practices. During the last quarter of FY 2004, NTSB began to develop a system inventory, started to provide security awareness training to employees, and provided specialized training to 40 percent of its employees with significant IT security responsibilities. Responding to a draft of this report, the NTSB Chairman agreed to take immediate actions to eliminate the high-risk and medium-risk vulnerabilities we identified. The NTSB Chairman also agreed to implement our recommendations by appointing a CIO and implementing an effective information security program in FY 2005. These corrective actions, when fully implemented, will establish a solid foundation for an effective information security program that will enhance the integrity, confidentiality, and availability of NTSB information system operations.

FINDING AND RECOMMENDATIONS

NTSB Needs To Implement an Agencywide Information Security Program

FISMA requires each agency, through the CIO, to implement an agencywide information security program to protect the information and information systems that support the operations and assets of the agency. To effectively implement this program, agencies need to develop and implement security plans and maintain a system inventory. As part of its responsibilities under FISMA, OMB also requires agencies perform security certification review on their information systems. However, we found that none of these requirements had been implemented at NTSB.

NTSB does not have an agency CIO. The Director of the Office of Research and Engineering has assumed limited CIO responsibilities for managing IT resource and providing information security to NTSB networks and computer systems. However, this official was not given clear authority and responsibility to develop and maintain an agencywide information security program, including effective implementation of security policies, procedures, and control techniques. Further, NTSB did not:

- Have an inventory of all the information systems used to support its operational needs;

- Develop security plans for protecting its information systems, which should address rules of behavior for system use, training requirements for security responsibilities, personnel controls, technical controls,

continuity of operations, incident response capabilities, and system interconnections.[2]

- Require information systems be certified as adequately secured commensurate with operational risks before accreditation for business use; and

- Document security weaknesses and corrective actions in the Plan of Action and Milestones, as required by OMB.

In response to our audit, NTSB has agreed to appoint a CIO and assign a priority to implementing an effective information security program in FY 2005. Specifically, NTSB has initiated an inventory of the information systems used by various offices to support their business operations, agreed to develop a security plan for each system, establish a target date to have all information systems undergo security certification reviews, and document security weaknesses and corrective actions as required by OMB.

NTSB Needs To Strengthen Network Security To Prevent Unauthorized Access by Insiders

In addition to publishing the final accident investigation results on its public websites, NTSB uses its private network to support investigation work, such as analyzing information from voice and data recorders, storing information concerning victims' family members, and processing payroll and personnel information. This private network can be accessed by authorized users at NTSB Headquarters and regional offices or from a remote location through telephone line (dial-up) connections.

To protect its private networks, NTSB has installed firewall security as the first-level defense against cyber attacks from the Internet and password security over remote access through telephone line connections. Using commercial scanning software, we performed a vulnerability assessment on NTSB private networks and the firewall server. Our assessment showed the firewall is reasonably configured to prevent unauthorized access from the Internet. However, we found that NTSB networks are vulnerable to unauthorized access by insiders—NTSB employees, contractors, and business associates.

Specifically, we identified a total of 5,309 (256 high-risk, 461 medium-risk, and 4,592 low-risk) vulnerabilities on 719 NTSB network computers. All the high-risk vulnerabilities we identified were on the "Top Twenty Vulnerabilities

[2] National Institute of Standards and Technology Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," December 1998.

List" jointly identified by the SANS Institute and the Department of Homeland Security. A summary of the scanning result is shown in the table.

Table. NTSB Network Scanning Results

Location	Vulnerabilities Found			Total Vulnerabilities	Computers Scanned
	High	Medium	Low		
HQ Networks	189	360	1809	2358	493
Field Networks	67	101	2783	2951	226
Total	**256**	**461**	**4592**	**5309**	**719**

While scanning the NTSB networks, we gained total (root-level) control of 28 computers, including a computer in the Chairman's office. With this level of control, we could have changed computer configurations, installed virus software, or deleted all files on the computers.

In fact, we were able to copy substantial information from these computers, such as NTSB payroll data that list the annual salaries and social security numbers of all NTSB employees, including the Chairman and Board members; internal documents on preliminary investigation issues; and identifiable personal information, including employee's birth dates, home addresses, and credit card numbers.

NTSB management was not aware of the existence of these vulnerabilities because NTSB has not obtained the proper tools and trained personnel to periodically scan its networks for protection. Also, our network activities went undetected because NTSB has no intrusion detection and monitoring capabilities that can detect abnormal activities on its private networks.

These network vulnerabilities existed due to inadequate configuration controls and patch management. NTSB did not meet the Government security configuration requirements for its computers. For example, among the 28 computers that we took control over, 24 of them required no passwords for the system administrator account, and the other 4 used passwords that could be easily guessed, such as "password." We also found NTSB has not established a procedure to promptly install software patches as required by OMB. For example, we found 14 critical software patches released by a manufacturer had not been installed on NTSB computers. Installing these patches could have easily eliminated 20 percent of the high-risk vulnerabilities we identified.

NTSB is taking actions to fix the high-risk and medium-risk vulnerabilities and is reviewing the remaining ones. In addition to strengthening network configuration

controls and patch management, NTSB also needs to establish vulnerability scanning and intrusion detection capabilities to protect its network computers against unauthorized access.

As we demonstrated, the lack of an agencywide information security program puts the integrity, confidentiality, and availability of NTSB business operations at risk. In our opinion, this constitutes a significant deficiency and should be reported as a material internal control weakness on the annual Federal Managers' Financial Integrity Act report to OMB and Congress.

RECOMMENDATIONS

A. We recommend that the NTSB Chairman:

1. Designate a Chief Information Officer to enhance the information security management practice in NTSB.

2. Direct the Chief Information Officer to implement an agencywide information security program by December 31, 2004, that includes:

    a. Providing security awareness training to all employees and specialized training to employees with significant IT security responsibilities,

    b. Completing an information systems inventory,

    c. Establishing a schedule to complete system security certification reviews of all systems,

    d. Providing guidelines to system owners for developing and implementing security plans to address security requirements and responsibilities for NTSB networks, facilities, and systems or groups of information systems, and

    e. Documenting security weaknesses identified and corrective actions taken in accordance with OMB guidance.

3. Direct the Chief Information Officer to enhance NTSB network security by:

    a. Correcting all high-risk and medium-risk vulnerabilities we identified by December 31, 2004.

    b. Ensuring network computers are properly configured in accordance with Government standards and developing procedures to ensure timely installation of software patches by March 31, 2005.

c. Obtaining proper tools and training personnel to periodically scan networks for potential vulnerabilities and deploying an intrusion detection capability to monitor network traffic for abnormal activities by June 30, 2005.

MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR GENERAL ANALYSIS

A draft of this report was provided to the NTSB Chairman for comments on September 20, 2004. The Chairman responded on September 22, 2004, and concurred with all recommendations (see Appendix). The actions planned by NTSB are reasonable and should provide a solid foundation to implement an effective computer security program. We will continue monitoring NTSB's progress in implementing these recommendations.

We appreciate the courtesies and cooperation of National Transportation Safety Board representatives during this audit. If you have any questions concerning this report, please call me on (202) 366-1992 or Theodore P. Alves, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1496.

Sincerely,

Alexis M. Stefani
Principal Assistant Inspector General
for Auditing and Evaluation

Enclosures (3)

Enclosure 1. Office of Inspector General Input to FISMA Report

FY 2004 marks the first time that NTSB needs to comply with FISMA, which requires independent evaluation of agencies' information security programs. Accordingly, the Department of Transportation Office of Inspector General performed a review of NTSB's information security program. NTSB's key missions are investigating accidents in all transportation modes, determining the causes, and making recommendations to improve safety. It has implemented an IT infrastructure, including communication networks, computer laboratories, and various software application systems, to support operations at NTSB Headquarters, 10 regional offices, and its Academy. NTSB invests about $2 million to $3 million annually in IT system operations.

Unlike the 24 large Federal agencies that first had to comply with FISMA, NTSB does not have a Chief Information Officer responsible for IT management and security. We also found that NTSB has not implemented an agencywide information security program, including establishing a system inventory, conducting system security certification reviews in accordance with the National Institute of Standards and Technology guidance, and developing security plans. In other words, when compared with large Federal agencies, NTSB is in an early stage of complying with FISMA requirements. Our answers to OMB questions reflect the fact that NTSB is in the *early stage* of implementing an IT security program.

Our independent evaluation also identified vulnerabilities in NTSB's networks, which enabled us (acting as an insider) to gain unauthorized access to sensitive information such as employees' salaries, social security numbers, home addresses, and credit card numbers, as well as preliminary accident investigation results. In our opinion, NTSB's information security program constitutes a significant deficiency and should be reported as a material internal control weakness to OMB and Congress under the Federal Managers' Financial Integrity Act of 1982.

NTSB has demonstrated a strong commitment to strengthening its information security practices. During the last quarter of FY 2004, it made an effort to develop a system inventory, started providing security awareness training to employees, and provided specialized training to 40 percent of its employees with significant IT security responsibilities. The NTSB Chairman also agreed to implement the recommendations specified in our independent evaluation report. These corrective actions, when fully implemented, will enhance the integrity, confidentiality, and availability of NTSB information system operations. We plan to conduct a detailed review of NTSB's implementation efforts and will include the results in next year's FISMA report.

2004 FISMA Report

Agency:	National Transportation Safety Board
Date Submitted:	09/28/2004
Submitted By:	OIG

Contact Information:

Name:	Rebecca Leng
E-mail:	Rebecca.C.leng@oig.dot.gov
Phone:	202-366-1488

To enter data in allowed fields, use password: fisma

Section A: System Inventory and IT Security Performance
NOTE: ALL of Section A should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

A.1. By bureau (or major agency operating component), identify the total number of programs and systems in the agency and the total number of contractor operations or facilities. The agency CIOs and IG's shall each identify the total number that they reviewed as part of this evaluation in FY04. NIST 800-26, is to be used as guidance for these reviews.

A.2. For each part of this question, identify actual performance in FY04 for the total number of systems by bureau (or major agency operating component) in the format provided below.

	A.1						A.2									
	A.1.a. FY04 Programs		**A.1.b.** FY04 Systems		**A.1.c.** FY04 Contractor Operations or Facilities		**A.2.a.** Number of systems certified and accredited		**A.2.b.** Number of systems with security control costs integrated into the life cycle of the system		**A.2.c.** Number of systems for which security controls have been tested and evaluated in the last year		**A.2.d.** Number of systems with a contingency plan		**A.2.e.** Number of systems for which contingency plans have been tested	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
NTSB					1	1	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
Agency Total	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**

Comments: This is the first year that NTSB has been asked to implement the FISMA reporting requirement. NTSB is in the process of identifying its program and systems. NSTB's financial system is operated by the Department of Interior. An application control for this system has been reviewed by an independent audit firm. NTSB has agreed to finalize its system inventory and develop a timetable for conducting C&A reviews by December 31, 2004.

A.3	
A.3. Evaluate the degree to which the following statements reflect the status in your agency, by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.	
Statement	**Evaluation**
a. Agency program officials and the agency CIO have used appropriate methods to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.	Rarely, or 0-50% of the time
b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, 800-26.	Rarely, or 0-50% of the time
c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.	Rarely, or 0-50% of the time
d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.	Rarely, or 0-50% of the time
e. The OIG was included in the development and verification of the agency's IT system inventory.	Rarely, or 0-50% of the time
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	Rarely, or 0-50% of the time
g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.	Rarely, or 0-50% of the time
Statement	**Yes or No**
h. The agency has begun to assess systems for e-authentication risk.	No
i. The agency has appointed a senior agency information security officer that reports directly to the CIO.	No

Comments: To meet the FISMA requirements, NTSB has initiated an effort to inventory the information systems used by program offices, and agreed to finalize the system inventory by December 31, 2004. In addition, the NTSB Chairman has designated an agency Chief Information Officer who is responsible for IT management and security.

Section B: Identification of Significant Deficiencies
NOTE: ALL of Section B should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

B.1. By bureau, identify all FY 04 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row, and identify which are repeated from FY03. In addition, for each significant deficiency, indicate whether a POA&M has been developed. Insert rows as needed.

B.1.

Bureau Name	FY04 Significant Deficiencies			
	Total Number	Total Number Repeated from FY03	Identify and Describe Each Significant Deficiency	POA&M developed? Yes or No
NTSB	1	0	NTSB information security protgram	No
Agency Total	1	0		

Comments: The lack of an agencywide information security program constitutes a significant deficiency. We recommend that this be reported to OMB and Congress under FMFIA as a material internal control weakness.

Section C: OIG Assessment of the POA&M Process
NOTE: Section C should *ONLY* be completed by the OIG. The CIO should leave this section blank.
To enter data in allowed fields, use password: fisma

C.1. Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone (POA&M) process. This question is for IGs only. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.

C.1

Statement	Evaluation
a. Known IT security weaknesses, from all components, are incorporated into the POA&M.	Rarely, or 0-50% of the time
b. **Program officials** develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.	Rarely, or 0-50% of the time
c. Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Rarely, or 0-50% of the time
d. **CIO** develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	Rarely, or 0-50% of the time
e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Rarely, or 0-50% of the time
f. The POA&M is the authoritative agency **and** IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	Rarely, or 0-50% of the time
g. System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11).	Rarely, or 0-50% of the time
h. OIG has access to POA&Ms as requested.	Rarely, or 0-50% of the time
i. OIG findings are incorporated into the POA&M process.	Rarely, or 0-50% of the time
j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Rarely, or 0-50% of the time

Comments: NTSB has not conducted any security reviews of its information systems, or used POA&M to track security weaknesses for corrections. NTSB has agreed to develop guidelines for security reviews and reporting POA&M by the end of December 31, 2004.

C.1 OIG Assessment of the Certification and Accreditation Process
Section C should only be completed by the OIG. OMB is requesting IGs to assess the agency's certification and accreditation process in order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST Special Publication 800-37 should be consistent with NIST Special Publication 800-37. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST Special Publication 800-37. Agencies were not expected to use NIST Special Publication 800-37 as guidance before it became final.

Statement	Evaluation
Assess the overall quality of the Agency's certification and accreditation process. Comments: NTSB has not performed security certification reviews on any of its information systems. NTSB has agreed to finalize its system inventory, and establish a schedule to complete Certification and Authorization (C&A) reviews on all systems in the system inventory by December 31, 2004.	

Section D
NOTE: ALL of Section D should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

D.1. First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agencywide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. **For example:** If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration controls are implemented, the answer would reflect "yes" and "51-70%". If appropriate or necessary, include comments in the Comment area provided below.

D.2. Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below.

D.1. & D.2.

	Yes, No, or N/A	Evaluation
D.1. Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?	No	
a. Windows XP Professional		
b. Windows NT		
c. Windows 2000 Professional		
d. Windows 2000		
e. Windows 2000 Server		
f. Windows 2003 Server		
g. Solaris		
h. HP-UX		
i. Linux		
j. Cisco Router IOS		
k. Oracle		
l. Other. Specify: MS SQL		
	Yes or No	**Evaluation**
D.2. Do the configuration requirements implemented above in D.1.a-f., address patching of security vulnerabilities?		

Comments: OIG review identified weak configuration controls and a lack of timely installation of software patches. NTSB has agreed to develop a procedure to implement Government security configuration standards on computer systems, and ensure timely patch installations by March 31, 2005.

Section E: Incident Detection and Handling Procedures
NOTE: ALL of Section E should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

E.1. Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.

E.1

Statement	Evaluation
a. The agency follows documented policies and procedures for reporting incidents internally.	Rarely, or 0-50% of the time
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	Rarely, or 0-50% of the time
c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov	Rarely, or 0-50% of the time

E.2.

E.2. Incident Detection Capabilities.

	Number of Systems	Percentage of Total Systems
a. How many systems underwent vulnerability scans and penetration tests in FY04?		

b. Specifically, what tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?

Answer:

NTSB has installed firewall security as the first-level defense against cyber attacks from the Internet, and password security over remote access through telephone line (dial-up) connections.

Comments:

NTSB has not established vulnerability scanning and incident reporting capabilities. Using commercial scanning software, OIG identified over 250 high, 460 medium, and 4,500 low vulnerabilities on over 700 computers. NTSB is taking actions to fix the identified vulnerabilities, and has agreed to establish vulnerability scanning and intrusion detection & reporting capabilities by June 30, 2005.

Section F: Incident Reporting and Analysis
NOTE: ALL of Section F should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

F.1. For each category of incident listed: identify the total number of successful incidents in FY04, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category VII, "Other". If appropriate or necessary, include comments in the Comment area provided below

F.2. Identify the **number of systems** affected by each category of incident in FY04. If appropriate or necessary, include comments in the Comment area provided below.

F.1., F.2. & F.3.

	F.1. Number of Incidents, by category:			F.2. Number of systems affected, by category, on:		
	F.1.a Reported internally	F.1.b. Reported to US-CERT	F.1.c. Reported to law enforcement	F.2.a. Systems with complete and up-to-date C&A	F.2.b. Systems without complete and up-to-date C&A	F.2.c. How many successful incidents occurred for known vulnerabilities for which a patch was available?
	Number of Incidents	Number of Incidents	Number of Incidents	Number of Systems Affected	Number of Systems Affected	Number of Systems Affected
I. Root Compromise	0	0	0	NA	NA	NA
II. User Compromise	0	0	0			
III. Denial of Service Attack	0	0	0			
IV. Website Defacement	0	0	0			
V. Detection of Malicious Logic	0	0	0			
VI. Sucessful Virus/worm Introduction	0	0	0			
VII. Other	0	0	0			
Totals:	0	0	0	0	0	0

Comments: As part of the FISMA audit, OIG was able to obtain root-level control of 28 computers on NTSB networks. These activities were undetected because NTSB has not established incident monitoring capabilities. NTSB has agreed to implement intrudsion detection capabilities by June 30, 2005.

Section G: Training
NOTE: ALL of Section G should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

G.1. Has the agency CIO ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? If appropriate or necessary, include comments in the Comment area provided below.

G.1.

G.1.a. Total number of employees in FY04	G.1.b. Employees that received IT security awareness training in FY04, as described in NIST Special Publication 800-50		G.1.c. Total number of employees with significant IT security responsibilities	G.1.d. Employees with significant security responsibilities that received specialized training, as described in NIST Special Publications 800-50 and 800-16		G.1.e. Briefly describe training provided	G.1.f. Total costs for providing IT security training in FY04 (in $'s)
	Number	Percentage		Number	Percentage		
430	0	0%	14	6	40%		

G.2.

	Yes or No	
a. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?	No	

Comments: NTSB will provide security awareness training to all employees by December 2004 and specialized training to the employees with significant IT security responsibilities by October 31, 2004.

Enclosure 2. Scope and Methodology

To fulfill the requirements under FISMA, we reviewed the NTSB information security program. We also provided input to NTSB's FISMA report by answering questions specified by OMB.

We interviewed managers in the Office of Chief Financial Officer, the Office of Research and Engineering, and the Office of Transportation Disaster Assistance to gather background information. We reviewed documents on security policies and network diagrams and observed operations in the three computer laboratories: the Material Research Laboratory, Vehicle Reorders Research Laboratory, and Vehicle Performance Research Laboratory. By using commercial scanning software, we performed a limited vulnerability assessment of NTSB private networks and the firewall server.

We performed our work between July and September 2004 at NTSB Headquarters in Washington, DC. The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States, and included such tests as we considered necessary to provide reasonable assurance of detecting abuse or illegal acts.

Enclosure 3. Major Contributors to This Report

The following individuals contributed to this report.

Name	Title
Rebecca C. Leng	Deputy Assistant Inspector General for Information Technology and Computer Security
Ping Z. Sun	Project Manager
John M. Johnson	Senior IT Specialist

Appendix. Management Comments

NTSB
National Transportation Safety Board
490 L'Enfant Plaza, SW
Washington, DC 20594-0001
www.ntsb.gov

Office of the Chairman

September 22, 2004

Theodore P. Alves
Assistant Inspector General for Financial
and Information Technology Audits
Department of Transportation
400 7th Street S.W.
Washington, DC 20590

Dear Mr. Alves:

Thank you for the opportunity to provide comments on the draft report of your review of the National Transportation Safety Board's information security program, as required by the Federal Information Security Management Act (FISMA). We agree with the general conclusions reached in your review of our information security program, and I am providing specific comments on the recommendations contained in the report as an enclosure to this letter.

We are pleased that you have recognized the Safety Board's commitment to developing a sound and compliant information security program, and for your work with our Information Technology staff to evaluate the threats to, and vulnerabilities of, our systems. We concur with the report's conclusion that the Safety Board's lack of a formal agency-wide information security program represents a material internal control weakness, and we will reflect that conclusion in our report to Office of Management and Budget and Congress under the Federal Manager's Financial Integrity Act (FMFIA) of 1982.

If you have any questions, please contact Dr. Vernon Ellingstad, Director of the Office of Research and Engineering and Chief Information Officer, on (202) 314-6501.

Sincerely,

Ellen Engleman Conners
Chairman

Attachment

Attachment

Recommendations and Responses

Recommendation 1:

Designate a Chief Information Officer to enhance the information security management practice in NTSB.

Response: Concur. Effective immediately, Dr. Vernon Ellingstad, Director of the Office of Research and Engineering, has been designated as the Safety Board's Chief Information Officer with responsibility and authority to develop and manage the Board's information security program.[1]

Recommendation 2:

Direct the Chief Information Officer to implement an agencywide information security program by December 31, 2004 that includes:

a) Providing security awareness training to all employees, and specialized training to employees with significant IT security responsibilities.
b) Completing an information systems inventory.
c) Establishing a schedule to complete system security certification reviews of all systems.
d) Providing guidelines to system owners for developing and implementing security plans to address security requirements and responsibilities for NTSB networks, facilities, and systems or groups of information systems.
e) Documenting security weaknesses identified and corrective actions taken in accordance with OMB guidance.

Response: Concur. The Safety Board has begun the development of a formal information security program and has identified the Gov Online Learning Center course titled "IT Security Awareness FY2004" as the appropriate training module for all Safety Board staff. All employees will be required to complete this on-line training by December 31, 2004. Specialized security training has been identified for all employees with significant IT security responsibilities, and these 14 individuals will have completed the training by October 31, 2004. A preliminary systems inventory has been completed and will be reflected in the Safety Board's FISMA report, which will be submitted to OMB by October 6, 2004. The broad outlines of the agency security plan, including a schedule for system security certification reviews in accordance with NIST guidelines, the development of security guidelines for NTSB system owners, and the formulation of a plan to monitor and document security weaknesses, will be completed by the end of calendar year 2004.

Recommendation 3:

Direct the Chief Information Officer to enhance NTSB network security by:

a) Correcting all high and medium-risk vulnerabilities we identified by December 31, 2004.
b) Ensuring network computers are properly configured in accordance with Government standards, and develop procedures to ensure timely installation of software patches by March 31, 2005.

---

[1] This action is not related to the Information Technology Management Reform Act, which imposed requirements on the 24 large Executive Branch agencies.

c) *Obtaining proper tools and training personnel to periodically scan networks for potential vulnerabilities, and deploy intrusion detection capability to monitor network traffic for abnormal activities by June 30, 2005.*

Response: Concur. We have determined that a majority of the vulnerabilities identified in the DOT Inspector General's network scan were generated by a small number of desktop PCs used for software development and testing, or network devices controlling functions such as network scanners and copiers, the video surveillance system, and the Board's Keyscan security system. Steps have already been taken to eliminate most of these vulnerabilities and we will correct the balance of the high- and medium-risk vulnerabilities by December 31, 2004.

The network security plan (to be completed by December 31, 2004) will specifically address the issue of configuration management of desktop workstations. The plan will include procedures to ensure the timely installation of needed software patches, and these procedures will be implemented by March 31, 2005.

Personnel assignments have been adjusted to ensure proper staffing of network security functions and proper training of staff with system security responsibilities. A significant part of the duties of a recently hired network specialist, for example, includes the implementation of an intrusion detection system and regular review of system logs for security issues. Efforts are currently underway to identify specific hardware and software tools to accomplish internal vulnerability scans and to monitor for intrusion detection. A basic set of such tools will be acquired, and staff training for their application completed, by June 30, 2005.