INFORMATION SECURITY PROGRAM

National Transportation Safety Board

Report Number: FI-2006-001
Date Issued: October 7, 2005

U.S. Department of
Transportation

Office of the Secretary
of Transportation

Office of Inspector General
Washington, D.C. 20590

October 7, 2005

The Honorable Mark V. Rosenker
Acting Chairman
National Transportation Safety Board
490 L'Enfant Plaza, SW
Washington, DC 20594

Dear Acting Chairman Rosenker:

This report presents the results of our audit of the National Transportation Safety Board's (NTSB) information security program. 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.

This is the second year that small agencies such as NTSB are required to report to the Congress on their information security program.[1] 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 at NTSB's Headquarters, 10 regional offices, and its 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

[1] FISMA requires 24 large Federal agencies to report annually to the Congress on their information security programs. Last year the Office of Management and Budget expanded FISMA reporting requirements to all Departments and agencies that are subject to the Paperwork Reduction Act of 1995, including NTSB.

investigation results to the American public. NTSB invested about $2.7 million in IT system operations in Fiscal Year (FY) 2005.

Responding to FISMA requirements, the Department of Transportation's Office of Inspector General (OIG) performed an audit of NTSB's information security program last year for the first time. We found that NTSB lacked basic information security elements such as a system inventory, process to certify and accredit systems security, mechanisms to identify network vulnerabilities, and ability to respond to security incidents in a timely manner.

As a result, we reported to NTSB that its information security program should be reported to OMB as a material weakness under the Federal Managers' Financial Integrity Act (FMFIA) of 1982 and recommended immediate corrective actions.[2] NTSB management had agreed to take aggressive actions, including appointment of a Chief Information Officer (CIO) to lead the effort.

This year, we did a follow-up review of NTSB's information security program and network security. The objectives were to determine whether (1) NTSB has made adequate progress in implementing the planned actions, (2) network connections to outside entities, including the Internet, are adequately protected to prevent cyber attacks, and (3) internal network computers are properly configured to reduce the risk of attacks.

We conducted the performance audit in accordance with Generally Accepted Government Auditing Standards as prescribed by the Comptroller General of the United States, and performed such tests as we considered necessary to detect fraud, waste, and abuse. Our input to NTSB's annual FISMA report to OMB is in Enclosure 1. Our scope and methodology are described in Enclosure 2.

RESULTS IN BRIEF

While a CIO was appointed in September 2004, NTSB has made limited progress in enhancing its information security program. Our review of the network security controls also identified a significant number of vulnerabilities that exposed NTSB computers to unauthorized access from both inside and outside of the agency. During the audit, our staff was able to crack the password in an Internet router that is used to control access from the Internet. In addition, we were able to obtain sensitive investigation information from NTSB computers, including real-time audio recording between air traffic controllers and pilots during an accident.

[2] OIG Report Number FI-2004-097, "NTSB Information Security Program," September 28, 2004. OIG reports can be found at www.oig.dot.gov.

Accordingly, it is our opinion that NTSB's information security program remains a material weakness to its safety investigation mission.

The following summarizes what we found.

NTSB did not make a strong commitment to implement an agencywide information security program as promised. The following summarizes the status of NTSB's corrective actions (see Table 1).

Table 1. Delays in Implementing Planned Corrective Actions

Recommended Corrective Actions	Target Completion	Current Status as of September 30, 2005
1. Appoint a Chief Information Officer		Completed
2. Implement an information security program		
2a. Provide security training to employees	December 31, 2004	82% completed
2b. Complete an information systems inventory	December 31, 2004	Open
2c. Establish a schedule to have systems security certified and accredited	December 31, 2004	Open
2d. Provide guidelines for developing security plans	December 31, 2004	Open
2e. Document security weaknesses and corrective actions	December 31, 2004	Open
3. Enhance network security		
3a. Correct high- and medium-risk network vulnerabilities identified	December 31, 2004	85% completed
3b. Configure and patch computers securely	March 31, 2005	Open
3c. Scan networks for potential vulnerabilities and deploy an intrusion-detection system	June 30, 2005	Open

Until an agencywide information security program is established, NTSB management cannot assure the public that its computer systems are adequately secured to ensure integrity, confidentiality, and availability of its safety investigation mission.

According to the CIO, the delay in implementing these corrective actions was partially due to the inability to secure funding when competing with other operational needs. During the first quarter of FY 2005, the CIO initiated action to award a contract to help finalize the NTSB system inventory, develop security policies and procedures, and conduct security certification reviews on selected systems. However, the funding was not approved until June 2005—after the newly appointed NTSB Managing Director became aware of limited progress in this area. NTSB awarded a contract in August and the actual contract work started September 13, 2005—almost a year later than originally planned.

NTSB computers are vulnerable to unauthorized access from both inside and outside of the agency. We found weak password encryption in NTSB's routers[3] and vulnerabilities in its computers. As a result, we were able to take control over the routers and could have reconfigured them to allow unauthorized entities to access NTSB computers from the Internet. In addition, like last year, we obtained sensitive information from NTSB computers without being detected.

- **Connections to the Internet were not adequately protected.** Employees are allowed to access NTSB computer systems from the Internet. NTSB relies on its network routers to prevent unauthorized access to its internal network and direct legitimate network traffic between NTSB Headquarters and regional offices. Although its routers were reasonably configured, they did not have proper password protection, as required by Government standards. NTSB provided us with the configuration files that contained the router passwords. Even though the passwords were encrypted for security protection, we were able to easily crack all passwords. As a result, we gained total control (root-level access) over its Internet router from the Internet. As an insider, we could also gain total control of other internal routers. With root-level access to all NTSB routers, we could have changed configuration settings to open paths from the Internet to allow unauthorized entities to access NTSB's private network. Once inside the private network, the entities could obtain sensitive information from NTSB computers or launch attacks to disrupt its operations.

- **Computers hosted on the private network were vulnerable.** We used a commercial scanning software tool to perform a vulnerability assessment of computers hosted on the NTSB network. We found over 1,400 potential high-risk vulnerabilities, which could allow insiders—NTSB employees, contractors, and business associates—to gain unauthorized access to NTSB business information stored on these computers. For example, our staff was able to obtain sensitive investigative information from these computers including real-time audio recording between air traffic controllers and pilots during an accident.

  Last year, we performed a similar but more limited vulnerability check and found hundreds of high-risk vulnerabilities.[4] We recommended that, in

[3] Routers are network devices. They are used to screen network activities to prevent unauthorized access to an organization's internal networks and direct legitimate network traffic among its internal networks.

[4] Last year our network assessment performed about 400 vulnerability checks versus more than 1,200 vulnerability checks performed this year.

addition to correcting these vulnerabilities, NTSB management obtain proper tools so that it could assess network vulnerabilities regularly. NTSB has corrected about 85 percent of the high-risk vulnerabilities we identified last year and procured a software tool for vulnerability assessment. However, it did not have trained staff to utilize the tool and accordingly was not aware of these additional high-risk vulnerabilities. Conducting frequent network vulnerability assessments is critical because new vulnerabilities, such as the ones exploited by computer viruses, are uncovered daily.

- **Security incident monitoring and response capabilities are still lacking.** Like last year, our unauthorized access to NTSB computers went undetected because NTSB has not implemented an intrusion-detection system to identify potential security breaches on its network. To secure a computer network, management needs to not only patch/eliminate vulnerabilities in computers but also develop the capability to identify and respond to security incidents. This detective control is especially critical to networks with direct connections to the Internet because of relentless attacks by hackers worldwide. For example, Government agencies with intrusion-detection systems deployed on their networks have reported hundreds of potential security breaches on a daily basis.

We are making specific recommendations to enhance network security. NTSB management concurred with, and has begun implementing, recommended corrective actions. In addition, we recommend that the Acting Chairman require the Chief Information Officer to submit monthly reports to the Managing Director on progress made in finalizing a system inventory, developing security plans, and accrediting systems security.

FINDINGS

NTSB Did Not Make a Strong Commitment To Implement an Agencywide Information Security Program as Promised

In last year’s FISMA report, we made a series of recommendations to enhance NTSB’s information security program and NTSB management agreed to take corrective actions. During FY 2005, NTSB made little progress implementing our recommendations. It appointed a CIO, provided security awareness training to 82 percent of its employees and specialized training to all employees with significant security responsibility, and initiated an effort to hire a contractor to perform tasks to meet FISMA requirements. However, most of the recommended actions have not yet been implemented.

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 reviews on their information systems. However, we continue to find that these requirements have not been implemented at NTSB.

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;[5]

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

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

Until an agencywide information security program is established, NTSB management cannot assure the public that its computer systems are adequately secured to ensure integrity, confidentiality, and availability of its safety investigation mission.

This was because NTSB had not made a strong commitment as promised and did not assign a high enough priority to implement an effective information security program. During the first quarter of FY 2005, NTSB initiated an effort to award a contract, which includes finalizing NTSB's system inventory, developing security policies and procedures, and conducting security certification reviews on the selected systems. However, according to the NTSB CIO, the funding for this contract did not get NTSB management's approval until the end of June 2005. NTSB awarded this contract in August and the actual contract work did not start until September 13, 2005, almost one year later than originally planned. Without the contract, NTSB was not able to implement the key FISMA requirements.

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

NTSB Computers Were Vulnerable to Unauthorized Access from Both Inside and Outside of the Agency

We continue to identify security weaknesses in NTSB's networks, such as inadequate password protection in the Internet router, thousands of vulnerabilities in network computers and lack of intrusion-detection and monitoring capabilities. As a result, our staff was able to take control over the Internet router and obtained sensitive investigation information from NTSB computers without being detected.

➢ *Network Routers Not Properly Protected*

We reviewed configurations of 13 NTSB routers, which are used to screen network activities to prevent unauthorized access to NTSB's internal network and direct legitimate network traffic between NTSB Headquarters and regional offices. Although our review showed that the NTSB routers are reasonably configured to protect its internal network, we found that NTSB did not use strong password encryption to adequately protect its routers, which could present a potential risk to the entire NTSB network.

NTSB provided us with configuration files for the 13 routers. These files contained the encrypted passwords. However, by using basic password cracking software available on the Internet, we were able to crack within minutes the weak passwords for all 13 NTSB routers located throughout NTSB Headquarters and its field offices. In fact, using the decrypted passwords we were able to have total control (root-level access) over NTSB's Internet router from anywhere in the world. As an insider, we could also gain total control to the other 12 routers. With root-level access to all NTSB routers, we could have changed configuration settings to open paths from the Internet to allow unauthorized entities to access NTSB computers and information stored on its private network.

These vulnerabilities existed because NTSB did not comply with the Government security configuration requirements and industry best practice when applying password security in network routers. To prevent easy password cracking, the National Institute of Standards and Technology recommends Government agencies to encrypt critical passwords with a 128-bit algorithm or higher. However, passwords in NTSB's routers were encrypted with a weaker manufacturer's algorithm, which provided little security assurance and can be easily cracked with common software.

In response to our finding, NTSB management has already begun upgrading security protection in its network routers.

➢ *Network Vulnerabilities Not Assessed*

According to the NTSB progress report in March 2005, NTSB took action to eliminate 85 percent of high and medium network vulnerabilities we identified last year, acquired network scanning software, and set June 30, 2005 as its target date for having staff trained in using this software to perform network vulnerability assessments. To verify the strength of NTSB's network security, we performed a network vulnerability assessment on NTSB internal networks. Our assessment results once again demonstrated that NTSB internal networks are vulnerable to attacks.

Last year, we performed a similar but more limited vulnerability check and found hundreds of high-risk vulnerabilities. This year, we expanded the vulnerability check and found more than 28,100 potential vulnerabilities (1,400 high-risk, 1,900 medium-risk and 24,800 low-risk)[6] on NTSB network computers, some of which were also identified last year.

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, one of the most commonly known vulnerabilities is weak security over the administrator's account in a computer. Hackers always look for opportunities to use this privileged account as an entry point to gain controls over the entire computer. We found that among the 17 computers that we could take control over, 15 of them used blank passwords for the administrator account and 2 used "Administrator" as its password. Accordingly, hackers could easily gain total control (root-level access) over these computers, change computer configuration (setup), install malicious software, or add/change/delete all files stored in these computers. In fact, we did obtain sensitive investigation information from these computers, including real-time audio recording between air traffic controllers and pilots during an accident.

Despite the effort of correcting 85 percent of the vulnerabilities we identified last year, NTSB continues to have a significant amount of network vulnerabilities because NTSB:

- Does not have a procedure in place to ensure that its computers are adequately configured before being put on the networks. Six of the computers with blank password protection over the administrator's account were put on the network during FY 2005.

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

- Has not utilized the vulnerability scanning software acquired in October 2004. According to NTSB officials, this tool was not utilized due to lack of trained staff. While the training funds were available, NTSB had difficulties in allocating existing personnel resources to assume this additional responsibility. Conducting frequent network vulnerability assessments is critical because new vulnerabilities, such as the ones exploited by computer viruses, are uncovered daily.

➢ *Security Incident Monitoring and Response Capabilities Still Lacking*

Like last year, our unauthorized access to NTSB computers went undetected because NTSB has not implemented an intrusion detection system to identify potential security breaches on its network, as we recommended a year ago.

Intrusion detection is the process of detecting unauthorized use of, or attack upon, a computer or network. Intrusion-detection systems are software or hardware systems that detect such misuse. The National Institute of Standards and Technology recommends deploying such systems as necessary additions to an organization's security infrastructure. This security is particularly important to organizations with direct connections to the Internet because of constant hacking attacks. For example, Government agencies with intrusion-detection systems deployed on their networks have reported hundreds of potential security breaches on a daily basis.

Installing an intrusion-detection system is a critical step for agencies in developing a security incident monitoring and response capability. Knowing that small agencies may not have technical resources to develop this capability, the Office of Management and Budget (OMB) has initiated an effort for qualified entities (Centers of Excellence) to provide cross-agency services in this area. The General Services Administration is taking the lead to implement this effort, called the Information Security Services Line of Business. NTSB should consider using this service as soon as possible.

As we demonstrated, NTSB computer networks remain vulnerable. Also, the lack of progress in implementing an agencywide information security program continues to put 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 FMFIA report to OMB and Congress.

RECOMMENDATIONS

We recommend that the NTSB Acting Chairman:

1. Ensure that NTSB's information security program receives the priority and funding to accomplish the following in FY 2006:

    a) Finalizing the system inventory and completing risk assessment for all systems in accordance with Federal Information Processing Standards 199.

    b) For high-risk systems, completing security certification and accreditation reviews and documenting planned actions and milestones for remediation.

    c) For the remaining medium- and low-risk systems, establishing a timetable to complete security certification and accreditation reviews.

2. Require the Chief Information Officer to submit monthly reports to the Managing Director describing progress made in implementing the following critical elements of an agencywide information security program.

    a) Finalizing the system inventory.

    b) Issuing guidance for system owners to develop security plans.

    c) Assisting senior management in accrediting systems security.

    d) Implementing a mechanism to track and prioritize security weakness correction efforts, as required by OMB.

    e) Ensuring all employees receive security awareness training annually.

3. Direct the Chief Information Officer to take immediate actions to enhance network security by:

    a) Enhancing security protection of passwords on network routers, such as using stronger password encryption.

    b) Developing procedures to ensure computers are properly configured before being implemented for production use.

    c) Providing proper training and performing vulnerability assessments of all network computers with the acquired scanning tool on a regular basis.

    d) Establishing network security incidents monitoring and response capabilities.

MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

A draft of this report was provided to the NTSB Acting Chairman for comments on September 23, 2005. The Acting Chairman responded on October 7, 2005, and concurred with all recommendations (see Appendix). The actions planned by NTSB are reasonable and should provide a solid foundation for implementing an effective information security program. We will continue monitoring NTSB's progress in implementing these recommendations.

NTSB's response also included comments regarding our characterization of the vulnerability of its Internet connections. We acknowledge that NTSB may have other protections built into its overall network infrastructure—protections that make system intrusion by the general public unlikely. However, as noted in the report, we base our conclusion about NTSB's systems' vulnerability on the cumulative risk inherent in the systems' present architecture. By gaining root-level access to 13 NTSB routers, we could have changed configuration settings to open paths from the Internet to allow unauthorized entities to access NTSB computers and information stored on its private network. Despite the presence of a firewall between the routers, the ability to reconfigure these routers to allow unauthorized network traffic through the firewall may not be difficult when attempted by those with sophisticated knowledge of computers.

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 at (202) 366-1992 or Rebecca C. Leng, Assistant Inspector General for Information Technology and Computer Security, at (202) 366-1488.

Sincerely,

Theodore P. Alves
Principal Assistant Inspector General for
Auditing and Evaluation

Enclosures (3)

ENCLOSURE 1. OFFICE OF INSPECTOR GENERAL INPUT TO FISMA REPORT

This is the second year that NTSB has been required to comply with FISMA, which requires independent evaluation of agencies' information security programs. NTSB is responsible for investigating accidents in all transportation modes to determine their cause, and for recommending changes to improve safety and reduce the likelihood and consequences of future accidents.

Responding to FISMA requirements, the Department of Transportation's Office of Inspector General (OIG) performed an audit of NTSB's information security program last year for the first time. We reported to NTSB that its information security program should be reported to OMB as a material weakness under the FMFIA and recommended immediate corrective action. NTSB management agreed to take aggressive action, including appointing a Chief Information Officer to lead the effort. While a Chief Information Officer was appointed last September, NTSB is behind in implementing the planned actions to enhance its information security program. Since only limited progress has been made, we performed a limited review focusing on NTSB network security.

Our independent evaluation continues to identify significant security weaknesses in NTSB's networks, such as inadequate password protection in the Internet router, thousands of vulnerabilities in network computers, and lack of intrusion-detection capabilities. These security weaknesses enabled us to gain unauthorized access to sensitive information, including real-time audio recording between air traffic controllers and pilots during an accident.

The lack of progress in implementing an agencywide information security program continues to put 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 FMFIA report to OMB and the Congress. We are making specific recommendations to enhance network security. NTSB management concurred with, and has begun implementing, recommended corrective actions. Until an agencywide information security program is established, NTSB management cannot assure the public that its computer systems are adequately secured to ensure the integrity, confidentiality, and availability of its safety investigation mission.

Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name: National Transportation Sefety Board

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation , a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						**Question 2**					
		a. FY 05 Agency Systems		**b. FY 05 Contractor Systems**		**c. FY 05 Total Number of Systems**		**a. Number of systems certified and accredited**		**b. Number of systems for which security controls have been tested and evaluated in the last year**		**c. Number of systems for which contingency plans have been tested in accordance with policy and guidance**	
Bureau Name	**FIPS 199 Risk Impact Level**	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
NTSB	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized			1	0	1	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Agency Totals	**High**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	#DIV/0!	**0**	#DIV/0!	**0**	#DIV/0!
	Moderate	**0**	**0**	**0**	**0**	**0**	**0**	**0**	#DIV/0!	**0**	#DIV/0!	**0**	#DIV/0!
	Low	**0**	**0**	**0**	**0**	**0**	**0**	**0**	#DIV/0!	**0**	#DIV/0!	**0**	#DIV/0!
	Not Categorized	**0**	**0**	**1**	**0**	**1**	**0**	**0**	#DIV/0!	**0**	#DIV/0!	**0**	#DIV/0!
	Total	**0**	**0**	**1**	**0**	**1**	**0**	**0**	#DIV/0!	**0**	#DIV/0!	**0**	#DIV/0!

Question 3

In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.

3.a.	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. Response Categories: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time	- Rarely, for example, approximately 0-50% of the time"

3.b.	The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. Response Categories: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 0-50% complete
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	no
3.d.	The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	no
3.e.	The agency inventory is maintained and updated at least annually.	no
3.f.	The agency has completed system e-authentication risk assessments.	no
Question 4		
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. 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 area provided below. For items 4a.-4.f, the response categories are as follows: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time		
4.a.	The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	- Rarely, for example, approximately 0-50% of the time"
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	- Rarely, for example, approximately 0-50% of the time"
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Rarely, for example, approximately 0-50% of the time"
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Rarely, for example, approximately 0-50% of the time"
4.e.	OIG findings are incorporated into the POA&M process.	- Rarely, for example, approximately 0-50% of the time"
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	- Rarely, for example, approximately 0-50% of the time"
Comments: NTSB did not meet key FISMA requirements during FY 2005, such as having a complete system inventory, performing certification and accreditation (C&A) on the identified systems, reporting security weakness and corrective action plan (POA&M) to OMB, and developing security plan and related policies. NTSB hired a contractor in September 2005 to start implementing key FISMA requirements.		
Question 5		
OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199 (February, 2004), "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 .		
	Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Failing
Comments: NTSB has not performed security certification reviews on any of its information systems. NTSB hired a contractor to finalize its system inventory and will perform C&A reviews on selected systems.		

Section B: Inspector General. Question 6, 7, 8, and 9.

Agency Name:

Question 6

6.a.	Is there an agency wide security configuration policy? Yes or No.	No
	Comments: NTSB currently does not have an agency wide security configuration policy. However, a desktop configuration standard (Windows XP) is under development. The configuration guides for other software products will be established by the NTSB contractor.	
6.b.	Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.	

Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	No	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows NT	No	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows 2000 Professional	No	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows 2000 Server	No	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows 2003 Server	No	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Solaris	No	No	
HP-UX	No	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Linux	No	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Cisco Router IOS	No	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Oracle	No	No	
Other. Specify:			

Comments: OIG network assessment identified many security weaknesses. However, NTSB hired a contractor to establish configuration management standards.

Question 7

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	No
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	No
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	No

Comments: NTSB has no incident reporting policies and procedures internally or externally. However, NTSB hired a contractor to develop policies and procedures on incident response.

Question 8

8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or approximately 81-95% of employees have sufficient training

Question 9

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

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 the key network administration and management officials in the Office of Research and Engineering to gather information on implementation status of NTSB's information security program. Based on the collected information, we provided answers to OMB's questions on FISMA reporting. By using commercial scanning software, we performed a limited vulnerability assessment of NTSB private networks, dial-up connections and configuration of NTSB routers. Due to time constraints, we performed limited penetration tests by exploiting some of the identified vulnerabilities.

We performed our work between July and September 2005 at NTSB Headquarters in Washington, DC. The performance audit was conducted in accordance with the Generally Accepted 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

Name	Title
Rebecca C. Leng	Assistant Inspector General for Information Technology and Computer Security
Edward Densmore	Program Director
Dr. Ping Z. Sun	Project Manager
John M. Johnson	Senior IT Specialist
Aaron Nguyen	Computer Scientist
Michael P. Fruitman	Communications Adviser

APPENDIX. MANAGEMENT COMMENTS

National Transportation Safety Board

Washington, D.C. 20594

October 7, 2005

Office of the Chairman

Mr. Theodore P. Alves
Principal Assistant Inspector General for
  Auditing and Evaluation
U.S. Department of Transportation
400 7th Street, SW
Washington, DC 20590

Dear Mr. Alves:

Thank you for the opportunity to provide comments on the draft report of your follow-up review of the National Transportation Safety Board's information security program and network security. We do not dispute the observation that the development of the NTSB's information security program has not progressed as rapidly as we had hoped. We have, however, devoted considerable resources to this process and are committed to its completion.

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 have reflected that conclusion in our report to Office of Management and Budget and to Congress under the Federal Manager's Financial Integrity Act (FMFIA) of 1982.

If you have any questions, please contact Mr. Joseph Osterman, Managing Director, at (202) 314-6060.

Sincerely,

Mark V. Rosenker
Acting Chairman

Enclosure

ENCLOSURE

DOT IG RECOMMENDATIONS:

Recommendation 1: Ensure that NTSB's information security program receives the priority and funding to accomplish the following in FY 2006:

a) ***Finalizing the system inventory and completing risk assessment for all systems in accordance with Federal Information Processing Standards 199.***
   Response: Concur. The system inventory and FIPS 199 risk assessment for all systems will be completed on 10-31-05.

b) ***For high-risk systems, completing security certification and accreditation reviews and documenting planned actions and milestones for remediation.***
   Response: Concur. If the 10-31-05 final assessment identifies any high-risk systems, defined as systems which the loss of confidentiality, integrity, or availability of the system could be expected to have a severe or catastrophic effect on organizational operations, organizational assets, or individuals, the NTSB will complete a plan with milestones for remediation for any high-risk system by November 30, 2005.

c) ***For the remaining medium- and low-risk systems, establishing a timetable to complete security certification and accreditation reviews.***
   Response: Concur. A plan of action with milestones for the accomplishment of certification and accreditation for all remaining systems and major applications will be completed by January 9, 2006.

Recommendation 2: Require the Chief Information Officer to submit monthly reports to the Managing Director describing progress made in implementing the following critical elements of an agency wide information security program.

a) ***Finalizing the system inventory,***
b) ***Issuing guidance for system owners to develop security plans,***
c) ***Assisting senior management in accrediting systems security,***
d) ***Implementing a mechanism to track and prioritize security weakness correction efforts, as required by OMB;***
e) ***Ensuring all employees receive security awareness training annually.***

Response: Concur. The CIO will report daily to the Managing Director on progress until October 31, 2005, and then monthly thereafter.

i. The system inventory will be completed by October 31, 2005.
ii. Security plan guidance will be completed by January 9, 2006.

iii. A plan to accredit systems security will be completed by September 30, 2006.

iv. A mechanism to track and prioritize security weakness correction efforts will be deployed by May 31, 2006.

v. All employees will complete training for calendar year 2005 by October 31, 2005. The NTSB training officer will prepare a plan to ensure that all employees receive security awareness training annually, by December 31, 2005.

Recommendation 3: Direct the Chief Information Officer to take immediate actions to enhance network security by:

a) ***Enhancing security protection of passwords on network routers, such as using stronger password encryption;***
Response: Concur.

Following the IG's audit, the NTSB configured the Internet router with vendor provided strong encryption per NIST guidance (Router Security Configuration Guide v1.1b, 12-05-2003).

The NTSB will take the following actions as established by NIST guidelines and standards by October 20, 2005:

- Shutdown all unneeded services
- Apply additional access filters to restrict remote access and attacks
- Limit remote management to internal, encrypted sessions only
- Implement router logging capability

b) ***Developing procedures to ensure computers are properly configured before being implemented for production use;***
Response: Concur. An interim procedure will be completed by October 20, 2005 and a final procedure by December 5, 2005.

c) ***Providing proper training and performing vulnerability assessments of all network computers with the acquired scanning tool on a regular basis;***
Response: Concur. The Chief Information Security Officer and his backup will receive scanning tool training or if appropriate training is unavailable, a contractor will provide scanning services by December 24, 2005. A plan for periodic vulnerability scanning will be completed by October 13, 2005.

d) ***Establishing network security incidents monitoring and response capabilities.***
Response: Concur. The NTSB will complete a plan and policy for network security monitoring and response capabilities, including an assessment of alternative reporting, by December 5, 2005.

DOT IG RECOMMENDATIONS:

SCHEDULE

October 1, 2005: Following the IG’s audit, the NTSB configured the Internet router with vendor provided strong encryption per NIST guidance (Router Security Configuration Guide v1.1b, 12-05-2003).

October 7, 2005: The CIO will report daily to the Managing Director on progress until October 31, 2005, and then monthly thereafter.

October 20, 2005: The NTSB will take the following actions as established by NIST guidelines and standards:

1. Shutdown all unneeded services
2. Apply additional access filters to restrict remote access and attacks
3. Limit remote management to internal, encrypted sessions only
4. Implement router logging capability

October 31, 2005: The system inventory and FIPS 199 risk assessment for all systems will be completed.

October 31, 2005: The system inventory will be completed.

October 31, 2005: All employees will complete training for calendar year 2005.

October 31, 2005: A plan for periodic vulnerability scanning will be completed.

November 30, 2005: If the 10-31-05 final assessment identifies any high-risk systems, defined as systems which the loss of confidentiality, integrity, or availability of the system could be expected to have a severe or catastrophic effect on organizational operations, organizational assets, or individuals, the NTSB will complete a plan with milestones for remediation for any high-risk system.

December 5, 2005: An interim procedure will be completed.

December 5, 2005: The NTSB will complete a plan and policy for network security monitoring and response capabilities, including an assessment of alternative reporting.

December 24, 2005: The Chief Information Security Officer and his backup will receive scanning tool training or if appropriate training is unavailable, a contractor will provide scanning services.

December 31, 2005: The NTSB training officer will prepare a plan to ensure that all employees receive security awareness training annually.

January 9, 2006: A plan of action with milestones for the accomplishment of certification and accreditation for all remaining systems and major applications will be completed.

January 9, 2006: Security plan guidance will be completed.

May 31, 2006: A mechanism to track and prioritize security weakness correction efforts will be deployed.

September 30, 2006: A plan to accredit systems security will be completed.