INFORMATION SECURITY PROGRAM

National Transportation Safety Board

Report Number: FI-2007-001
Date Issued: October 13, 2006

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

Office of Inspector General
Washington, D.C. 20590

October 13, 2006

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

Dear Chairman Rosenker:

This report presents the results of our audit of the National Transportation Safety Board's (NTSB) information security program, required by the Federal Information Security Management Act (FISMA) of 2002. We have also included our FISMA evaluation submission to the Office of Management and Budget (OMB) in Enclosure 1.

In fiscal year (FY) 2006, NTSB made a concerted effort to correct security weaknesses identified in prior years, including establishing a new Chief Information Officer office, developing a system inventory and a timetable to complete system security certification reviews, implementing password lockouts on computers, and providing information security awareness training to NTSB employees. In addition, NTSB should be commended for having established capabilities to perform network vulnerability scans and monitor networks for possible intrusions.

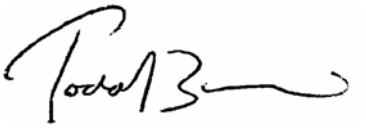
However, continued management attention is needed in several areas: (1) assessing systems risk and assigning a priority to reviewing and testing security protection of systems with a higher-risk impact on NTSB operations, (2) enforcing and following through on the newly established network security requirements, and (3) identifying systems containing sensitive personally identifiable information for proper protection. As a result, NTSB's information security program in our opinion still has a significant deficiency that should be reported as a material internal control weakness on the annual Federal Managers' Financial Integrity Act (FMFIA) report to OMB and Congress.

We are making a series of recommendations starting on page 11 to help NTSB strengthen its information security program. On September 28, 2006, NTSB

provided us with its response to a draft of this report. Although NTSB did not specify whether it concurs with each recommendation, NTSB appears to have some disagreements. We have included NTSB's response in its entirety in Enclosure 4. We added our analysis of the response to each report section as appropriate.

We appreciate the courtesies and cooperation of NTSB representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-6767; David Dobbs, Acting Principal Assistant Inspector General for Auditing and Evaluation, at (202) 366-0500; or Rebecca C. Leng, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1496.

Sincerely,



Todd J. Zinser
Acting Inspector General

Enclosures (4)

INTRODUCTION

To support its investigative operations nationwide, NTSB has implemented an information technology (IT) infrastructure that includes communications networks, computer laboratories, and software application systems at its Headquarters, 10 regional offices, and Academy. This 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 public.

This is the third year that independent agencies such as NTSB have been required to report to the Congress on their information security programs.[1] The Department of Transportation's Office of Inspector General (OIG) performed audits of NTSB's information security program for FY 2004 and FY 2005.[2] Last year, we found that NTSB had made limited progress in enhancing its information security program, and many network vulnerabilities exposed NTSB computers to unauthorized access from both inside and outside the Agency. As a result, we suggested to NTSB that its information security program should be reported to OMB and Congress as a material weakness under the Federal Managers' Financial Integrity Act of 1982 and recommended corrective actions, which NTSB management agreed to do.

In FY 2006, NTSB continued to correct information security weaknesses; however, it experienced leadership turnovers in the Chief Information Officer (CIO) office. As a result, the NTSB Deputy Managing Director assumed the role of the Acting CIO in May 2006 and provided critical leadership during this transition period. Our objectives for this year's review were to evaluate (1) whether system risks were properly assessed and security weaknesses were reported for correction, (2) the effectiveness of enhanced network security operations, and (3) the progress made by NTSB in protecting sensitive agency information.

We conducted this 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 contribution to NTSB's annual FISMA report to OMB appears as Enclosure 1. Our scope and methodology are described in more detail in Enclosure 2.

---

[1] FISMA requires the 24 large Federal agencies to report annually to the Congress on their information security programs. Two years ago the Office of Management and Budget (OMB) expanded FISMA reporting requirements to all departments and agencies subject to the Paperwork Reduction Act of 1995, including NTSB.

[2] OIG Report Number FI-2006-001, "NTSB Information Security Program," October 7, 2005, and OIG Report Number FI-2004-097, "NTSB Information Security Program," September 28, 2004. OIG reports can be found at www.oig.dot.gov.

RESULTS

System Impact Assessments Need To Be More Thorough To Protect Against Disruption

NTSB's information security has improved from last year, but its data and information systems remain at risk. NTSB did not differentiate its systems by risk level. The key reason for this is that NTSB did not fully implement policies that included all requirements of the National Institute of Standards and Technology (NIST). As a result, NTSB has not prioritized the certification and accreditation (C&A)[3] reviews of its information systems.

Impact Levels of NTSB Systems Need More Review

As part of FISMA, agencies are required to use Federal Information Processing Standards (FIPS) Publication 199 ("Standards for Security Categorization of Federal Information and Information Systems," February 2004) to categorize the risk impact levels of each of their information systems. FIPS 199 establishes three potential levels of impact (low, moderate, and high) relevant to securing Federal information and information systems to adequately ensure the confidentiality, integrity, and availability of the data. FIPS 199 and 200[4] stress the importance of (1) prioritizing levels of risk and (2) meeting minimum security requirements commensurate with the risk level.

Last year we recommended that NTSB assign a high priority to completing the C&A reviews of its high-risk (most critical) systems. NTSB hired a contractor to assist it in the risk assessment and has since concluded that it has no high-risk systems. All six NTSB systems[5] are deemed to have a moderate level of risk for all three security components—confidentiality, integrity, and availability.

However, NTSB only assessed the risk impact level for three systems—General Support, Accident Investigation, and Financial Management. It did not perform specific risk assessment on the other three systems (Telephone, Physical Security, and Laboratory Environment). NTSB decided that the three systems not assessed would also merit a moderate risk rating because they used to be sub-components of the three assessed systems.

---

[3] According to NIST Special Publication 800–37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004), certification is the comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implanted correctly. Accreditation is the official management decision given by a senior agency official to authorize operations of an information system and to explicitly accept the risk to agency operations.

[4] FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006.

[5] The six systems are the General Support System, Telephone System, Physical Security System, Laboratory Environment System, Accident Investigation System, and Financial Management System.

We are concerned that under this assessment scheme, all systems will receive the same level of security protection, even though some are clearly more sensitive than others. For example, the Laboratory Environment System, used to analyze aircraft black-box recordings, should receive a higher level of risk assessment and security protection than other systems, such as the Telephone Switch System. NTSB's laboratory environment contains highly sensitive audio recordings that, by law, are not to be disclosed to the general public. Further, justification for the moderate-level categorizations in NTSB's risk assessments was lacking. For example, NTSB did not use vulnerability and threat information to support the security categorizations that it identified for each system, as FIPS 199 requires.

In addition, NTSB's interpretation of NIST guidance for high-risk impact systems needs to be reevaluated. According to FIPS 199, the impact on an organization should be categorized high if "the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals."

NTSB management informed us that unlike air traffic control systems, none of its systems could result in loss of human lives and so are not high-risk impact systems. We confirmed with NIST that systems with a severe impact on the Agency's mission capability and organizational assets, including but not limited to loss of human lives, should be categorized as high-risk impact systems for security planning and testing.

NTSB's response to our draft report indicated that it disagreed that vulnerability and threat information were not incorporated into its security categorizations. Our analysis of NTSB's three risk assessments did not find any vulnerability and threat data. According to NIST 800-37, the methods used to assess risk include considering vulnerabilities and threats in the information system. These vulnerabilities are identified by evaluating the effectiveness of current or proposed security controls applied to a system. Vulnerabilities resulting from the absence of these controls provide the basis for determining the agency-level risk posed by the systems operation. This provides a starting point for NTSB's overall risk management process.

The risk assessments also did not show the overall level of risk for each control by applying the NIST-recommended formula to define risk: RISK = Likelihood x Magnitude of Impact. The assessment lacked the following information: likelihood of occurrence, threat-source identification, and risk level matrix to conclude their systems impact level. This analysis is needed for agency officials to properly assess risk and categorize their systems in accordance with FIPS 199, which states that security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

Unless NTSB performs more thorough risk assessments, it may be underestimating the impact these systems could have on its operations and mission if they were to be compromised. Further, it cannot be assured that NTSB has implemented the most appropriate set of controls to reduce risk to an acceptable level.

Planned Systems Security Reviews Need To Be Better Prioritized

OMB requires Federal agencies to establish a certification and accreditation process for formally authorizing systems to operate. Security certification and accreditation provides Agency officials with the necessary information to understand the risks and other factors pertaining to their systems that could adversely affect mission goals.

Last year, we recommended that NTSB establish a timetable to complete security certification and accreditation reviews for all of its systems. While NTSB has established such a timetable, the majority of the systems security (certification and accreditation) reviews are scheduled to be completed in early FY 2008 (see Table 1). Accordingly, NTSB will not have any system certification and accreditation reviews completed in time for next year's FISMA review, and its systems could remain vulnerable for another year. NTSB should accelerate its certification and accreditation review process based on the result of reassessing its systems' impact levels.

Table 1. NTSB Certification and Accreditation Target Completion Dates

NTSB System	Certification and Accreditation Target Completion Dates
General Support System	9/30/2007
Telephone System	10/31/2007
Physical Security System	10/31/2007
Laboratory Environment System	12/31/2007
Accident Investigation System	12/31/2007
Financial Management System	Completed 7/2004 (by the service provider)[a]

[a] This system is operated under contract by the Department of the Interior, which owns it; however, NTSB retains ownership of the data it contains.

Further, in the timetable NTSB provided, the process for completing the C&A review for the General Support System was broken down into its individual steps, such as conducting a risk assessment, creating a security plan, and conducting contingency planning. For the remaining systems, however, projected completion

dates for each of these three component steps were not recorded in the plan of action and milestones (POA&M). Establishing more specific milestone dates would help ensure that all required steps are identified and accomplished for prompt completion of its certification and accreditation reviews.

NTSB's Network Security Has Been Enhanced, but More Is Needed

During FY 2006, NTSB improved its network security operations by implementing stronger encryption protection for passwords on its network routers, deploying an Agencywide computer lockout policy, and issuing a series of internal operations bulletins. In addition, NTSB should be commended for successfully developing network vulnerability scanning and intrusion-detection capabilities. However, NTSB has much to do to further improve its network security protection.

Password Security Requirements Need To Be Enforced

On June 30, 2006, NTSB issued specific operations bulletins to address the FISMA requirement for minimally acceptable system configuration settings, including password security settings for more than 400 network users logging onto the NTSB network. However, we found that the actual configuration of NTSB network computers—specifically, password settings—did not comply with NTSB's security requirements.

For example, the NTSB policy required users to have a minimum password length of eight characters with a mixture of letters, numbers, and special symbols. While the minimum password length was configured as eight characters, the requirement for using a mixture of letters, numbers, and special symbols was not enforced. As a result, users could set their passwords as "12345678" or "abcdefgh," which could be easily guessed or cracked by hackers to gain unauthorized access to NTSB information systems.

Responding to a draft of the report, NTSB's Acting CIO stated that "NTSB Operations Bulletin … *recommends* … complex passwords.… Our written policy does not require complex passwords; however, our security policies *do* enforce strong password requirements…" On the basis of this enforcement, the Acting CIO asked that we delete this issue from our draft report.

However, as of August 23, 2006, the network configuration setting for "Password must meet complexity requirements" was *disabled.* Clearly, then, password complexity requirements are not being enforced. Enforcing this basic password

security practice is included in NIST guidance[6] and is commonly practiced in the Federal Government and in industry. We recommend, therefore, that NTSB make the use of complex passwords a clear requirement, and that NTSB enable its password complexity setting (i.e., passwords not meeting the complexity standard would be rejected).

NTSB Has Not Completed Work Necessary To Correct Previously Identified Vulnerabilities

During FY 2006, NTSB established auditing, monitoring, and reporting policies, which include periodic vulnerability assessments of its IT infrastructure and mitigation of identified weaknesses. In addition, Agency officials were trained in using vulnerability scanning software and started periodically assessing their network in December 2005. However, critical vulnerabilities were not adequately and promptly remediated.

For example, NTSB's scanning results from May 2006 identified a total of 17,006 vulnerabilities (827 high, 549 medium, and 15,630 low).[7] Our review of NTSB's scanning results found some of the same vulnerabilities that we identified a year ago.

- Eleven of the high vulnerabilities were password-related, four of which were found on the same computers that we had identified during our FY 2005 FISMA review.[8] These vulnerabilities could result in unauthorized access to or modification of business information stored in NTSB computers.

- Seventeen of the high vulnerabilities are related to buffer overflow,[9] 11 of which were found on the same computers that we had identified during last year's FISMA review. This type of vulnerability could allow remote attackers to take full control of the computer, who could then modify data files or capture all of a user's activities displayed on the screen.

OMB requires agencies to develop a POA&M to track, assess, and prioritize corrective actions taken to address security weaknesses identified. None of the network weaknesses identified during NTSB's network scanning were recorded in

---

[6] NIST SP 800-68: Passwords Must Meet Complexity Requirements. This setting makes it more difficult to guess or crack passwords. Enabling this setting implements complexity requirements including not having the user account name in the password and using a mixture of character types, including upper case and lower case letters, digits, and special characters such as punctuation marks.

[7] 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, that they can then use to compromise a computer system.

[8] OIG Report Number FI-2006-001, "NTSB Information Security Program," October 7, 2005.

[9] Buffer overflow happens when more data are put into a buffer or memory holding area than it can handle; this can result in a system crash or the overwriting of the data into the adjacent buffers and the hijacking of control of the program.

the POA&M. As a result, NTSB management may not be effectively assigning resources toward mitigating the critical vulnerabilities identified.

While NTSB's response stated that aggressive actions had taken place in addressing previously identified vulnerabilities, no documentary evidence was provided to support this assertion. As stated above, our review of NTSB's scanning results from May 2006 showed some of these same vulnerabilities on the same computers that we reported on last year. NTSB also claimed that many of the vulnerabilities were false-positives associated with network printers or similar equipment. However, we confirmed in our FY 2005 FISMA review that not all of the vulnerabilities cited were false-positives.

We agree with NTSB that vulnerabilities, such as buffer overflow, could be addressed using an automated patch management system like the one deployed by NTSB. However, a patch to correct the buffer overflow vulnerability referenced above has been available from the vendor for over 2 years.

NTSB Has Established Intrusion-Detection Capabilities but Must Follow Up and Investigate Potential Cyber Security Incidents

Responding to last year's OIG recommendations, NTSB developed policies and procedures that established the Agency's cyber security incident monitoring and response capabilities. These policies and procedures provided basic criteria for incident classification, timelines for internal and external reporting to United States Computer Emergency Readiness Team (US-CERT), and responsibilities of appropriate officials.

Further, in February 2006, NTSB reported having successfully implemented its intrusion-detection system (IDS) for monitoring and detecting potential cyber security incidents. However, security events recorded by IDS were not adequately investigated. Our review of NTSB's IDS log of activity between March and August 2006 uncovered signs of potential hacking activities taking place in April and July. These activities originated from two separate foreign countries and attempted to compromise the main NTSB web site. Yet NTSB management was not aware of these events and did not investigate them or report them to US–CERT. According to NTSB policy, these suspicious and unusual activities should have been investigated. Overall, NTSB did not provide sufficient evidence to show that the IDS log was properly reviewed or that potential incidents were investigated. Without implementing proper procedures to review and investigate its IDS event log, NTSB has no assurance that security incidents will be identified and preventive action against cyber attacks taken.

NTSB responded that it had provided evidence to support that IDS logs were periodically reviewed. However, the evidence does not support this assertion. NTSB showed us a printout of the computer screen, containing the names and size-and-date data of five log files. This does not demonstrate that the files themselves were actually reviewed.

NTSB's current IDS also has certain limitations, such as not being comprehensive enough to detect intrusions from inside the organization. One option for NTSB to consider is to acquire the IDS service from a "Center of Excellence"[10] when it becomes available in FY 2008.

NTSB Must Establish Policies and Procedures for Privacy Protection

While NTSB has developed policies to protect portable computers and data from loss and virus infections and a process to report such losses to both agency management and to US-CERT, much work remains to meet the requirements of NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems" (February 2005).

For example, NTSB's docket system (part of the Accident Investigation System) contains investigators' information on aircraft accidents and may contain sensitive personal information on aircraft victims, mechanics who worked on the aircraft and approved its airworthiness, or the medical condition of the pilots at the time of the accident. To adequately secure these data and meet the requirements of the E-Government Act of 2002, NTSB needs to develop a detailed privacy policy and procedures. This policy should enable the Agency to perform a methodical assessment to identify systems processing or storing sensitive personal identifiable information; incorporate privacy analysis into the C&A process; determine if these systems require completion of a Privacy Impact Analysis to meet the requirements of the E-Government Act of 2002; and implement sufficient controls—such as encryption—to prevent loss, misuse, or unauthorized access to these data. Such unauthorized access and misuse may put NTSB at risk of compromising people's privacy.

In view of the security weaknesses that still require correction, NTSB's information security program will need the continued support and attention of its senior management. Until NTSB corrects these problems, it will not have assurance that the level of protection being provided to its Agency assets is adequate. In FY 2007, it will be critical for NTSB to make significant progress in

[10] OMB is currently asking agencies to submit proposals to either become a service provider (Center of Excellence) for other agencies or migrate to another agency, from which they would acquire expert security services. Incident-response capabilities are part of this initiative, scheduled to be available in FY 2008. According to NIST, monitoring threats through IDS is an essential part of incident response; therefore, we assume that service providers for incident-response monitoring would include an IDS service. In our opinion, NTSB should become a client of one of these other agencies, when these services become available, to enhance its IDS capability.

these areas to move forward in implementing an effective information security program. As a result of this year's assessment, we are making a series of recommendations to help NTSB strengthen its information security program.

RECOMMENDATIONS

To strengthen NTSB's information security program**,** we recommend that the National Transportation Safety Board:

1. Improve the quality of the certification and accreditation process by:

   (a) ensuring that NTSB reassess risk levels for each of its systems by December 31, 2006, and

   (b) prioritizing certification and accreditation reviews to ensure that all systems deemed to have a high risk of impact on NTSB operations are certified and accredited by June 30, 2007.

2. Improve NTSB's network security by:

   (a) updating its password policies to enforce the use of a mixture of letters, numbers, and special symbols to construct user passwords to prevent easy guessing or cracking;

   (b) configuring network password settings, in accordance with NTSB security policies, by October 31, 2006;

   (c) categorizing and incorporating identified vulnerabilities into Agency POA&Ms by December 31, 2006;

   (d) taking immediate action to correct highly critical vulnerabilities by December 31, 2006;

   (e) establishing (in the short term) procedures to periodically review and analyze its IDS event log and report computer security incidents to proper authorities in a timely manner; and

   (f) acquiring (in the long term) the intrusion-detection monitoring service from a center of excellence when such services become available in FY 2008.

3. Take immediate action to protect systems containing sensitive personal identifiable information from unauthorized access and loss by:

(a) developing a privacy policy, including methodologies and criteria for identifying systems that contain personally identifiable information;

(b) incorporating proper security requirements and testing as part of the certification and accreditation process, along with performing a privacy impact assessment for these systems; and

(c) implementing controls, including security software, for encryption protection of personally identifiable information on laptop computers as soon as possible.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL ANALYSIS

A draft of this report was provided to NTSB for comments on September 27, 2006. The Deputy Managing Director and Acting CIO responded on September 28, 2006. The response did not specify whether NTSB concurred with our recommendations. We include the response in its entirety in this report (see Enclosure 4).

The response focused on describing NTSB's current processes relating to assessing systems risk, enforcing password security, remediating vulnerabilities, and reviewing intrusion-detection logs. We reviewed these processes during our audit and identified deficiencies, as described in our report. NTSB's response did not add any new information for us to evaluate.

Overall, the response indicated that NTSB is satisfied that its actions to strengthen security are adequate. However, this is the third year we have reviewed NTSB's information security program, and although NTSB continues to make progress, its information security program continues to have significant deficiencies. For example, NTSB has gone 3 years without completing any system certification and accreditation review, and is not planning to complete any before September 30, 2007. In its response, NTSB also suggested that we remove a critical finding from our report concerning not using a mixture of alpha, numeric, and special characters to construct passwords. Enforcing this basic password security practice is included in NIST guidance and is commonly practiced in the Federal Government and in industry. In our view, this response illustrates that NTSB is still not taking aggressive action to implement an effective information security program.

ACTION REQUIRED

We are requesting that you provide a written clarification of your response to our recommended actions within 30 days of this report's issuance. If you concur with

our recommendations, please indicate the specific action taken or planned for each recommendation and the target date for completion. If you do not concur, please provide your rationale. You may provide alternative courses of action that you believe would resolve the issues presented in this report.

OFFICE OF INSPECTOR GENERAL CONTRIBUTION TO FISMA REPORT

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

Agency Name:

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 over the past fiscal year 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. Agency Systems		b. Contractor Systems		c. 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
National Transportation Safety	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
Board	Moderate	5	0	1	0	6	0	1	#DIV/0!	0	#DIV/0!	0	#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**5**	**0**	**1**	**0**	**6**	**0**	**1**	**16.7%**	**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	**5**	**0**	**1**	**0**	**6**	**0**	**1**	#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**	**0**	**0**	**0**	**0**	**0**	#DIV/0!	**0**	#DIV/0!	**0**	#DIV/0!
	Total	**5**	**0**	**1**	**0**	**6**	**0**	**1**	#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 and/or NIST 800-53 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	- Almost Always, for example, approximately 96-100% of the time
3.b.1.	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 96-100% complete
3.b.2.	If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.	Missing Agency Systems: Missing Contractor Systems:
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
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.	Yes
3.e.	The agency inventory is maintained and updated at least annually.	Yes
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.	- Frequently, for example, approximately 71-80% 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).	- Frequently, for example, approximately 71-80% of the time
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Almost Always, for example, approximately 96-100% of the time
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-100% 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	- Sometimes, for example, approximately 51-70% of the time
Comments: NTSB's POA&M process did not contain all of our recommendations made last year nor NTSB's scanning results		

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	- Poor
Comments: NTSB has improved its information security program by establishing a systems inventory, establishing an interim POA&M process, and performing risk assessments on three systems. However, NTSB has not completed any certification and accreditation reviews for its 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.	Yes
	Comments: Although NTSB's security configuration standards are incorporated within several NTSB operation bulletins including the IT security, identification and authentication, and access control policies, these bulletins did not explicitly address the individual products listed in 6.b.	

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	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows NT	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2003 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Solaris	N/A	No	
HP-UX	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Linux	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Cisco Router IOS	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Oracle	N/A	No	
Other. Specify: SQL Server	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software

Comments: According to NTSB officials, the Agency has 10 legacy systems running on Unix and Linux that are in the process of being phased out due to recent migration to Windows environment. Some of these computer systems, located at the NTSB laboratory, are used to analyze information from voice and data recorders as part of accident investigations.

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.	Yes
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.	Yes

Comments: During the FY 2006, NTSB reported 1 incident of a stolen laptop that potentially contained Personally Identifiable Information. However, there was no evidence that other potential security events recorded by the Agency intrusion-detection-system were properly investigated.

	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	- Almost Always, or approximately 96-100% 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

SCOPE AND METHODOLOGY

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

We assessed NTSB's progress in correcting weaknesses identified in last year's FISMA review and interviewed key management officials in the Office of the CIO to gather information on the implementation status of NTSB's information security program. We also reviewed key documentation related to NTSB's information security program, such as systems inventory, risk assessments, plans of action and milestones, network scanning results, and policies and procedures relating to personally identifiable information. Based on the collected information, we provided answers to OMB's questions on FISMA reporting.

We used the audit methodologies recommended by the Government Accountability Office and guidelines issued by other Government authorities such as NIST.

We performed our work between August and September 2006 at NTSB Headquarters in Washington, DC. This performance audit was conducted in accordance with Generally Accepted Government Auditing Standards prescribed by the Comptroller General of the United States and included such tests as we considered necessary to detect fraud, waste, or abuse.

MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Edward Densmore	Program Director
Henry Lee	Project Manager
Dr. Ping Sun	Project Manager
Michael P. Fruitman	Communications Adviser
Jim Mallow	Senior Auditor
Aaron Nguyen	Computer Scientist
Atul Darooka	IT Specialist
Vasily Gerasimov	IT Specialist
Kathleen Huycke	Writer-Editor

National Transportation Safety Board

Washington, D.C. 20594

Office of the Managing Director

September 28, 2006

Rebecca Leng
Assistant Inspector General
for Financial and Information Technology Audits
Department of Transportation Inspector General
400 Seventh St. S.W., Room 9210
Washington, D.C. 20590

Thank you for giving me the opportunity to comment on your draft report on the NTSB's information security program, scheduled for release later this month. We appreciate your recognition of the concerted effort that the NTSB has made to improve its information security program and to correct the deficiencies that were identified in prior years. This letter constitutes my comments concerning your draft findings, and I request that this letter be made part of your final report.

Risk Assessment

Your draft report raises concerns about our application of Federal Information Processing Standard (FIPS) 199. Specifically, your draft report states that the NTSB completed risk assessments for only 3 of its 6 systems, and you note that all of our systems have been categorized as having the same impact level. The NTSB agrees that careful application of FIPS 199 is essential for accurately categorizing risk and mission impact level; however, the NTSB disagrees that vulnerability and threat information were not incorporated in our security categorizations. Our staff provided the audit team with an overview of the methods used to complete our FIPS 199 assessment, and we provided documentation that carefully explains how FIPS 199 practices were adhered in our assessment.

As we explained to your team, our risk assessment was conducted on a census, a 100% sample, of information types that make up our information systems. At the time of our risk assessment, the NTSB inventory listed 3 systems, including our General Support System (GSS). Our careful, high water mark analysis of these information types has led us to categorize each of our six systems as having a moderate risk level. Due to NTSB organizational changes and changes in managerial and financial oversight, and following suggestions from your office, 3 new systems were disaggregated from our GSS. As we certify and accredit (C&A) each of our systems, we will produce a system security plan (SSP) for each system that will detail the information types that make up the respective information system. Because one or more of the SSPs may include fewer information types than were included in the FIPS 199 risk assessment, it is conceivable–though unlikely–that one or more of our systems could be downgraded to a low

impact system. However, because no new information types will be listed in any system's SSP, no system will be upgraded to a high impact system. Therefore, it is likely that all of our systems will remain categorized at the moderate impact level.

That said, we recognize your concern that because our systems are all categorized at the same impact level, we could be faced with difficult decisions concerning which systems to C&A first, or how to provide appropriate protection for our various systems. We want to assure you that this is not the case. Our Program of Action and Milestones (POAM) sets forth a timetable for completion of C&A activities for each of our systems. This timetable represents our priority order for conducting our C&A responsibilities. Our GSS SSP will house the vast majority of common security controls for all of our systems, and therefore remains our highest priority for C&A.

We have confirmed with the National Institute of Standards and Technology (NIST) that there is no inherent expectation that agencies will assign different impact levels to their systems. Rather, agencies are required to comply with FIPS 199 definitions and precepts in determining security categorization levels. The NTSB takes its FIPS 199 responsibilities very seriously. Consequently, we are concerned that your draft oversimplifies of our view of this process. FIPS 199 defines high impact systems as those for which the "...loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals" (p. 3). The standard further states that a severe or catastrophic effect is one that might: "(i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organization assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries" (p. 3). The NTSB operates no such systems.

Password Security Requirements

The NTSB agrees with the best practice of using complex passwords and will incorporate it wherever possible in the appropriate SSPs. In fact, NTSB Operations Bulletin CIO-GEN-003, Paragraph 7(E) *recommends* constructing complex passwords by using a combination of letters, numbers, and special symbols. Our written policy does not require complex passwords; however, our security policies *do* enforce strong password requirements for those operating systems that support such enforcement. The NTSB suggests that this section be deleted from your report.

Previously Identified Vulnerabilities

The NTSB agrees that accurate vulnerability analysis and corrective action are critical components of an effective information security program, and we provided evidence to your audit team that we took aggressive action in this area. We provided documentation of our scanning program and procedures including meeting schedules, vulnerability reports, staff actions, and subsequent reviews detailing vulnerability remediation efforts. The information provided demonstrates that immediately after conducting our initial vulnerability scans, the NTSB began prioritizing the most critical vulnerabilities of password compliance issues and

patch management. CIO employees were directed to address over 92 computers that we identified as having password related vulnerabilities. Corrections were made and verified through subsequent vulnerability scans; however false vulnerability reports were noted and verified (e.g., one such machine reporting a false positive for administrative user names and passwords is CVR_CD). Other false positives have been noted as network printers or similar appliances whose operating systems have been customized by the manufacturer and are unable to be further modified. Because these appliances have limited CD burning or printing capability and are protected behind firewalls, the risks have been mitigated.

As noted in NIST Special Publication (SP) 800-42, *Guideline on Network Security Testing*, vulnerability testing may result in many false positive results. Therefore, proper identification of false positives, and analysis of mitigating controls is essential to this effort. We explained to audit staff, and we provided documentation to show that the vulnerability scan reports include many false vulnerability reports. For example, some network printers are erroneously reported by the software as Cisco routers, and some computers are erroneously listed as having password vulnerabilities that are not actually present on those computers. Although your team did not request it, a demonstration of the false positives identified in prior year IG scanning results as well as ongoing NTSB vulnerability scanning efforts could quickly resolve this issue.

Vulnerabilities such as buffer overflow have been addressed at the NTSB by using an automated patch management system that deploys security patches to NTSB desktop computers automatically upon their receipt. An overview of this system was provided to the IG staff as well as evidence of procurement activities that are currently underway to further augment this system. Automated patch management is an industry- and NIST-recommended (see NIST SP 800-42) best practice for addressing new security vulnerabilities, which are discovered every day. This approach enables the NTSB correct or mitigate vulnerabilities such as buffer overflow as they arise.

Intrusion Detection Capabilities

We appreciate your recognition that the NTSB implemented its intrusion detection capabilities in February 2006. However, Operations Bulletin CIO-GEN-005 *Incident Response and Handling Policy* and CIO-GEN-009 *Auditing, Monitoring, and Reporting Policy* were issued in June 30, 2006. As recommended for medium impact systems by NIST SP 800-53, the NTSB conducted periodic reviews of our intrusion detection logs. We provided evidence of this to your audit team.

Privacy

Your draft report notes that our docket system may contain privacy information , and it notes that the NTSB needs to develop a detailed privacy policy and procedures to ensure these data are properly protected. Although we do not disagree that more work remains, we note our *Docket Procedures Manual* contains our "Redaction User's Guide" that was published in March 2006. The Guide carefully explains what types of private information must be protected from

public release, and it provides detailed procedures for preparing docket materials for public release in a manner that ensures that private information will remain private.

Thank you again for the opportunity to provide these comments. We look forward to the issuance of your final report.

Sincerely,

David L. Mayer, Ph.D.
Deputy Managing Director & Acting CIO