U.S. Department of Transportation

Office of the Secretary
of Transportation

Office of Inspector General
Washington, D.C. 20590

August 4, 2006

The Honorable Mark V. Rosenker
Acting Chairman
National Transportation Safety Board
490 L'Enfant Plaza, S.W.
Washington, D.C. 20594

Dear Acting Chairman Rosenker:

We will be performing a limited review of the National Transportation Safety Board's (NTSB) information security program this year to meet the reporting requirements of the Federal Information Security Management Act of 2002 (FISMA). The audit objective is to determine the effectiveness of NTSB's information security program. Specifically, we will evaluate (1) whether system risks were properly assessed and security weaknesses were reported for corrections, (2) the effectiveness of the enhanced network security operations, and (3) the progress made by NTSB in protecting sensitive agency information.

The decision to do a limited review again this year is based on the current status of NTSB's information security program. During Fiscal Year (FY) 2006, NTSB has made a concerted effort to correct security weaknesses identified in the past, including establishing a new Chief Information Officer position; submitting progress reports to the Congress; providing security training to all employees; and, most noticeably, enhancing network security protection against both internal and external attacks.

One area that NTSB did not make sufficient progress in was reviewing, testing, certifying, and accrediting its information systems as adequately secured to support NTSB operations. This process, called certification and accreditation (C&A), serves as the backbone for implementing a viable information security program. Last year, we recommended that NTSB assign a high priority to completing the C&A review of its high-risk (most critical) systems. NTSB has since concluded that it has no high-risk systems and is now developing plans to perform C&A reviews on its systems. Given that

NTSB has not accredited any of its systems,[1] a complete review by our office is not warranted. We met with the Deputy Managing Director and Acting Chief Information Officer several times to discuss improvement to the C&A review process.

First, NTSB should consider disaggregating its systems inventory into smaller and more discrete entities to better align system ownership and to accelerate the security review process. NTSB initially reported only three systems for its entire inventory: the Financial Management System, Accident Investigation System, and General Support System. However, these systems perform 33 functions, some of which are not related even though they were grouped together under the same system. For example, the General Support System contains components supporting not only the network infrastructure but also facilities, fleet, and equipment management. After discussing this issue with us, NTSB officials increased the system inventory from three to six by "unbundling" functions that were previously embedded under the Accident Investigation System and the General Support System.[2] We commend this action and recommend NTSB reevaluate separating out components associated with the Financial Management System, too.

Second, NTSB should consider having more specific risk assessments to help prioritize its security review activity. The agency rated all systems as having the medium level of risk. We are concerned that under this assessment, all systems will receive the same level of security protection, even though some components are more sensitive than others. For example, the components used to analyze aircraft black-box recordings or to track the families of accident victims should receive a higher level of risk and protection than other components, such as policy and guidance tracking. NTSB officials informed us that they have correctly assessed the level of risk associated with each system. We plan to further evaluate this issue during the audit.

The audit will be conducted at NTSB Headquarters in Washington, D.C. We will contact your staff to establish an entrance conference. The project manager for the audit is Henry Lee. If you have any questions, please call me at (202) 366-1496, or Ed Densmore, Program Director, at (202) 366-4350.

Sincerely,

Rebecca Leng

Rebecca Leng
Assistant Inspector General
for Financial and Information Technology Audits

[1] NTSB processes its accounting, payroll, and travel transactions on the Department of the Interior's financial management systems. Interior has certified these systems for the portion that it is responsible for. However, Interior's certifications do not address operations that individual customer are responsible for, such as the integrity of data input into the system by the customer.

[2] The three new systems are the Telecommunications System, Physical Security System, and Laboratory Environment System.