Before the Committee on Government Reform
U.S. House of Representatives

For Release on Delivery
expected at
10:00 a.m. EST
Thursday
April 7, 2005
CC-2005-025

Department of Transportation's Implementation of the Federal Information Security Management Act

Statement of Theodore Alves

Assistant Inspector General for Financial
And Information Technology Audits

U.S. Department of Transportation

Mr. Chairman, Ranking Member Waxman, and Members of the Committee:

Thank you for the opportunity to testify today on progress and challenges the Department of Transportation (DOT) faces in implementing the Federal Information Security Management Act (FISMA). This Committee has been a driving force behind the improvements the Federal Government has made in protecting important information and information systems over the last several years. These improvements are essential to prevent the severe disruptions that can result from attacks by hackers or by others who are intent on harming the United States and its citizens. I also want to take this opportunity to compliment the Office of Management and Budget (OMB), the National Institute for Standards and Technology (NIST) and the Government Accountability Office (GAO) for the leadership roles they have played in this effort.

The Department of Transportation's 12 component agencies are responsible for one of the largest information technology (IT) investment portfolios among civilian agencies. An annual budget of about $2.7 billion supports over 480 information systems that are critical to carrying out the Department's mission of ensuring fast, safe, efficient, accessible, and convenient transportation. For example, the National Highway Traffic Safety Administration maintains a safety defects information system that receives manufacturer early warning reporting information to track and manage automobile defect and recall data. The Federal Highway and Federal Transit Administrations maintain systems that process over $35 billion in grants awarded to states and local governments.

The Federal Aviation Administration (FAA) operates about 100 systems to provide safe and efficient air traffic control services. Recognizing the critical role the air traffic control system plays in the nation's economic health and the mobility of our citizens, the President determined that the air traffic control system is a critical national infrastructure that must be protected from attack and must be able to reconstitute its operations rapidly in the event of an attack.

The results of fiscal year (FY) 2004 FISMA reports provided by Federal agencies and the Offices of the Inspectors General (OIG) show that a number of agencies have made significant progress meeting the goals set out by this Committee and OMB. DOT is one of the agencies that made significant progress last year and should be proud of the progress it has made. It is also important to recognize that Federal agencies, including DOT, are in the early stages of protecting their information and information systems and that continued attention must be paid to strengthening security to protect against evolving threats. Understanding the actions DOT has taken to improve its security posture may help the Committee to identify actions needed at other departments that have made less progress.

You asked us to address DOT’s progress in strengthening information security practices and the challenges it still faces, whether the Inspector General (IG) community needs an auditing framework to guide computer security audits, and the approach we take to audit computer security issues in DOT. Today I will discuss each of those issues.

DOT Made Significant Progress Improving Information Security

DOT made significant progress over the last 2 years protecting its information and information systems, but still faces challenges to secure its systems. To a large extent, DOT’s progress can be directly attributed to the support and commitment of Secretary Mineta.

This progress was accomplished against a backdrop of increased attention to this important issue. In addition to the annual FISMA audit, DOT’s efforts to enhance its information security program are closely monitored by OMB as part of the President’s Management Agenda. The President also issued several directives requiring agencies to protect the Nation’s critical infrastructure.

The commitment to improve information security begins at the top, and we attribute much of the improvement DOT has made in this area to support from Secretary Mineta. In early 2003, the Secretary appointed a Chief Information Officer (CIO) and significantly strengthened his role and responsibilities. Since then, the CIO has played a much more prominent role in managing IT issues, including ensuring that the Department adopted disciplined processes to enhance its information security program in all DOT component agencies.

The following summarizes major improvements made by the Department.

- **Increased focus on security in IT investment decisions.** DOT is currently consolidating its Headquarters IT infrastructure by combining the services currently provided by 11 component agencies into a single infrastructure. In addition to reducing costs and improving operations, reducing the number of system access points and the number of potential vulnerabilities should significantly improve security.

- **Strengthened DOT’s ability to protect networks from internal and external attacks.** In 2003, DOT established a Department-wide security incident response center. This center, which operates 24 hours a day, prevents, detects, and analyzes hundreds of potential intrusions from the Internet. During FY 2004, DOT expanded its vulnerability checks to cover not only its public web sites but also computers on internal networks. DOT’s recent progress contrasts sharply with its prior efforts to protect its systems. In 1997, we reported that the Department lacked firewalls to prevent outsiders from accessing sensitive internal systems from the Internet. In 2000, we reported that the Department had installed firewall security; however, it was not properly managed. As a result, our staff was able to penetrate the firewall and gained unauthorized access to 250 DOT computers from the Internet. Today, DOT not only has strengthened security over the Internet entry points (the "front door") but also other network connection points (the "back door") to DOT systems.

- **Increasing the number of systems certified and accredited from 33 percent to over 90 percent.** System security certifications are a critical and effective way to provide confidence that systems are secured commensurate with their individual operational risks. DOT trailed behind the Government average by having only 10, 12, and 33 percent of its systems completing such reviews during FYs 2001, 2002, and 2003, respectively. During FY 2004, DOT made a concerted effort to increase the number of system security certification reviews by dedicating resources to do the reviews and closely monitoring progress.

- **Strengthened background checks.** DOT improved its security practices by performing background checks on contractor personnel hired to perform sensitive work such as administering DOT networks. We previously reported a widespread lack of background checks on contractor personnel. This was a major concern to DOT due to the large number of contractor personnel, estimated to be around 18,000. In recent years, the Department established better mechanisms to track contractor personnel movement and ensured that the background checks were performed regardless of the contract length.

DOT Faces Challenges Improving Information Security

Notwithstanding recent progress, DOT still faces many challenges to secure its computer systems. This will require continued senior management attention to implement more disciplined risk-based computer security processes. Our FY 2004 FISMA report cautioned that DOT, and FAA in particular, needed to follow through aggressively in implementing corrective actions to prevent the security program from deteriorating into a significant deficiency in FY 2005. The following summarizes key challenges facing the Department.

- **Air traffic control system security must be enhanced.** We have reported several significant security deficiencies affecting air traffic control en route computer systems, which are used to support high-altitude traffic. Because of the sensitive nature of these deficiencies, we can only discuss two of the issues at this public hearing. First, although FAA had certified that the en route systems were adequately secured, the reviews were limited to developmental systems located at FAA's Technical Center computer laboratory. Operational systems deployed to the 20 en route centers also need to be reviewed because they are not mirror images of the developmental systems. Second, FAA has agreed to identify a cost-effective contingency plan to restore essential air service in the event of a prolonged en route center service disruption.

We recently communicated to the FAA Administrator, the Office of the Secretary, and the CIO our concern that FAA has not made sufficient progress correcting these deficiencies. We are working closely with the departmental and FAA CIOs to ensure continued progress. FAA needs to continue to make progress to prevent the security program from deteriorating into a significant deficiency in FY 2005.

- **Security certification process needs to be improved**. The Department made good progress in completing these reviews during FY 2004. However, our review of the quality of the certification reviews identified various deficiencies, such as inadequate assessments of the risks facing the system; lack of evidence that tests were performed; and in one case, a test item that had been listed as "passed" failed when we re-tested it. We also found that the appropriate senior official did not always make the decision to allow the system to operate. Obtaining system accreditation from the correct authorizing official is critical because this official not only has to accept the system risk (impact) on business operations but also has to have the authority to allocate budget resources to secure the system. The CIO office agreed to continue its efforts to enhance security certification and accreditation reviews.

- **DOT needs to focus attention on emerging threats from new technologies.** Evolving technologies create new vulnerabilities. DOT needs to continually be on guard to understand the emerging risks that come from new products, and new threats as hackers discover new ways to exploit software vulnerabilities. The CIO Office needs to consider emerging threats such as spyware (malicious software used to capture sensitive user information), phishing (emails leading users to compromised websites), or unsecured wireless communications.

Framework for Auditing Information Security Issues

In your invitation to us to testify, you asked us to discuss whether a framework for information security audits is needed. The fact that you raised this question suggests that the current framework does not fully meet oversight requirements. The DOT OIG supports and participates in several efforts to develop better computer security guidance for agencies and auditors to use, including an effort initiated by the President's Council on Integrity and Efficiency—a group of

Presidentially appointed IGs—to develop additional guidance for FISMA reporting. This group has begun looking at whether more standardization is needed but has not reached a consensus.

The IG community would benefit from greater clarity and understanding of how IG FISMA reports could be better structured to benefit both oversight organizations, such as this Committee, and the affected Department. Similarly, oversight organizations would benefit from understanding the challenges the IG community faces in addressing computer security issues in agencies with very different systems and missions. Discussions about this issue could help achieve a consensus. A key near-term action would be for the key players—OMB, GAO, congressional staff, and the IG community—to begin discussions of the pros and cons of increased standardization. Overall, we believe certain aspects of FISMA audits lend themselves to a more structured framework. The IGs also need to have the flexibility to deploy their limited resources in a cost-effective way to address the unique and evolving threats faced by their agencies.

Our Approach To Meet FISMA Requirements

The DOT OIG uses a two-pronged approach to meet the FISMA reporting requirements. Every year, we select a subset of systems and do detailed tests to answer the OMB performance measure questions, such as the percentage of systems with contingency plans tested. Throughout the year, we also perform various computer security audits with a focus on issues critical to DOT's mission. For example, we are currently conducting reviews of a system used by FAA to maintain air traffic control field equipment, a system used by the National Highway Traffic Safety Administration to track problem drivers, and the network infrastructure used by the Federal Railroad Administration to support its safety inspection program. Based on all this work, we then make judgments about the strengths and weaknesses of DOT's information security program when preparing our annual FISMA report.

We primarily rely on our IT audit staff to perform FISMA-related work, with limited contractor help in reviewing financial systems. Our staff consists of auditors, IT specialists, and computer scientists. This skill mix allows us to address both IT management and technical issues. In conducting our work, we follow GAO, NIST, and OMB guidance. Although neither FISMA nor OMB requires that our FISMA report meet Government auditing standards, we prefer to do so.[1] We believe that reports based on Government auditing standards provide users with more assurance that the underlying work can be relied on for decision-making purposes.

[1] FISMA allows IGs to issue either an audit report or an evaluation report. Audit reports must comply with Government auditing standards established by GAO, while evaluation reports do not.

Mr. Chairman, this concludes my oral testimony. More details are provided below. I would be happy to answer any questions.

PROGRESS DOT HAS MADE AND CHALLENGES IT FACES TO IMPROVE INFORMATION SECURITY

The Department has significantly improved its information security program over the last 2 years, and those improvements account for the significant strides DOT made in FY 2004. This progress is the result of strong commitment and support from Secretary Mineta who, in early 2003, significantly strengthened the CIO's role and responsibilities. Before FY 2003, the CIO did not play a central role in ensuring that IT systems were secured against attack. Since then, the CIO's role in Department-wide IT issues, including computer security, has become much more prominent. The CIO, with support from the Secretary and other senior leaders, has made good progress ensuring that component agencies take the steps needed to ensure their systems are secure. For example, the CIO Office now performs oversight of the quality of component agency IT system security reviews. That oversight provides added assurance that systems have been adequately secured.

The attributes of effective Information Resources Management and computer security programs begin with a commitment and support at the top of the organization. The commitment requires the appointment of a strong CIO with the authority and resources to set direction, provide the correct mix of skills to do the job, establish policies and guidelines, and ensure that subordinate organizations implement disciplined practices. When we began focusing resources on computer security issues back in the late 1990s, DOT did not have those attributes. In fact, we found an almost total lack of attention to protecting critical systems and information. To illustrate, in April 1997, we reported that the Department's computer systems lacked firewalls to prevent outsiders from accessing sensitive internal systems and information directly from public pages on the Internet. Over the next several years, we identified additional weaknesses, including unprotected telephone connections to DOT computer systems, a lack of background investigations for staff performing sensitive functions, and the lack of an effective process to certify systems as secure.

While DOT officials worked for several years to address these problems, their efforts were hampered initially by the lack of a strong CIO with the authority and resources to implement disciplined processes or to require the various component agencies to take computer security issues seriously. As a result, in FY 2000, we were still able to gain unauthorized access to 250 DOT computers through the Internet.

In November 2002, the Inspector General testified that the Department lacked those attributes. He pointed out that DOT had a long way to go to secure its computer systems and in fact had operated for the prior 1½ years without a CIO.

He specifically recommended that the Department promptly appoint a CIO with the authority to provide Department-wide leadership and enforce compliance with security guidance. The Inspector General's testimony also occurred against the backdrop of the President's effort to focus attention on computer security issues through the President's Management Agenda and to better protect critical national infrastructures through Presidential Decision Directives. The Department took the following actions:

- Secretary Mineta appointed a CIO in March 2003 and ensured that the CIO had the authority to implement disciplined information resource management and computer security practices;

- Within months, the CIO provided strong leadership by invigorating the Investment Review Board, which reviews IT investments to determine whether they should be modified, terminated, or allowed to continue. The Investment Review Board is headed by the Deputy Secretary with support provided by the CIO Office.

- The CIO has secured a commitment from component agencies to implement the Department's information security program. This effort is being carried out with the help of over 400 trained information security personnel. The CIO and component agencies also supplement these staff with contractor resources to address key technical issues.

- The CIO has made good progress implementing disciplined processes to enhance the information security program. For example, DOT has established a risk-based approach to perform system security reviews and to test system security. DOT also provides specialized training to security specialists.

- The CIO Office also took on more operational responsibilities, including establishing a full-time unit to monitor activity on all DOT networks. This has significantly strengthened DOT's ability to detect and report attempted intrusions into DOT networks.

The CIO's broader responsibilities led to increased funding needs to support the more disciplined processes and more intensive reviews, as well as the new operational responsibilities. However, the CIO Office needs to provide better justification for its IT budget requests. Because of the high level of generality and vagueness in the budget justification, Congress reduced the CIO Office's FY 2004 budget by $15.9 million, from $23.4 million to $7.5 million. Our review confirmed that the CIO's budget request and supporting documentation lacked the details oversight organizations, including OMB and Congress, needed to understand how the funds would be used.

The CIO Office subsequently had to submit to both the House and Senate Committees on Appropriations a reprogramming request of about $2.5 million to cover costs associated with computer security activities, including funding to support its certification and accreditation reviews. The Committees approved the reprogramming, and the CIO Office agreed to provide more complete information in future budget requests, so that decision-makers can make informed decisions about the appropriate level of funding.

The CIO also needs to improve how security-related budget requests are coordinated between the CIO Office and component agencies. For example, in its FY 2005 budget, the CIO Office requested $2 million to install advanced vulnerability remediation and patch management software to protect the Department's IT infrastructure. About 90 percent of the installation would have been on FAA network computers. However, FAA had also set aside funds to acquire a similar solution, and the two requests had not been adequately coordinated.

DOT's Progress Improving Information Security

The changes instituted by Secretary Mineta led to significant improvements in DOT's ability to secure its information and information systems over the last 2 years and especially in FY 2004. Some of the most noteworthy progress DOT has made in information security includes:

- **Increased focus on security in IT investment decisions.** The departmental Investment Review Board expanded its review of component agency investment projects to ensure that investment plans adequately addressed security issues. The CIO also directed component agencies to evaluate opportunities to consolidate common administrative and business systems. For example, DOT is currently consolidating its Headquarters IT infrastructure by combining the services currently provided by 11 component agencies into a single infrastructure. In addition to being an important initiative to reduce costs and improve operations, it should also significantly improve security by reducing the number of system access points and therefore, the number of potential vulnerabilities.

- **Strengthened ability to protect networks from internal and external attacks.** DOT has made significant progress protecting its systems from internal and external attacks. This serious problem persisted for several years. In 2003, DOT established a Department-wide security incident response center. In cooperation with a similar center operated by FAA, this center operates 24 hours a day to prevent, detect, and analyze hundreds of potential intrusions from the Internet. During FY 2004, DOT expanded its vulnerability checks to cover not only its public web sites but also computers on internal networks in all component agencies. The CIO Office also issued guidelines for configuring computers in a secure manner to prevent vulnerabilities.

- **Increased the number of systems certified and accredited from 33 percent to over 90 percent.** System security certifications are a critical and effective way to provide confidence that systems are secured commensurate with their individual operational risks. This action provides additional assurance that DOT program operations that depend on computer systems support can maintain the integrity, confidentiality, and availability of the information they rely on to carry out their missions.

- **Strengthened background checks.** DOT also made significant progress ensuring that background checks are performed on contractor staff performing sensitive services. Previously, we found that DOT did not require all contractors to undergo background checks and even when the checks were required, many were never performed. DOT improved its security practices by requiring background checks for all contractor personnel performing sensitive activities, regardless of the contract length. Previously, background checks were not performed if the contract term was for less than 6 months.

Challenges to Sustain This Progress

Notwithstanding recent progress, DOT still faces many challenges to secure its computer systems. This will require continued senior management attention to implement more disciplined risk-based computer security practices. This is key to ensuring that critical information and systems are secure, especially the air traffic control system. For example:

- **Air traffic control system security must be enhanced.** During FYs 2003 and 2004, we reported several significant security deficiencies associated with air traffic control en route computer systems. En route systems control high-altitude traffic. Because of the sensitive nature of these deficiencies, we can only discuss two of the issues at this public hearing. We have previously discussed all of the issues with this Committee's staff.

  First, although FAA certified that the en route systems were adequately secured, the reviews were limited to developmental systems located at FAA's Technical Center computer laboratory. Operational systems deployed to en route centers also need to be reviewed. FAA has agreed to review operational en route systems by the end of FY 2005 and to review all other air traffic control systems—at approach control and airport terminal facilities—by the end of December 2007.

Second, FAA has agreed to identify a cost-effective contingency to restore essential air service in the event of a prolonged service disruption at an en route center. This is important because the President has designated the air traffic control system to be a critical national infrastructure. Presidential guidance calls for critical infrastructures to have contingency plans in place to restore essential services in a timely manner. FAA will use the results of an alternatives analysis to identify cost-effective alternatives. FAA needs to focus now on the near-term actions it can take to restore partial services in the event of a prolonged disruption.

- **The security certification process needs to be improved**. The security certification review, which is performed by system owners in conjunction with the CIO Office, is a critical and effective security measure to determine whether individual systems are adequately secured commensurate with operational risks. The Department made good progress in completing these reviews during FY 2004. However, the CIO office needs to continue working with component agencies to improve the quality of the reviews. Our review of the quality of the certification reviews for 20 systems identified 1 or more deficiencies in 14 cases. These deficiencies included inadequate assessments of the risks facing the system; lack of evidence that tests were performed; and, in one case, a test item that had been listed as “passed” failed when we re-tested it.

  We also found that the appropriate senior official did not always make the decision to allow the system to operate. One of the most important steps in completing a security certification and accreditation review is the responsible senior official’s (the system user’s) decision whether to accept the remaining security weaknesses and allow (accredit) the system to operate. Obtaining system accreditation from the correct authorizing official is critical because this official not only has to accept the system risk on business operations but also has to have the authority to allocate budget resources to secure the system. In 4 of 20 systems we reviewed, technical managers and not the appropriate senior official accredited the systems for operations. The CIO office agreed to continue its efforts to enhance the process of the security certification and accreditation reviews.

- **DOT needs to focus attention on emerging threats from new technologies.** Evolving technologies create new vulnerabilities. DOT needs to continually be on guard to understand the emerging risks that come from new products and new threats as hackers discover new ways to exploit software vulnerabilities. The CIO Office needs to consider emerging threats associated with technologies, including:

- Software, called spyware, that allows malicious individuals to covertly capture sensitive information from a user's system,

- Phishing, which is a form of email that directs users to a compromised web site that then solicits personal, financial, or business information.

- Wireless technologies, which can increase risks that agency information will be compromised. Wireless technology poses a threat in part because the devices tend to be managed by individuals, who may be less security conscious than system administrators.

Overall Security Program Status

Our FY 2004 FISMA report concluded that based on the progress the Department made, the overall status of the security program, and FAA's commitment to take aggressive action to correct air traffic control deficiencies, DOT's information security program warranted downgrading from a material weakness to a reportable condition. We cautioned, however, that DOT, and FAA in particular, needed to followed through aggressively in implementing corrective actions to prevent the security program from deteriorating into a significant deficiency in FY 2005. We cited FAA's progress reviewing operational systems and implementing en route center contingency plans as a key factor we will use in making our determination of whether DOT's security program contains significant deficiencies in FY 2005.

Now, 6 months later, we are concerned that FAA has not made sufficient progress correcting en route air traffic control deficiencies we reported last year, including security certification reviews of computer systems at en route centers and development of contingency plans to restore air traffic control services in case of a prolonged service disruption at an en route center. We have communicated these concerns in writing to the responsible DOT officials, including the CIO, the Office of the Secretary, and the Federal Aviation Administrator. The FAA CIO responded to those concerns, indicating FAA's continued commitment to pursue timely implementation of corrective actions. We are now engaged in further discussions with the departmental and the FAA CIOs about the actions needed to ensure continued progress to address these important issues.

FRAMEWORK FOR AUDITING INFORMATION SECURITY

The fact that you raise the question about whether a framework for information security audits is needed indicates that the current framework does not fully meet your oversight requirements. The DOT OIG supports and participates in several efforts to develop better computer security guidance for agencies and auditors to use,[2] including an effort initiated by the President's Council on Integrity and Efficiency—a group of Presidential appointed IGs—to develop additional guidance for auditing security issues and for reporting FISMA results. This group has begun looking at whether more standardization for FISMA reporting is needed but has not reached a consensus.

The IG community would benefit from greater clarity and understanding of how IG FISMA reports could be better structured to benefit both oversight organizations, such as this Committee, and the affected Department. Similarly, oversight organizations would benefit from understanding the challenges the IG community faces in addressing computer security issues in agencies with very different systems and missions. Discussions about this issue could help achieve a consensus. A key near-term action would be for the key players—OMB, GAO, congressional staff, and the IG community—to begin discussions of the pros and cons of increased standardization. Overall, we believe certain aspects of FISMA audits lend themselves to a more structured framework. The IGs also need to have the flexibility to deploy their limited resources in a cost-effective way to address the unique and evolving threats faced by their agencies.

Some key issues that the DOT OIG believes need to be considered in this dialogue follow.

- **The IG community needs to retain the flexibility to address the unique and evolving threats and vulnerabilities faced by each agency.** Both agencies and auditors need the flexibility to focus their resources on the burning issues of the day. We all need to use a risk-based approach to strengthen computer security, and we need to adjust our focus to address evolving risks. For example, DOT maintains a wide variety of systems with very different vulnerabilities and consequences. The consequences from an attack on a system that maintains information about employee training are very different than the consequences of an attack on an air traffic control system. Similarly, because agencies have achieved different levels of maturity in addressing computer security issues, agencies and auditors must focus their limited resources on the most vulnerable security processes faced by the agency. For example, some OIGs are still reporting that their agencies lack a complete inventory of systems or a reliable system to track vulnerabilities and action plans. Those agencies and their auditors need to be

[2] Our Deputy Assistant Inspector General for Information Technology and Computer Security is also a member of the Information Security and Privacy Advisory Board. The Board is responsible for advising NIST and the OMB Director on information security and privacy issues pertaining to Federal Government information systems. The Board was established by the Computer Security Act of 1987 and reauthorized by FISMA.

able to focus their attention on getting those basic processes in place to correct those high-risk deficiencies.

- **NIST and GAO have provided a common framework for implementing and auditing computer security.** NIST recently issued a series of guidelines and standards for agencies to use, as required by FISMA. We find NIST guidance to be very useful because it is generally complete, adequately detailed, and authoritative. DOT applies NIST guidance, and we use it as criteria when we evaluate how effectively DOT's security program is operating. GAO has also issued guidance for auditing security over individual computer systems, called the Federal Information Systems Control Audit Manual. The entire IG community commonly uses this manual when auditing security over individual systems.

- **Agencies and auditors also need to ensure that they devote adequate resources to improve all information resources management processes.** This is because computer security is an important subset of information resources management. Instituting disciplined management practices is critically important to ensure that agencies receive value for the billions of dollars spent on IT, but it is also critical to ensure adequate security. Efforts to strengthen the CIO and Investment Review Board functions have spill-over effects that lead to improved computer security. For example, a strong investment review process can build computer security into the system, a much more cost-effective approach than identifying and correcting deficiencies after system deployment. Some estimates show it costs 10 times as much to correct problems after deployment.

- **Financial statement and FISMA audits**. You also asked whether financial statement audit guidance provides a model for computer security audits. The American Institute of Certified Public Accountants developed the financial statement audit requirements, which are supplemented by the GAO's Financial Audit Manual. Financial audit guidance has evolved continuously over the last 100 years, most recently to incorporate the stronger requirements to audit management controls imposed by the Sarbanes-Oxley Act. Most IGs also conduct a wide range of other financially related audits to address financial management issues that are not covered by financial statement audits. Because computer security did not receive a lot of attention until about 20 years ago when Congress passed the Computer Security Act of 1987, information security audits are still in their infancy. Certain aspects of information security audits clearly lend themselves to a structured framework, including network vulnerability assessments, system penetration testing, and intrusion detection and incident response capabilities.

OUR APPROACH TO MEETING FISMA REQUIREMENTS

The DOT OIG approaches the FISMA reporting requirement as a part of our efforts to ensure that DOT has effective IRM processes in place. We perform a series of computer security audits during the year focused on the issues we believe involve the highest risk or the issues that most need management's attention. The results of those efforts are then included in our annual FISMA report.

Throughout the year, we focus a significant amount of our IT resources on information security issues. Our IT audit staff consists of auditors, IT specialists, and computer scientists. This mix of IT management and technical skills allows us to address both the management processes and the detailed technical issues the Department faces as it strengthens its computer security capabilities. For example, we use our computer scientists to do very technical reviews, including penetration testing or identification of system design or software flaws. We use our IT auditors to analyze the quality of management processes, like the certification and accreditation process, and to make constructive recommendations to strengthen processes. As we stated earlier, disciplined processes are essential to an effective computer security program. We also hire contractors to help us audit computer controls related to financial systems.

To be ready to meet the annual FISMA reporting requirement, we monitor the CIO's efforts to comply with OMB reporting requirements throughout the year. After OMB issues its guidance specifying which performance measures it wants tracked, we select a subset of systems and do detailed tests of the source data to answer the OMB performance measure questions. Our FISMA report also draws on all other audit work we have done during the year to make judgments about the strengths and weaknesses of DOT's computer security efforts.

For example, we recently initiated two computer security audits. We are reviewing the National Highway Traffic Safety Administration's National Driver Registry system. The system is a central repository of information about individuals who have had their driver's license suspended or revoked. The information that resides on the system, such as social security numbers, is subject to Privacy Act protection. Unauthorized disclosure of this information could lead to identity theft, a problem that has affected nearly 10 million Americans. We will review this system to ensure that the information is reliable and that access to the information is only available to authorized personnel. We have discussed this audit with your staff members who have expressed interest in the results.

We are also reviewing the Federal Railroad Administration's (FRA) network infrastructure, which is critical to the missions of DOT and FRA. FRA is one of five DOT component agencies that have its own direct Internet connections, allowing the public to access the DOT network from the Internet. We will review the network infrastructure to ensure security weaknesses do not exist that could jeopardize the confidentiality, integrity, and availability of the data residing on FRA and DOT systems.

In conducting our work, we follow GAO, NIST, and OMB guidance. GAO establishes Government auditing standards, which we follow in performing computer security audits. Although neither FISMA nor OMB requires that our FISMA report meet Government auditing standards, we prefer to do so. We believe that reports based on Government auditing standards provide users with more assurance that the underlying work can be relied on for decision-making purposes.