Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform

U.S. House of Representatives

For Release on Delivery
expected at
10:00 a.m. EST
Tuesday
November 19, 2002
CC-2003-027

Computer Security Challenges Within The Department of Transportation

Statement of

The Honorable Kenneth M. Mead

Inspector General

U.S. Department of Transportation

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

We appreciate the opportunity to testify today on computer security issues concerning the Department of Transportation (DOT). Computer security has received increased attention since the Nation successfully completed the Year-2000 (Y2K) conversion. The events on September 11 and the war on terrorism made DOT more aware of the need to protect computer systems in today's worldwide-interconnected environment.

I would like to thank you, Mr. Chairman, for your leadership in the areas of information technology, computer security, and good management practices in general. We will all remember your persistent and unwavering commitment to solve the Y2K computer crisis, which led to a smooth transition into the 21st century.

There are in fact numerous similarities between the Y2K crisis and computer security vulnerabilities facing the Nation today. Both require identification of vulnerabilities, risk assessments, priority setting as to which vulnerabilities to fix first and at what cost, and top level management commitment. However, an important difference is that there was a date certain by which computers had to be Y2K compliant and all agencies knew that date was at the turn of the millennium.

While addressing computer vulnerabilities requires more technical sophistication than Y2K, the ultimate success for securing computer systems still depends on sound management, not technical, solutions. DOT, with $3.6 billion in planned expenditures in Fiscal Year (FY) 2003, has one of the largest information technology (IT) investments of all Federal civilian agencies. About 70 percent of IT expenditures are for the Federal Aviation Administration (FAA).

DOT computer systems are essential to our national economy, security, and smooth operation of the Nation's transportation system. DOT has 561 mission-critical systems that are used to perform such functions as directing air traffic, rescuing distressed ships, and distributing money to build the Nation's highway and transit systems. About 100 of these mission-critical systems are essential to the nation's defense, economic security, or public confidence (infrastructure-critical) and need to be secured on a priority basis. Securing these systems is more important today because at least some of them are likely to interface with the new Department of Homeland Security.

Last year, DOT's information security program received a failing grade from both this committee and the Office of Management and Budget (OMB). DOT also reported its information security program as a material weakness. During FY 2002, under Secretary Mineta's leadership, DOT made a strong commitment to improve information security and received a favorable rating from OMB on its progress.

The most noteworthy improvements were in three areas. **First**, DOT hired a senior official to lead the information security program. **Second**, DOT significantly enhanced its defense against intrusions from the Internet. In 1997, DOT did not use firewall security software to ensure that only authorized users gained access to DOT computer systems from the Internet. Today, not only has DOT installed more sophisticated firewall security at all Internet connection points, it also has network intrusion detection systems that monitor access around the clock. **Third**, FAA, which has most of DOT contractor employees, has increased the percentage of background checks on contractor employees from 23 to 84 percent in the past 2 years.

Notwithstanding recent progress, DOT still has a long way to go to adequately secure its computer systems. Today, DOT's information security program remains a material weakness and requires continued senior management attention. Our recent report on DOT's Information Security Program (FI-2002-115) can be viewed at www.oig.dot.gov. For security reasons, specifics concerning the weaknesses and vulnerabilities we identified and our audit procedures are not discussed in the audit report or this testimony statement. Our testimony will focus on the following key points:

- DOT needs a Chief Information Officer (CIO) with the authority to provide departmentwide leadership and to enforce compliance with security guidance. For the 6 years since passage of the Clinger-Cohen Act, DOT has had an agencywide CIO for only 18 months and the position has been vacant since January 2001.
- While DOT has significantly enhanced its network security to prevent intrusion from the Internet, DOT's computer systems are still vulnerable because of other unsecured network entry points, such as direct connections with non-DOT computers or telephone line (dial-up) connections which can be used from almost anywhere to access DOT computer systems.
- DOT reported more than 25,000 incidents to the Federal Computer Incident Response Center (the Center) during FY 2002. However, DOT did not perform sufficient analyses to determine whether these incidents were caused by intrusion activities or by innocent acts such as making an error when entering passwords. DOT did not bother reporting 3 of 10 major incidents involving web defacements.
- Web security and privacy protection are essential for encouraging the public to use DOT E-government services. DOT has made good progress to better protect the public's privacy but still needs to better protect its web sites. Although DOT has implemented procedures to identify and correct vulnerabilities for 36 percent of its computer systems, we identified 453 vulnerabilities on DOT web servers, 113 of which were on the Federal Highway Administration's systems. DOT has corrected these vulnerabilities.

- Performing background checks on contractor employees is very important to DOT because of the large number of contractor employees. During the past 2 years, FAA has made good progress by increasing its background check completion rate from 23 to 84 percent. However, FAA still needs to do more as do the other Operating Administrations for which the completion rate increased only from 13 to 14 percent.
- Only about 22 percent of DOT mission-critical systems have undergone security certification reviews. Because of slow progress, DOT needs to double the number of annual reviews to meet the December 2005 milestone to identify vulnerabilities in all mission-critical systems and determine the costs to fix the security weaknesses.

DOT needs the leadership of an appointed CIO to prioritize the use of financial and people resources to improve computer security. We also are concerned that the Operating Administrations are placing too much reliance on our auditors or the General Accounting Office to identify vulnerabilities in their computer systems. Program managers need to proactively evaluate computer systems to decide whether systems are adequately secured commensurate with perceived risks. DOT has a plan to get all of these done by December 2005. The DOT CIO office is in the process of developing a specific corrective action plan for submission to OMB by the end of December 2002.

CIO LEADERSHIP AND AUTHORITY

The Clinger-Cohen Act of 1996 requires DOT to establish an agency CIO responsible for acquiring and managing IT resources. The Government Information Security Reform Act of 2000 further directs the agency CIO to develop and maintain an agencywide information security program, including effective implementation of information security policies, procedures, and control techniques.

In addition to appointing an agency CIO, DOT needs to ensure that the CIO can exercise authority, that authority is reinforced by the Office of the Secretary, and that individual Operating Administrations are held accountable for following the CIO office's security guidance. This is important because of DOT's complex organizational structure. From an IT investment perspective, the major challenge within DOT is that almost all of the $3.6 billion budgeted for IT expenditures is under the control of the individual Operating Administrations, not the DOT CIO.

To be effective, the CIO needs specific authority from the Secretary to address cross-cutting issues such as computer security. Also, to better coordinate IT

investments, DOT needs a CIO with the proper authority to set departmental priorities, ensure effective IT acquisitions, and implement security procedures.

DOT Needs to Appoint a CIO

For the 6 years since passage of the Clinger-Cohen Act, even with its active recruiting efforts, DOT has had an agencywide CIO for only about 18 months and the position has been vacant since January 2001. This leadership is essential to effective administration of IT systems acquisitions and information security requirements. To its credit, the DOT CIO office recently issued guidance on network security, cyber incident reporting, and capital planning. While this security guidance is sound, it alone will not correct system vulnerabilities. We found that the DOT Operating Administrations did not effectively implement the guidance and generally were not held accountable for doing so.

For example, we first reported in 1999 that contract employees working on critical DOT systems did not receive background checks. Since then, the CIO office issued several directives for corrective actions. We recently sampled 178 contractor employees employed by FAA, the Transportation Security Administration (TSA), and the Office of the Secretary. We found 43 (24 percent) individuals did not receive background checks.

Another example is that the Operating Administrations did not follow the guidance issued by the CIO office in estimating security costs. Although the Operating Administrations doubled their estimates from $51 million to $103 million between FYs 2002 and 2004, they could not provide support for the budget estimates as required by the CIO guidance.

The CIO Needs Specific Authority to be Effective

Effective implementation of computer security guidance has been a long-standing problem in DOT for several reasons. In addition to not having an appointed CIO, the DOT CIO office does not have the proper authority necessary to effect meaningful change in the Operating Administrations. Unlike some counterparts in other Federal agencies, the DOT CIO office does not provide input or approve Operating Administrations' IT budgets, and does not provide input to performance appraisals of their CIO.

In contrast, within the Department of Agriculture, appropriated funds cannot be used to acquire new IT systems or upgrades without the approval of its CIO. In the Department of Commerce, the CIO participates in the performance appraisal of bureau CIOs. The General Accounting Office also praised the Veterans Affairs

Department's recent decision to give its agency CIO oversight authority for all IT funds.

Until it is clear that there are management and budget consequences for noncompliance with the CIO security guidance, the Operating Administrations' current practices are likely to continue. To address this issue, we recommended in our recent report on DOT's Information Security Program that the Deputy Secretary establish the CIO's authority and clarify the consequences for noncompliance with the CIO office's security guidance. The Deputy Secretary is considering these recommendations.

NETWORK AND SYSTEMS SECURITY

DOT has thousands of computers on its networks and about one million web pages that provide E-government services to the public through the Internet. In recent years, DOT has focused its efforts on network defenses against intrusions from the Internet. For example, FAA issued guidance on improving Internet connection points, deployed more intrusion detection mechanisms at major network control points, and established a cyber incident response center with a continuous operation capability. The DOT CIO office also issued cyber incident reporting guidelines and reported some significant incidents to the Federal Computer Incident Response Center operated by the General Services Administration.

However, DOT's computer systems are still vulnerable to intrusion because of other unsecured network connections. DOT needs to secure these network entry points such as direct connections with non-DOT computers or telephone line (dial-up) connections which can be used from almost anywhere to access DOT computer systems.

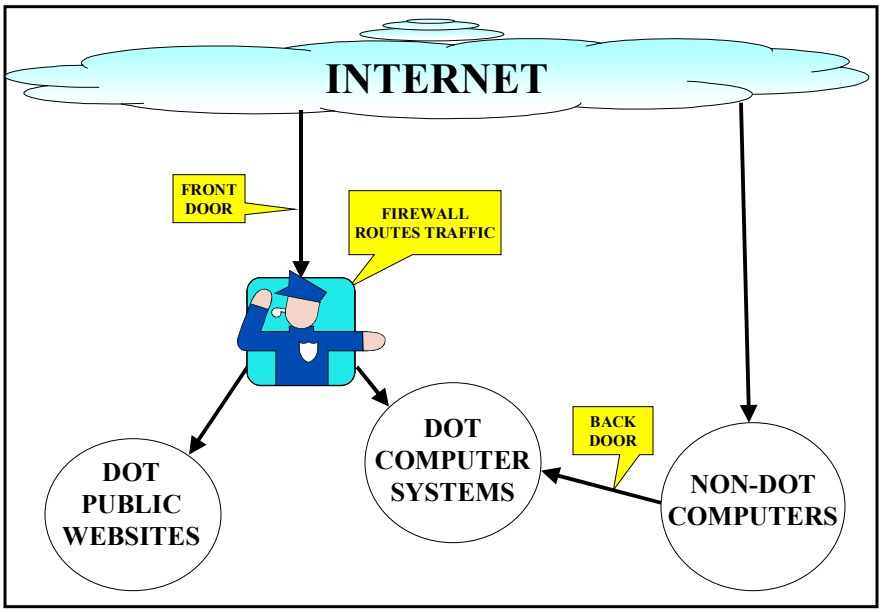
Also, more than 100,000 DOT employees, contractors, grantees, and industry associations are authorized to pass through the firewall security and enter DOT's computer networks (insiders). According to the Federal Bureau of Investigation, about 50 percent of unauthorized access activities in FY 2001 were by insiders.

Controls over Direct Connections From Non-DOT Computers are Weak

DOT employees, contractors, grantees, and industry associations access DOT's computer networks through either the Internet (front doors) or other means such as direct computer connections or dial-up telephone lines (back doors). DOT has installed firewall security at all authorized Internet connection points to direct citizens to DOT public web sites for E-government services.

Meanwhile, employees, contractors, and business associates can access DOT computer systems, as pictured in Table 1.

Table 1
Access to DOT Networks



DOT has made good strides in securing its front doors. For example, in 1997, we reported that DOT did not use firewall security software to ensure that only authorized users could enter DOT's computer networks from the Internet. In 2000, DOT installed firewall security but did not do it right. As a result, we were able to penetrate DOT security and gained unauthorized access from the Internet to about 270 DOT computers. Today, not only has DOT installed firewall security at all authorized Internet connection points, it also has established network intrusion detection systems monitoring access around the clock and cyber incident response capabilities.

However, controls over the back doors remain weak. When we testified before this committee in 1998, we reported that DOT systems were not adequately protected because of unsecured network connections or dial-up lines. Since then, the CIO office issued multiple guidance on corrective actions. Nonetheless, we recently found three unsecured direct network connections to contractor sites and about 300 unauthorized telephone line (dial-up) computer connections at one FAA facility. Because of the relationship between this facility and air traffic control systems, it is critical that these back doors be secured. We brought this issue to FAA's attention and corrective actions were taken to secure these connections.

Cyber Incidents Need to be Analyzed to Identify Major Trends

While DOT has significantly enhanced its network defense against intrusion, no technology can totally prevent hacking attacks in today's dynamic environment. Under OMB's direction, DOT has installed intrusion detection mechanisms and reported more than 25,000 incidents to the Federal Computer Incident Response Center (the Center) during FY 2002.

However, DOT did not perform sufficient analyses to determine whether these incidents were caused by intrusion activities or by innocent acts such as making an error when entering passwords. As a result, DOT may have slowed down the Center's capability in identifying major trends in cyber attacks. Meanwhile, 3 of 10 significant incidents involving DOT web defacements were not reported to the Center. DOT needs to enhance its cyber incidents reporting process.

Public Web Sites Providing E-government Services Need to Be Protected

One of the President's Management Agenda items is to use technologies and the Internet to improve Government services to the public (E-government). Web security and privacy protection are essential for encouraging the public to use DOT's E-government services. Attacks on these web sites could result in defacing web sites, manipulating data, placing web servers out of service, or disrupting business by deleting regulatory reports.

DOT has made good progress to better protect the public's privacy and proactively identify and correct vulnerabilities on 36 percent of its web systems. Notwithstanding, we identified 453 vulnerabilities throughout DOT, 113 of which were on the Federal Highway Administration's systems. Seventy-nine (79) of these vulnerabilities were rated as high because they might allow attackers to execute remote commands to take over DOT web sites. DOT corrected all of these vulnerabilities and plans to develop a process to periodically scan all DOT web sites for vulnerabilities.

Unfortunately, the events on September 11 and the war on terrorism made DOT more aware of protecting sensitive information from inappropriate disclosure. DOT searched its web sites and removed information now considered to be sensitive. We also scanned web sites and found a few documents labeled "For Official Use Only" and sensitive security information displayed on DOT's public web sites. DOT removed these documents. DOT needs to increase employee awareness training to identify appropriate materials to display on public web sites.

Background Checks Are Needed on People Working on Sensitive Computer Systems

The lack of background checks is a particular concern in DOT because of the large number of contractor employees, estimated to be around 18,000, working on DOT systems. While background checks provide no guarantee as to a person's loyalty or trustworthiness, they do provide valuable information that might keep some people who are at risk from working on DOT systems. We first reported this concern in 1999 and DOT issued multiple memoranda for corrective actions. However, this year we still found 24 percent of the individuals we checked did not receive background checks, but they were still working on DOT computer systems.

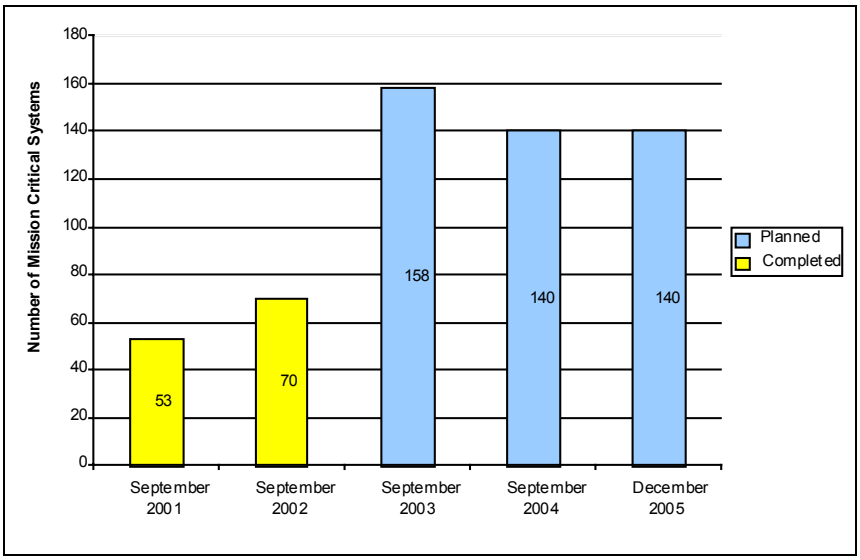
Most contractor employees work for FAA. FAA has made significant progress in this area by increasing its background check completion rate from 23 to 84 percent between FYs 2000 and 2002. However, FAA still needs to do more as do the other Operating Administrations. During the same period of time, other Operating Administrations only increased their completion rate from 13 to 14 percent. For example, none of the 10 TSA contractor employees we reviewed received background checks. DOT has again issued guidance requiring the Operating Administrations to complete background checks within 6 to 12 months.

Program Managers Need to Perform Security Certification Reviews to Identify System Vulnerabilities and Remediation Costs

A simple and effective management control is to periodically perform reviews to certify that major computer systems are adequately secured. As we stated earlier, this review requires program managers to proactively evaluate computer systems and use their judgment to decide whether systems are adequately secured commensurate with perceived risks. So far, only 22 percent (123 of 561) of DOT's mission-critical systems have received such reviews. Most security weaknesses that we identified could have been detected and corrected had DOT conducted such reviews. For example, at two FAA sites, we found about 100 people who no longer work there could still access air traffic control systems because their access accounts were never closed. In another case, the Operating Administration identified about 100 missing computers that were loaded with critical software. However, we found no followup actions were initiated.

The Secretary has established a goal to have all DOT mission-critical systems certified and accredited by December 2005. This is a major challenge for DOT because it needs to double the number of annual system certification reviews in the next 3 years. DOT plans to develop a schedule detailing the systems to undergo certification reviews during FYs 2003, 2004, and 2005 (see Table 2).

Table 2
Certification and Accreditation of Mission-critical Systems



Until all mission-critical systems have undergone at least one security certification review, DOT does not really know how much money is needed to secure critical systems. Some corrective actions such as establishing business continuity capabilities for infrastructure-critical systems may require significant investments. Conversely, security over other systems could be significantly enhanced at little cost through good business practices such as enforcing periodic password changes or deleting access accounts when employees are terminated. DOT should assign a funding priority to complete security certification reviews of all mission-critical systems.

Finally, DOT is making progress addressing computer security issues. However, based on our recent results, more work needs to be done and management attention should be focused on identifying computer vulnerabilities that need immediate fixing.

Mr. Chairman, this concludes our statement. I would be pleased to answer questions.