# Memorandum

**U.S. Department of Transportation**
Office of the Secretary of Transportation
Office of Inspector General

Subject: ACTION: Report on Web Systems Security, DOT FI-2002-118

Date: September 30, 2002

From: Alexis M. Stefani
Assistant Inspector General for Auditing

Reply to Attn. of: Meche

To: Acting Chief Information Officer, DOT

This report presents our audit results on the Department of Transportation (DOT) web systems security. We conducted this audit to respond to the statutory requirements of the Government Information Security Reform Act (GISRA). GISRA assigns responsibility to the Office of Inspector General (OIG) for evaluating the DOT information security program.

Our audit objectives were to determine whether DOT's public web systems are (1) adequately secured to reduce the risk of being attacked and are equipped to detect and report abnormal activities or cyber incidents, (2) properly configured to protect the public's privacy, and (3) free of sensitive information. Our scope and methodology are discussed in Exhibit A.

## INTRODUCTION

Implementing Electronic-government (E-government) to improve Government services to the public is on the President's Management Agenda. The primary goals for E-government initiatives are to use technologies and the Internet to:

- Make it easy to obtain services from and interact with the Federal Government;
- Improve Government efficiency and effectiveness; and
- Improve the Government's responsiveness to citizens.

The Government Paperwork Elimination Act of 1998 also requires agencies to provide the option of electronic submission or disclosure of information as a substitute for paper by October 2003. DOT has more than 200 web sites with about

1 million web pages accessible through the Internet. DOT uses these web sites to conduct business such as accepting payments, or to disseminate information such as motor carrier safety records. DOT also is leading the development of Online Rulemaking, which is 1 of 23 cross-agency E-government initiatives approved by the President's Management Council.

Web security is essential for E-government services. Attacks on Government web sites could result in embarrassment (web sites defaced), inconvenience to the public (web servers out-of-service), or disruptions to business (reports to meet regulatory requirements deleted). DOT has developed a performance measurement program (scorecard) to monitor its implementation of the President's E-government agenda. Enhancing computer security accounts for 20 percent of the measurement.

With the move to provide more E-government services, privacy protection is important because the public will not use Government web sites unless they are confident that their privacy will not be violated.[1] The tragic events on September 11 also require that agencies reevaluate whether sensitive information is disclosed on public web sites.

## RESULTS IN BRIEF

DOT made good progress to better protect the public's privacy since our last audit.[2] Our statistical sample of web pages did not identify unauthorized use of persistent cookies[3] and the Operating Administrations corrected the web security vulnerabilities we identified last year. To its credit, the DOT Office of the Chief Information Officer (CIO office) implemented a process to have about 30 percent of DOT public web sites scanned for web security vulnerabilities.

During Fiscal Year (FY) 2002, DOT also deployed cyber incident detection mechanisms at 15 Internet connection points and major network control points. Notwithstanding this progress, more remains to be done to secure DOT web sites. We found the following vulnerabilities and deficiencies:

- **Web Site Vulnerabilities**. Using a commercial scanning software on 175 of DOT's 201 public web servers, we identified 453 vulnerabilities[4] across the

[1] In the Fiscal Year 2001 Consolidated Appropriations Act, Congress required the OIG at each Federal agency to report on the agency's collection and review of personally identifiable information on Internet sites.

[2] Report on DOT Web Privacy, Report Number: FI-2001-034, February 26, 2001.

[3] A persistent cookie represents a mechanism used on web sites to collect information by placing small bits of software on web users' computers.

[4] Identified vulnerabilities were associated with 59 types of vulnerabilities.

Operating Administrations (Exhibit B), 66 percent of which were on the Federal Aviation Administration (FAA) and Federal Highway Administration (FHWA) web sites. We rated these vulnerabilities as 79 high, 283 medium and 91 low.[5] Eight Operating Administrations had no high vulnerabilities. Adopting a process for regular scanning of public web sites could mitigate risks from recurring vulnerabilities. We provided these vulnerabilities to management for corrective action. As of September 10, 2002, DOT already had corrected 435 vulnerabilities, including all vulnerabilities identified in FAA and FHWA. The remaining vulnerabilities are being reviewed.

- **Need for Network Services.** The CIO office issued security guidance in June 2001 requiring the Operating Administrations to disable unneeded network services on DOT web systems because they can provide easy access to unauthorized users. We found a particular network service was available on 106 DOT web servers. We used this network service to gain access to payroll and personnel information on a web server on DOT's private network. DOT immediately disabled this network service on the payroll web server and is reviewing whether it should be disabled on other web servers.

- **Web Sites Operated by Third Parties.** DOT has at least 35 web sites that operate on third-party computers. For example, a web site containing motor carrier safety records is operated by a contractor. Although we did not scan these 35 web sites due to uncertainty with respect to legal rights and potential liability, we found that service providers were not required to provide assurance that DOT web sites are adequately protected. None of the 35 web system owners was able to provide assurance of adequate security, and DOT had no policy requiring such assurance from third-party providers.

- **Cyber Incident Reporting.** To secure E-government services, the Office of Management and Budget (OMB) requires agencies to develop a cyber incident response capability to detect and report intrusion activities. During FY 2002, DOT reported more than 25,000 incidents to the Federal Computer Incident Response Center without sufficient analyses to determine whether these incidents were caused by intrusion activity or by innocent acts such as making an error when entering passwords. Meanwhile, DOT identified 10 actual incidents involving web defacements, but we found only 3 were reported.

[5] For security reasons, specifics concerning these vulnerabilities are not discussed in this report. High vulnerabilities may provide an attacker with immediate access into a computer system, such as allowing execution of remote commands. Medium and low vulnerabilities may provide an attacker with useful information, such as password files, to compromise DOT computers.

- **Sensitive information on Public Web Sites.** Protecting sensitive information from inappropriate disclosure is a new emphasis area for Government agencies. We found four documents labeled "For Official Use Only" and other sensitive information on DOT public web sites. DOT immediately removed this information from its web sites.

Although the CIO office issued memoranda addressing our prior recommendations, the Operating Administrations in most cases did not take effective implementation actions. To further enhance web security, we are recommending that DOT perform more comprehensive scans for web vulnerabilities, upgrade its scanning capability to cover all DOT public web systems, establish requirements to protect DOT web sites operated on third-party computers, enhance cyber incident reporting, increase employee awareness training on protecting sensitive information, and establish procedures to perform automatic searches for sensitive information on public web sites. The Acting Chief Information Officer concurred with our recommendations.

## FINDINGS AND RECOMMENDATIONS

### Security Needs to be Strengthened on DOT Web Sites

Using a commercial scanning software on 175 DOT public web servers, we identified 453 vulnerabilities across the Operating Administrations (Exhibit B). We rated these vulnerabilities as 79 high, 283 medium, and 91 low. Eight Operating Administrations had no high vulnerabilities. Of the high vulnerabilities, 21 are on the Federal Bureau of Investigation (FBI) Top 20 listing. These vulnerabilities could allow intruders to remotely execute malicious program codes or gain unauthorized access to the root directory[6] on DOT web servers, resulting in service interruption or embarrassment, such as web defacement.

We found that these vulnerabilities could be easily eliminated by installing vendor software patches or by system reconfiguration. We provided these vulnerabilities to management for corrective action. As of September 10, 2002, DOT already had corrected 435 vulnerabilities, including all vulnerabilities identified in FAA and FHWA, and all high vulnerabilities on the FBI Top 20 listing. The remaining vulnerabilities are being reviewed.

The CIO office issued a Server Security Checklist in June 2001 and directed its use to ensure that DOT servers are securely configured prior to connection to the DOT network. Although steps were taken to issue new guidance, we found that this control procedure was not implemented by all of the Operating Administrations, three of which were not aware that the checklist existed.

[6] From the root directory, intruders can create or delete files.

To its credit, the CIO office implemented a process during FY 2002 to use an automated scanning tool to check DOT public web servers for vulnerabilities. These scans covered about 30 percent of DOT public web servers and identified vulnerabilities that needed to be eliminated. This effort is a proactive step in the right direction and should be expanded to cover all web sites and upgraded to perform more comprehensive vulnerability assessments. Adopting a process for regular scanning of public web sites could mitigate risks from recurring vulnerabilities.

## Unneeded Network Services Should be Disabled

The CIO office issued guidance in June 2001 directing Operating Administrations to periodically evaluate their computers and disable unneeded network services. Network services are communications software used for connections between computers and can be used by unauthorized users to gain access to places for which they have no right to be. The DOT policy requires unneeded network services be disabled because they provide additional avenues for unauthorized access.

The CIO office's guidance was not being followed. We found a particular network service was available on 106 DOT web servers. In FY 2000, we used this network service to gain unauthorized access to a DOT financial system. During this audit, we used the same network service to gain access to payroll and personnel information on a web server on DOT's private network. DOT immediately disabled this network service on the payroll web server and is reviewing whether use of this network service on other web servers is necessary.

## Security Assurance is Needed from Third Parties

DOT has at least 35 web sites that operate on third-party computers. For example, a contractor operates DOT's web site containing motor carrier safety records. We did not scan these 35 web sites due to uncertainty with respect to legal rights and potential liability. Instead, we tried to determine what assurance DOT received from service providers that adequate security was provided for DOT web sites. None of the 35 web system owners was able to provide such assurance in writing. We found DOT had no policy requiring written assurance from third-party providers, and its contracts do not include language providing DOT authority to scan for vulnerabilities.

## Cyber Incidents Need Analyses Before Reporting

OMB requires agencies to develop a cyber incident response capability to adequately detect intrusion activities and to timely share the information with law enforcement authorities and the Federal Computer Incident Response Center (FedCIRC). The CIO office issued its Interim Incident Handling and Reporting Guidelines in December 2001. The guidelines require Information Systems Security Officers to

collect and report information regarding computer security incidents for their organizations to the CIO office, which then will share the information with FedCIRC or the FBI's National Infrastructure Protection Center.

We found that the interim reporting guidelines were not effectively implemented and need to be improved. During FY 2002, DOT reported more than 25,000 incidents to FedCIRC without sufficiently analyzing whether these incidents were caused by intrusion activities or innocent acts such as making an error when entering passwords. DOT used a variety of automatic intrusion detection systems to monitor its networks, which are capable of detecting thousands of potential cyber incidents in a short period of time. Without doing sufficient analyses, DOT reported incidents to FedCIRC such as failed computer connections, which could have resulted from innocent acts such as entering a wrong password. DOT must analyze its detections to determine whether there were other abnormal activities, such as checking what network services are operating on computers,[7] before reporting them as cyber incidents.

While DOT was reporting innocent acts to outside agencies, we found that actual cyber incidents were not reported as required. DOT identified 10 actual web defacements, but we found only 3 were reported. DOT needs to perform in-depth analyses before reporting cyber incidents to outside organizations.

## Sensitive Information Was Found on Public Web Sites

The tragic events on September 11 have increased agencies' awareness of limiting access to sensitive information. On March 19, 2002, the White House Chief of Staff directed an immediate re-examination of public documents. DOT asked its Operating Administrations to check the information displayed on public web sites and to remove "sensitive but unclassified information." In June 2002, the Operating Administrations reported progress, including removal of sensitive information identified, to the Secretary's office. On July 12, 2002, DOT responded by stating that the Department was working toward total compliance with the guidance for protecting sensitive information, and that the OIG would check for sensitive information as part of its ongoing audit of web systems security.

Our search on July 24, 2002, identified four documents labeled "For Official Use Only" on DOT public web sites. These documents discussed aviation safety risks. For example, one document discussed how FAA selects aviation repair facilities for safety inspections. DOT policy requires that information labeled "For Official Use Only" be protected against uncontrolled release. We also identified sensitive security information[8] on DOT web sites such as procedures for screening air travel passengers

[7] Commonly referred to as "port scan."

[8] The guidance concerning sensitive security information is stated in Title 49, Code of Federal Regulations, Part 1520.

carrying classified materials. When we brought these issues to management's attention, these documents immediately were removed from the web sites.

Because protecting sensitive information from inappropriate disclosure is a new emphasis area for Government agencies, DOT needs to increase employee awareness training on protecting sensitive information, and establish procedures to periodically review web content on its public web sites. The DOT Office of Security and Administrative Management has expertise that could be helpful in developing awareness training.

## RECOMMENDATIONS

We recommend that the Acting DOT Chief Information Officer, in coordination with the Operating Administrations' CIOs:

1. Eliminate the vulnerabilities and disable unneeded network services we identified by October 31, 2002.
2. Upgrade the automated scanning tool to perform more comprehensive vulnerability assessments and implement policy to have all DOT public web sites periodically scanned for potential vulnerabilities to include followup requirements to ensure implementation.
3. Establish policy that system owners obtain written assurance from third-party web service providers for compliance with DOT security requirements to include followup requirements to ensure implementation.
4. Consult with the DOT General Counsel and the Senior Procurement Executive to include contract language in web service contracts for the authority to scan third-party web sites for vulnerabilities.
5. Enhance DOT's cyber incident reporting capability by performing in-depth analyses on detected incidents and by establishing more specific criteria for reporting cyber incidents to the Federal Computer Incident Response Center.
6. Work with the DOT Office of Security and Administrative Management to increase employee awareness training on protecting sensitive information and establish procedures, including use of automated tools, to periodically review material on DOT public web sites.

## MANAGEMENT RESPONSE

A draft of this report was provided to the Acting DOT Chief Information Officer on September 24, 2002. He concurred with the recommendations as follows.

**Recommendation 1**. Concur. We note that our office has not reviewed all Operating Administration reports; consequently, we will need to work with the Operating Administrations to identify the complete list of vulnerabilities and network services that need to be addressed based on business risks.

**Recommendation 2**. Concur. We will implement the process by June 2003.

**Recommendations 3, 4, and 5**. Concur. We will implement the processes by September 2003.

**Recommendation 6.** Concur. While we concur in general and will work to implement appropriate review and training procedures by June 2003, we cannot commit to using automated tools at this time. We will pursue the potential for use of tools where and when budgets can accommodate this activity.

The complete text of management comments is in the Appendix.

## OFFICE OF INSPECTOR GENERAL COMMENTS

Actions taken and planned are reasonable, subject to followup requirements of DOT Order 8000.1C. We will continue to work closely with the CIO office to enhance web security throughout DOT.

We appreciate the courtesies and cooperation of DOT and the Operating Administrations' representatives. If you have questions concerning this report, please call me at (202) 366-1992 or John Meche at (202) 366-1496.

#

## EXHIBIT A. SCOPE AND METHODOLOGY

Using a commercial scanning tool, we performed a vulnerability assessment on 175 of DOT's 201 public web systems connected to the DOT homepage, including Operating Administration-specific web systems. We analyzed the vulnerabilities based on "The 20 Most Critical Internet Security Vulnerabilities" identified by the FBI. We also interviewed key security officials in each Operating Administration and collected data from the CIO office on cyber incident reporting.

To review web privacy protection, we developed a computer program to create a master list of DOT public web pages, totaling about 1 million. From the master list, we statistically sampled 1,211 web pages to check for existence of unauthorized persistent cookies.

To determine whether DOT public web systems contained sensitive information, we used the search engine on DOT web systems to perform the following key word search--For Official Use Only, Confidential, Sensitive Information, and Privacy Act Protected. We then reviewed web documents containing these key words and consulted with Transportation Security Administration officials in determining whether they should be removed from public web sites. We also searched for maps on web sites that may indicate locations of sensitive Government infrastructure.

This is our fourth report on web privacy and security. The prior reports are: Computer Security over DOT Web Sites (Report Number FI-2001-061, May 23, 2001); DOT Web Privacy (Report Number FI-2001-034, February 26, 2001), and Headquarters Computer Network Security (Report Number FI-2000-124, September 25, 2000).

Our audit work was performed between May and August 2002 at DOT Headquarters in Washington, D.C. The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States.

## EXHIBIT B. VULNERABILITIES BY OPERATING ADMINISTRATION

| Operating Administration | Vulnerabilities Found | | | Total Vulnerabilities | Web Servers Scanned |
|---|---|---|---|---|---|
| | High / Top 20 | Medium | Low | | |
| FAA | 30 / 7 | 133 | 23 | 186 | 70 |
| FHWA | 30 / 5 | 78 | 5 | 113 | 13 |
| OST | 10 / 1 | 22 | 9 | 41 | 23 |
| RSPA | 5 / 4 | 10 | 26 | 41 | 21 |
| TASC | 1 / 1 | 9 | 8 | 18 | 11 |
| NHTSA | 0 | 10 | 4 | 14 | 4 |
| FMCSA | 2 / 2 | 6 | 4 | 12 | 5 |
| BTS | 0 | 3 | 6 | 9 | 9 |
| STB | 0 | 6 | 0 | 6 | 1 |
| FTA | 0 | 2 | 3 | 5 | 5 |
| USCG | 0 | 3 | 0 | 3 | 8 |
| FRA | 0 | 0 | 2 | 2 | 2 |
| MARAD | 0 | 1 | 1 | 2 | 1 |
| TSA | 1 / 1 | 0 | 0 | 1 | 1 |
| SLSDC | 0 | 0 | 0 | 0 | 1 |
| **TOTAL** | **79 /21** | **283** | **91** | **453** | **175** |

# EXHIBIT C. MAJOR CONTRIBUTORS TO THIS REPORT

## THE FOLLOWING INDIVIDUALS CONTRIBUTED TO THIS REPORT.

| Name | Title |
|---|---|
| Rebecca Leng | Program Director |
| Ping Sun | Project Manager |
| William Coker | Senior Auditor |
| Bronwyn Gallagher | Computer Scientist |
| Henry Lee | Computer Scientist |
| Cynthia Tims | Information Technology Specialist |

# APPENDIX. MANAGEMENT COMMENTS

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

400 Seventh St., S.W.
Washington, D.C. 20590

September 27, 2002

**MEMORANDUM**

To: John L. Meche, Deputy Assistant Inspector General for Financial and Information Technology Audit

From: Eugene K. Taylor, Jr., Acting Chief Information Officer, S-80

cc: Lisa Schlosser, Associate CIO, IT Security

Subject: Draft Report on Web Systems Security, DOT

---

The Chief Information Officer has reviewed the subject report and thanks the Inspector General for the insight and recommendations as to how DOT can continue to improve its Information Technology Security Program. We substantially concur with the report and in FY 2003 will plan to implement the IG's recommendations as reflected below, with the exceptions noted:

1. IG Recommendation: Eliminate the vulnerabilities and disable unneeded network services identified by the IG by October 31, 2002.

   CIO Comment: We concur with this recommendation; however, we will note that our office has not reviewed all Operating Administration reports; consequently, we will need to work with the OAs to identify the complete list of vulnerabilities and network services that need to be addressed based on the OAs business risks.

2. IG Recommendation: Upgrade the automated scanning tool to perform more comprehensive vulnerability assessments and implement policy to have all DOT public web sites periodically scanned for potential vulnerabilities to include follow-up requirements to ensure implementation.

   CIO Comment: Concur. We will implement the process by June 2003.

3. IG Recommendation: Establish policy that system owners obtain written assurance from third-party web service providers for compliance with DOT security requirements to include follow-up requirements to ensure implementation.

   CIO Comment: Concur. We will implement by September 2003.

4. IG Recommendation: Consult with the DOT General Counsel and the Senior Procurement Executive to include contract language in web service contracts for the authority to scan third-party web sites for vulnerabilities.

   CIO Comment. Concur. We will implement the process by September 2003.

5. IG Comment: Enhance DOT's cyber incident reporting capability by performing in-depth analyses on detected incidents and by establishing more specific criteria for reporting cyber incidents to the Federal Computer Incident Response Center.

   CIO Comment. Concur. We will implement the process by September 2003.

6. IG Comment: Work with the DOT Office of Security and Administrative Management to increase employee awareness training on protecting sensitive information and establish procedures, including use of automated tools, to periodically review material on DOT public web sites.

   CIO Comment: While we concur with this recommendation in general, and will work to implement appropriate review and training procedures by June 2003, we cannot commit to using automated tools at this time, although we will pursue the potential for the use of tools where and when budgets can accommodate this activity.

In closing, although we do substantially agree with the recommendations made by the IG as noted above, the successful completion of all of these recommendations will be contingent upon adequate resources at both the Department and within the Operating Administrations. Additionally, we would like to note that the Department uses a different vulnerability reporting methodology than the IG which results in an increased number of vulnerabilities reported by the IG over that reported by the Department. We recommend that this be resolved in FY 2003.

Thank you for the opportunity to comment.