ARRA WEBSITES VULNERABLE TO HACKERS AND CARRY SECURITY RISKS

Department of Transportation

Report Number: FI-2011-006
Date Issued: 10/22/2010

Memorandum

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

Subject: ACTION: Report on ARRA Websites Vulnerable to Hackers and Carry Security Risks Department of Transportation Report Number: FI-2011-006

Date: October 22, 2010

From: Earl C. Hedges
Acting Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA–20

To: Chief Information Officer, DOT

On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 (ARRA) in response to the economic crisis facing the nation. ARRA requires unprecedented levels of transparency and accountability so that taxpayers know where their tax dollars are being spent. To address that requirement, the Department of Transportation (DOT) and its Operating Administrations (OA) deployed various Websites to collect and disseminate ARRA related information. With multiple Websites in play, DOT's ARRA program inevitably inherits security risks. In recent years, public Websites have become the target of cyber attacks. For example, hackers launched a malicious denial-of-service attack against DOT's main Website on July 5, 2009, resulting in the public's inability to access DOT information. In addition, vulnerabilities in Web-based technologies could allow attackers to gain unauthorized access to sensitive information stored in agency computers.

The objective of this audit was to determine if DOT's recovery Websites and database systems are properly configured to minimize the risk of cyber attacks. Accordingly, we performed assessments of these Websites and systems to identify vulnerabilities. A detailed description of the scope and methodology used on this audit can be found in exhibit A. We conducted this audit between December 2009 and July 2010 in accordance with generally accepted government auditing standards.

RESULTS IN BRIEF

DOT's ARRA-related Websites and databases contain a combination of high-, moderate-, and low-risk vulnerabilities.[1] By exploiting the high-risk vulnerabilities, hackers could attack the computers used by the public to access the Websites and gain access to sensitive data, such as password files stored on servers, take control of a server and attack other computers on DOT's networks. These vulnerabilities exist because the Websites, databases and servers are not configured in compliance with DOT configuration security standards. For security reasons, we are not presenting specific vulnerabilities in this report. However, we briefed department officials on specifics including potential fixes to address our recommendations.

BACKGROUND

Seven Operating Administrations (OAs) have received over 48 billion dollars in ARRA stimulus funds, with more than 93 percent of these funds allocated to FHWA, FRA and FTA (see Table 1).

Table 1. Distribution of ARRA Funds within DOT

OA	Stimulus Funds (millions)	Percent of Total
Federal Highway Administration (FHWA)	$27,500	57.15%
Federal Railroad Administration (FRA)	$9,300	19.33%
Federal Transit Administration (FTA)	$8,400	17.46%
Office of the Secretary (OST)	$1,500	3.12%
Federal Aviation Administration (FAA)	$1,300	2.70%
Maritime Administration (MARAD)	$100	0.21%
Office of Inspector General (OIG)	$20	0.04%
Total	**$48,120**	**100.00%**

Source: ARRA

ARRA outlined two different reporting requirements in order to track the use of Recovery funds--Section 1201 and 1512:

[1] High-risk vulnerabilities may provide an attacker with immediate access into a computer system, such as allowing execution of remote commands. Moderate-risk and low-risk vulnerabilities may provide an attacker with useful information, such as error messages revealing system configuration that they can then use to compromise a computer system.

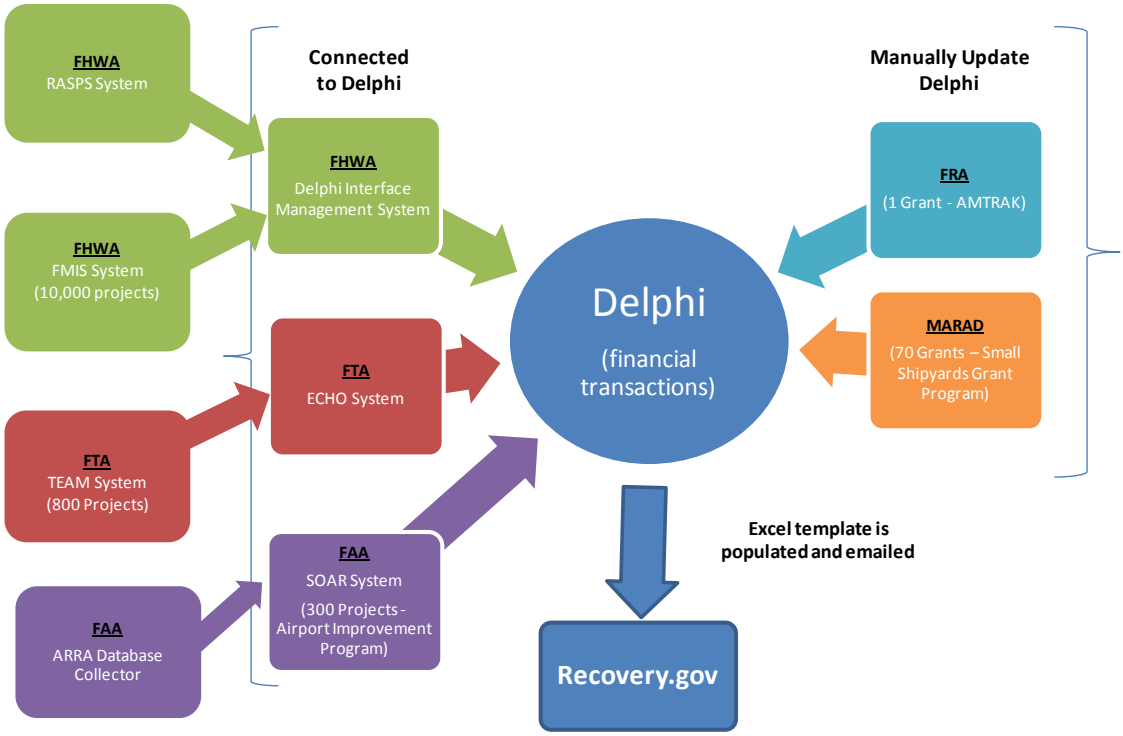
- Section 1201 requires agencies to provide periodic reports to Congress, tracking the amounts of Federal funds appropriated, numbers of projects put out to bid, numbers of projects awarded and the amounts awarded, numbers of projects for which work has begun or completed, numbers of jobs created, and aggregate expenditures by each grant recipient.

- Section 1512 requires recipients to submit quarterly reports to the Department identifying the total amount of funds received, the amount of funds obligated, a detailed list of projects for which funds were expended, and detailed information on any sub grants awarded by the grant recipient.

In fulfilling Section 1201 reporting requirements, DOT uses its existing financial systems to compile ARRA data. Five OAs--FHWA, FAA, MARAD, FRA, and FTA--have developed internal processes for collecting, storing, and reporting information on ARRA grant activities to OST. MARAD and FRA report this information directly through the departmental financial system, Delphi, while FHWA, FAA, and FTA use their own grant management systems to process and store data before it is electronically sent to the Delphi system. When the Department is ready to report on these funds, an extract of the data is populated into an Excel template by OST and emailed to the Recovery Accountability and Transparency Board for posting to the Recovery.gov website (see Figure 1).

In an effort to provide transparency to the public, these OAs post ARRA data to their individual Websites, and DOT's main Recovery Webpage and interactive map Website which displays geographical information on the ARRA projects. Currently, DOT's interactive map Website is maintained by the Research and Innovative Technology Administration (RITA). Our audit focused on DOT's recovery Websites.

Figure 1. DOT ARRA Reporting Process (Section 1201)



Source: OIG

ARRA Websites and Databases Are Vulnerable to Cyber Attacks

The OAs' ARRA-related Websites and databases, including the servers on which they are hosted, contain a total of 1,822 high-risk, 3,550 medium-risk, and 3,759 low-risk security vulnerabilities (see Table 2).[2] These vulnerabilities exist because the Websites, servers, and database systems are not configured in compliance with DOT's configuration security standards. As a result, the systems are vulnerable to cyber attacks which could not only undermine DOT's ARRA reporting, but also interrupt DOT's business operations.

[2] Due to the software manufacturer's use of slightly different definitions for classifications of vulnerability, we combined their "critical" and "high-risk" vulnerabilities into one "high-risk" category, and their "informational" and "low-risk" vulnerabilities into one " low-risk" category.

Table 2. Vulnerability Assessment Results

	Number Reviewed	Potential Vulnerabilities		
		High	Medium	Low
Server Level Assessment	16	7	6	48
Website Assessment	13	1759	1257	3541
Database Assessment	3	56	2287	170
TOTAL	32	1822	3550	3759

Source: OIG

Most of the high-risk vulnerabilities are associated with 13 Websites,[3] which contain Web pages used to post ARRA-related information for public use. These vulnerable Websites could put users' computers in danger by allowing hackers to gain access to the users' computer and their personal information, thus diminishing the public's trust in the Agency. For example, one particular vulnerability, found on 8 of the 13 Websites, could allow hackers to use the Websites to launch attacks on users' computers.

In addition, we identified high-risk vulnerabilities on the computer servers hosting ARRA information.[4] Such vulnerabilities could allow attackers to gain access to the ARRA data residing on the servers. By exploiting these vulnerabilities, we obtained password and system configuration files from one server. If an inside attacker were able to exploit the same vulnerability, he or she could potentially crack the passwords, take control of the server, and do harm, such as introducing viruses, to DOT's network.

We also identified several high-risk vulnerabilities on the databases, which could result in damage to the ARRA-related data stored in the databases. For example, to facilitate grantees' collection of information for external reporting, per ARRA Section 1512, FHWA implemented a database system known as the Recovery Act Data System (RADS). We found vulnerability on this database which could be exploited to compromise the database's server and result in unauthorized access allowing modification or destruction of ARRA data. For security reasons, we are

[3] A Website consists of many Web pages that display information for Internet users.

[4] These servers include those hosting DOT's TIGER Collector system. TIGER Collector was initially developed for OAs to centralize DOT's ARRA reporting. However, at the time of our audit, the system was no longer being used by OAs since OAs had found ways of using their own financial systems for ARRA reporting. Although the Web interface of TIGER Collector has been disabled, the two computer servers supporting this system were still active on DOT's internal network as of April 6, 2010.

not presenting specific vulnerabilities in this report. However, we provided detailed information to department officials for immediate corrective actions.

CONCLUSION

The Department of Transportation received an additional 48 billion taxpayer dollars through ARRA. Not only is DOT responsible for ensuring transparency and accountability of ARRA funds so that taxpayers know how these dollars are spent, it is also responsible for ensuring that its publicly accessible Websites are reasonably secured. DOT's ARRA-related Websites, servers and databases, however, are vulnerable to cyber attacks because they are not configured in compliance with the Department's security configuration standards. DOT management needs to take immediate corrective actions to minimize the risk of cyber attacks on these systems.

RECOMMENDATIONS

For security reasons, we are not disclosing the details of the potential fixes we provided to OA officials. Accordingly, we recommend that DOT's Chief Information Officer direct OA officials to (1) take immediate actions to correct the high-risk vulnerabilities found on ARRA-related Websites and databases, and (2) ensure that the planned corrections of other weaknesses identified during this audit are tracked and monitored in the OAs' Plan of Actions and Milestones (POA&M) system.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided a draft of this report to the DOT Chief Information Officer for comment on August 30, 2010, and received his response on September 30, 2010. He concurred with the two recommendations and discussed appropriate planned actions and target completion dates. The response is included in its entirety in Appendix A.

ACTIONS REQUIRED

The CIO's planned actions and target dates are responsive to our recommendations. We consider these recommendations addressed pending completion of the planned actions. We appreciate the courtesies and cooperation of Department of Transportation representatives during this audit. If you have any questions concerning this report, please call me at (410) 962-3612 or Louis King, Program Director, at (202) 366-1407.

#

cc: Chief Information Officer, FHWA
Chief Information Officer, FTA
Chief Information Officer, FRA
Chief Information Officer, FAA
Chief Information Officer, MARAD
Chief Information Officer, RITA
Martin Gertel, M-1

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusion based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusion based on our audit objective.

The audit work was performed from December 2009 to July 2010. We surveyed all Operating Administrations (OA) to collect specific information regarding all internal or public facing systems, such as Websites and databases that are related to ARRA reporting. Based on the OAs' input, we compiled an inventory of DOT's ARRA-related Websites and database systems. We also interviewed officials from the OAs that received ARRA stimulus funds in order to gain an understanding of DOT's ARRA reporting process.

To determine if DOT's recovery Websites and database systems are configured to minimize the risk of cyber attack, we performed vulnerability assessments on the computer systems, Websites and databases identified in the inventory. We performed the assessment using automated software tools as well as manual testing techniques. We reviewed the results of the scans to determine if the systems were in compliance with DOT's security configuration standards.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Louis King	Program Director, IT Audit
Dr. Ping Sun	Program Director, IT Audit Computer Laboratory
Michael Marshlick	Project Manager
Vasily Gerasimov	Computer Scientist
Atul Darooka	Information Technology Specialist
Susan Neill	Writer-Editor

APPENDIX A. AGENCY COMMENTS

Memorandum

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

Subject: **INFO:** Chief Information Officer Response - ARRA Websites Vulnerable to Hackers and Carry Security Risks

Date:
Reply to:
Attn. Of:

SEP 30 2010

From: Nitin Pradhan
Chief Information Officer

To: Louis King
Acting Assistant Inspector General for Financial
and Information Technology Audits

Prepared By: Andrew Orndorff
Chief Information Security Officer

The Department of Transportation takes seriously its responsibilities to protect the public trust and the use of Federal funds as appropriate, including implementing and enforcing effective information technology (IT) security measures. We understand the particular sensitivities associated with the use of funds from the American Recovery and Reinvestment Act of 2009 and are working with the Department's operating administrations to ensure, to the extent possible, that the Department's Recovery Act related IT capabilities are fully and appropriately secured.

Recommendation: Take immediate actions to correct the high-risk vulnerabilities found on ARRA-related Websites and databases, and ensure that the planned corrections of other weaknesses identified during this audit are tracked and monitored in the OAs' Plan of Actions and Milestones (POA&M) tracking system.

Response: Concur. We are working to address the report's findings as expeditiously as possible. Specifically, the Department's Chief Information Security Officer (CISO) consistent with the requirements of the Federal Information Security Management Act of 2002 (FISMA), has taken the following actions:

- Provided copies of the detailed vulnerability data to all operating administrations for whom vulnerabilities were identified as of September 9, 2010;

- Directed operating administration Information System Security Officers (ISSOs) and Information System Security Managers (ISSMs) to review the data and identify all false-positive vulnerabilities to the Office of the Inspector General and the CISO by September 17, 2010;

APPENDIX A. AGENCY COMMENTS

- Instructed ISSOs/ISSMs to follow the agency plan of actions and milestones (POA&M) management process for management of the remaining vulnerabilities, and to specifically remediate critical, high vulnerabilities within 90-days or have a specific plan of action for remediation of these registered in the agency security management system, CSAM, within 90-days, or November 8, 2010.

Overall, the Department is committed to focusing its efforts to ensure all bone fide high level vulnerabilities are remediated as quickly as possible and employing a prioritized approach to rectify the remaining vulnerabilities through completion. In light of the importance of this issue, my office ensures that the Deputy Secretary is kept apprised of our progress on a weekly basis.

Finally, we appreciate the OIG's efforts in this regard. Moving forward we would like to emphasize the importance of immediately notifying the Departmental CISO and the responsible OA of severe or critical security weaknesses identified during audit activities. Such issues should also be reported to the Departmental Cyber Security Management Center as cybersecurity incidents to help ensure they are identified and acted upon as quickly as possible. This will help to ensure that responsible offices are afforded an opportunity to remediate or mitigate a known risk and that Departmental information systems are not operating with known critical vulnerabilities.

If there are questions or need for further clarification on this response, please contact Andrew Orndorff, andrew.orndorff@dot.gov / 202.366.7111.