Office of Inspector General

Audit Report

MULTIPLE DOT OPERATING ADMINISTRATIONS LACK EFFECTIVE INFORMATION SYSTEM DISASTER RECOVERY PLANS AND EXERCISES

Department of Transportation

Report Number: FI-2016-024

Date Issued: March 3, 2016

Memorandum

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

Subject: **ACTION:** Multiple DOT Operating Administrations Lack Effective Information System Disaster Recovery Plans and Exercises
Department of Transportation
Report No. FI-2016-024

Date: March 3, 2016

From: Louis C. King
Assistant Inspector General
for Financial and Information Technology Audits

Reply to Attn. of: JA-20

To: Chief Information Officer

The Department of Transportation (DOT) relies on more than 450 information systems, including air traffic control, communication, and network systems, that provide fundamental capabilities for keeping the Nation's transportation system safe and operational. However, these systems are vulnerable to a variety of disruptions, ranging from mild (short-term power outage, hardware disk drive failure) to severe (equipment destruction, fire). As such, effective disaster recovery planning is critical to maintain information system safety and efficiency for DOT and its Operating Administrations[1] (OAs) in the event of an unexpected event.

The importance of disaster recovery planning was recently underscored in September 2014, when a Federal Aviation Administration (FAA) contract employee deliberately set fire to critical equipment at FAA's Chicago Air Route Traffic Control Center. This was the second time since May 2014 that a fire at a Chicago area air traffic control facility resulted in delays and cancellations of hundreds of flights in and out of O'Hare and Midway international airports.

Given these concerns, we initiated this audit to review the effectiveness of DOT's disaster recovery plans and exercises. Our objectives were to determine whether (1) DOT and its OAs have developed adequate disaster recovery plans for their key information systems and (2) DOT and its OAs conduct effective test exercises of these plans to ensure they will work in the event of a disruption.

[1] See exhibit C for list of DOT Operating Administrations we reviewed.

We conducted our work in accordance with generally accepted Government auditing standards. Exhibit A describes our scope and methodology.

RESULTS IN BRIEF

Several of the Department's OAs have not developed adequate disaster recovery plans for restoring key information systems. Specifically, 4 of the Department's 12 OAs had disaster recovery plans that were not in compliance with DOT policy.[2] For example, one OA did not develop a required Business Impact Analysis (BIA), which helps to determine how critical an information system is to its supported mission and business processes. As a result, this OA cannot effectively determine the impact of potentially losing its systems' operations and plan accordingly. Another OA did not have system data backup processes, which are essential for limiting loss of data during system recovery procedures. Because of these weaknesses, DOT cannot ensure that its OAs can return to normal operations quickly and effectively in the event of an unexpected system disruption.

The Department's OAs do not all conduct effective test exercises of their plans to ensure they will work in the event of a disruption. First, FAA did not conduct annual contingency plan testing for certain high-impact systems, as required. This includes the Web-Based Operations Safety System, which develops, records, and tracks safety responsibilities, and which FAA has deemed mission critical. As a result, it is unclear whether FAA's disaster recovery planning for this system is sufficient. Furthermore, four OAs did not conduct required functional[3] disaster recovery testing to ensure that their systems comply with DOT policy and can effectively handle operations during an unexpected event.

We are making nine recommendations to improve the effectiveness of disaster recovery planning and testing for DOT and its OAs.

SEVERAL OA DISASTER RECOVERY PLANS ARE INADEQUATE AND DO NOT COMPLY WITH DOT POLICY

DOT OAs have not all established effective disaster recovery plans for their information systems. We identified significant weaknesses with the disaster recovery plans of multiple OAs. In particular, the Federal Highway Administration's (FHWA) disaster recovery plans did not comply with key elements of DOT policy.

[2] Departmental Cybersecurity Compendium Supplement to Departmental Cybersecurity Policy.
[3] A functional exercise is a simulation prompting a full recovery and reconstitution of the information system to a known state and ensures that staff are familiar with the alternate facility.

Significant Weaknesses Limit the Effectiveness of OAs' Disaster Recovery Plans

An Information System Contingency Plan (ISCP) is a key element of an OA's disaster recovery plan and establishes procedures for the assessment and recovery of a system following a system disruption. The ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of the recovered system.

ISCPs for 4 of 12 OAs did not meet all DOT policy requirements and contained weaknesses that limit the effectiveness of the plans. Specifically:

- **Unreliable System Backups.** Effectively backing up critical data is an essential aspect of disaster recovery planning, in order to prevent unnecessary data loss during an unexpected event. However, the Federal Motor Carrier Safety Administration (FMCSA) did not include procedures for conducting system backups in the disaster recovery plan for its selected systems. Additionally, the Federal Railroad Administration (FRA) did not perform annual testing of backup information, as required in DOT policy.[4] OAs cannot be sure of the reliability of their backup data media without conducting proper testing.

- **Lack of Alternate Telecommunications Plans.** FMCSA and the Pipeline and Hazardous Materials Safety Administration (PHMSA) did not address alternate telecommunications services in the contingency plan for their selected systems. DOT policy states that systems owners must establish alternate telecommunications services, including necessary agreements, to permit the resumption of information system operations for essential missions and business functions. This lack of information could hinder the resumption of services if staff are not aware of the procedures and agreements for establishing backup telecommunications.

The Federal Highway Administration's Disaster Recovery Plan Does Not Comply With DOT Policy

The Federal Highway Administration's (FHWA) disaster recovery plan is not in compliance with DOT policy. As a result, FHWA cannot ensure that it can return to normal operations quickly and effectively in the event of an emergency. Specifically, both systems we reviewed—the Fiscal Management Information

[4] Departmental Cybersecurity Compendium Supplement to Departmental Cybersecurity Policy.

System (FMIS)[5] and the Rapid Approval and State Payment System (RASPS)[6]—did not comply in the following key areas:

- **Lack of a Business Impact Analysis (BIA).** FHWA has not conducted a BIA for implementing both systems' contingency planning security controls. According to the National Institute of Standards and Technology (NIST),[7] a BIA is a key step in implementing these controls and the first source for determining resiliency and contingency planning strategies.[8] BIA results help an OA determine how critical a system is to the supported mission/business processes, therefore allowing them to plan accordingly for disaster recovery procedures. FHWA officials informed us that they are in the process of developing this BIA.

- **Lack of System Downtime Analysis.** FHWA did not identify system allowable unavailability timelines, such as Maximum Tolerable Downtime (MTD)[9] and Recovery Time Objective (RTO),[10] in both systems' disaster recovery plans. Determining the system's downtime is important because it could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method and (2) the depth of detail that will be required when developing recovery procedures, including their scope and content. FHWA officials informed us that they will develop these timelines via the BIA process.

- **Non-Compliant Backup Storage Location.** DOT policy requires that the system backup data storage site for high-impact systems be located at least 50 miles away from the primary site, which protects the backup site from being susceptible to the same threats and weather-related incidents as the primary site. However, FHWA systems' backup data storage site (12 miles away from the primary site) does not meet this requirement. FHWA informed us that its authorizing official has formally accepted risk for the FHWA systems backup data storage site being 12 miles away from the primary site. Although FHWA's authorizing official accepted the risk for this item, the Agency did not receive a waiver from the DOT CIO office for not complying with DOT cybersecurity policy.

---

[5] FMIS is FHWA's major financial information tracking system and tracks Federal-aid highway projects, by storing highway project data for projects funded with Federal-aid highway money.
[6] RASPS reimburses States for the Federal share of highway construction and highway-related projects.
[7] NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
[8] NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems.
[9] The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations.
[10] RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD.

- **Unencrypted Backup Media.** Backup data storage media for both FHWA mission-critical systems were not encrypted prior to being sent offsite for storage, even though these media contained sensitive security information. By not encrypting backup storage media, FHWA is at risk for potential data theft or unauthorized disclosure of sensitive data.

CONTINGENCY PLAN TESTING IS EITHER NOT OCCURRING OR INSUFFICIENT TO DETERMINE THE EFFECTIVENESS OF THE PLANS

The Department's OAs are not effectively testing their disaster recovery plans. For example, 4 of 12 OAs did not conduct annual contingency plan testing for their selected mission-critical and high-impact systems, as required by DOT policy. A contingency plan contains detailed guidance and procedures for restoring a system after an unplanned shutdown, and must be tested to validate its recovery capabilities. DOT policy requires the Department and its OAs to test and update their system contingency plans at least annually.

For example, FAA did not conduct annual contingency plan testing for two systems in the prior 2 years, 2014 and 2015. We selected the Enhanced Flight Standards Automation System (eFSAS)[11] and Web-based Operations Safety System (Web OPSS)[12] from 97 high or moderate-impact systems scheduled for testing in 2015. These are mission-critical high-impact systems that FAA scheduled for testing during the audit time frame. We planned to witness the disaster recovery exercises for these two systems and determine whether the systems could be recovered successfully. However, FAA officials informed us that the Agency delayed the required contingency plan testing for these two systems for fiscal year 2015 in order to "focus on different priorities."

FAA also did not conduct a functional disaster recovery exercise for either of these high-impact systems in fiscal year 2014 at the Agency's alternate sites, as required. Under a disaster recovery plan, OAs designate an alternate site for transferring information system operations during unexpected events. DOT policy requires that for high-impact systems, system owners must test the contingency plan at the alternate site annually. These tests are important to familiarize contingency personnel with the facility and available resources and to evaluate the alternate site's capabilities to support contingency operations.

[11] eFSAS supports the Flight Standards Service (AFS) by maintaining information on regulated entities such as air carriers, air agencies, designated airmen, and check airmen.
[12] WebOPSS is a mission-critical regulatory system that develops, records, and tracks safety authority from FAA and is required for all commercial air operators and air agencies.

Similarly, FRA did not complete annual contingency plan testing for a moderate-impact system. Specifically, FRA began contingency plan testing for its Railroad Safety Information System—the principal monitoring system for railroad safety—in March 2015, but the test was terminated and has yet to be completed because FRA identified an expired license that prevented further testing.

Two of the OAs, FMCSA and PHMSA, performed contingency plan testing for their selected systems, but only performed a tabletop exercise[13] for these moderate-impact systems, rather than the more thorough functional exercise[14] because they believed tabletop testing of these systems was sufficient. This includes FMCSA's Enforcement Management Information System (EMIS)[15] and PHMSA's Hazardous Materials Information System (HMIS).[16] As a result, these tests were not able to fully determine the effectiveness of the OAs' contingency plans for these systems.

Failure to perform annual functional disaster recovery tests on high- and moderate-impact systems decreases the likelihood that DOT and its OAs will be able to quickly restore system operations in the event of a disaster.

CONCLUSION

Our Nation's transportation systems are vitally important to the economic health and security of our country, and DOT and its OAs are responsible for ensuring safe, secure, and efficient transportation services to all users of our transportation systems. However, ineffective disaster recovery planning and testing can create risks to DOT's transportation information systems and operations that may inhibit its safety mission. To better prepare for potential information system outages and incidents, DOT and its OAs must improve their contingency plan testing procedures to address identified weaknesses and better prepare alternate sites for contingency operations. Until these risks are remediated, the Agency will remain vulnerable to possible lengthy and costly disruptions.

[13] A tabletop exercise is a discussion-based simulation of an emergency situation in an informal, stress-free environment; designed to elicit constructive scenario-based discussions for an examination of the existing ISCP and individual state of preparedness.
[14] Departmental Cybersecurity Compendium Supplement to Departmental Cybersecurity Policy (DOT-CP-4).
[15] EMIS is a moderate-impact system that monitors, tracks, and stores information related to FMCSA enforcement actions.
[16] HMIS is a moderate-impact system that houses all company-specific hazardous materials safety information, which serves as the basis for regulation development and enforcement.

RECOMMENDATIONS

To improve the effectiveness of information systems contingency planning and testing, we recommend that the DOT Chief Information Officer work with OAs to:

1. Develop, document, and implement user and system-level data backup processes for the FMCSA Enforcement Management Information System.

2. Develop, document, and implement user and system-level data backup processes for the FRA Railroad Safety Information System.

3. Specify alternate telecommunications services including necessary agreements for the FMCSA Enforcement Management Information System contingency plan.

4. Specify alternate telecommunications services including necessary agreements for the PHMSA Hazardous Materials Information System contingency plan.

5. Update the contingency plans for the two FHWA systems: (1) Fiscal Management Information System and (2) Rapid Approval and State Payment System (RASPS) by:

    a. Developing a Business Impact Analysis for their two selected systems.

    b. Identifying allowable system unavailability timelines such as Maximum Tolerable Downtime (MTD) and Recovery Time Objective (RTO) for their system contingency plans.

    c. Reevaluating both systems' alternate backup data storage sites so they are geographically dispersed from the primary system operational site as required by DOT policy.

    d. Implementing a process for ensuring the encryption of backup data prior to transferring the data offsite.

6. Conduct annual functional contingency plan testing for FAA systems, including (1) Enhanced Flight Standards Automation System and (2) Web-based Operations Safety System.

7. Conduct annual functional contingency plan testing for the FRA Railroad Safety Information System.

8. Conduct annual functional contingency plan testing for the FMCSA Enforcement Management Information System.

9. Conduct annual functional contingency plan testing for the PHMSA Hazardous Materials Information System.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided the Department with our draft report on January 14, 2016, and received its response on February 8, 2016, which is included as an appendix to this report. The Department concurred with all nine of our recommendations and proposed appropriate corrective actions and target completion dates for seven recommendations. For the remaining two recommendations—recommendations 3 and 4—the Department proposed alternative actions and target completion dates that meet the intent of our recommendations. Accordingly, we consider all recommendations resolved but open pending completion of planned actions.

We appreciate the courtesies and cooperation of the Department and its OA representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-4350, or Kevin Dorsey, Program Director at (202) 366-1518.

#

cc: DOT Audit Liaison, M-1

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted our work from April 2015 through January 2016 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 findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To assess the effectiveness of DOT's information systems' disaster recovery plans and exercises, we focused on two key objectives: to determine whether: (1) DOT and its OAs have developed adequate disaster recovery plans for their key information systems; and (2) DOT and its OAs conduct effective test exercises of these plans to ensure they will work in the event of a disruption.

We coordinated with departmental and OA Chief Information Officers (CIO) and obtained and reviewed the disaster recovery plan and exercises for 13 out of 270 high- and moderate-impact systems. We interviewed OAs' disaster recovery exercise subject matter experts and used document and data analysis to validate the completeness of the planning, testing, and recovery process.

We selected systems[17] based on the following criteria:

- High- and moderate-impact systems.
- Systems from different OAs.
- Schedule of disaster recovery exercises that fit within the survey and verification phases of the audit.

We conducted site visits to observe disaster recovery exercises for selected FHWA and FTA systems. We interviewed FHWA and FTA contingency plan testing teams at the site locations. We also reviewed after-action reports for the system disaster recovery exercises.

[17] See exhibit D for a list of the OA systems we selected and reviewed.

EXHIBIT B. ORGANIZATIONS VISITED OR CONTACTED

We conducted visits to observe disaster recovery exercises at the following sites:

(1) FHWA disaster recovery site visited on March 28, 2015 at Turner Fairbank Highway Research Center (TFHRC), McLean, VA.

(2) FTA recovery site visited on May 2, 2015 at Vienna, VA.

EXHIBIT C. DOT'S OPERATING ADMINISTRATIONS

1. FAA – Federal Aviation Administration
2. FHWA – Federal Highway Administration
3. FMCSA – Federal Motor Carrier Safety Administration
4. FRA – Federal Railroad Administration
5. FTA – Federal Transit Administration
6. MARAD – Maritime Administration
7. NHTSA – National Highway Traffic Safety Administration
8. OIG – Office of Inspector General
9. OST – Office of the Secretary
   (a) OST Volpe Center – Volpe National Transportation Systems Center
10. PHMSA – Pipeline and Hazardous Materials Safety Administration
11. SLSDC – Saint Lawrence Seaway Development Corporation
12. STB[18] – Surface Transportation Board

[18] The Surface Transportation Board is no longer an element of the Department of Transportation. STB Reauthorization Act of 2015 (P.L. 114-110) establishes the STB as a wholly independent Federal agency.

EXHIBIT D. SELECTED OA SYSTEMS REVIEWED IN THIS AUDIT

1. FAA – (a) Enhanced Flight Standards Automation System (eFSAS)
   (b) Web-based Operations Safety System (Web OPSS)
2. FHWA – (a) Fiscal Management Information System (FMIS)
   (b) Rapid Approval and State Payment System (RASPS)
3. FMCSA – Enforcement Management Information System (EMIS)
4. FRA – Railroad Safety Information System (RSIS)
5. FTA – Transportation Electronic Awards and Management System (TEAM)
6. MARAD – Mariner Outreach System (MOS)
7. NHTSA – National Driver Register (NDR)
8. OIG – Infrastructure
9. OST – Office of the Secretary
   (a) Volpe Center– User Accountability System (UAS)
10. PHMSA – Hazardous Materials Information System (HMIS)
11. SLSDC – Financial Management System (FMS)
12. STB – Surface Transportation Board

EXHIBIT E. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Kevin Dorsey	Program Director
James Mallow	Project Manager
Nileshkumar Patel	Information Technology Specialist
Jason Mott	Information Technology Specialist
Audre Azuolas	Writer-Editor

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

Memorandum

Subject: **INFORMATION:** Management Comments – Office of Inspector General (OIG) Draft Report on Disaster Recovery Plans and Exercises

Date: February 8, 2016

From: Richard McKinney
DOT Chief Information Officer

KRISTEN K. BALDWIN
Digitally signed by KRISTEN K. BALDWIN
DN: c=US, o=U.S. Government, ou=DOT Headquarters, ou=OSTHQ, cn=KRISTEN K. BALDWIN
Date: 2016.02.08 16:57:06 -05'00'

Reply to Attn. of:

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

In fiscal year (FY) 2015 and FY 2016, the Department of Transportation (DOT) Chief Information Officer (CIO) prioritized funding for the expansion of data center facilities at DOT headquarters, to assess a portion of agency networks for optimization and enhancement and to migrate critical infrastructure services to a FedRAMP-authorized cloud service provider capable of providing improved security and availability. These investments and actions are reflective of the DOT CIO's imperative to improve the security and availability of DOT information systems and services, and to do so in ways that are efficient, cost effective and reduce overall agency risk.

Based upon our review of the draft report, we concur with the following recommendations as written: 1, 2, 5, 6, 7, 8, and 9. Our target action date for completing these recommendations is December 31, 2016.

For recommendations 3 and 4, we propose to address the identified weaknesses by coordinating with FMCSA and PHMSA to implement a solution that is consistent with DOT planning for data center consolidation, secure Internet access, shared services and infrastructure operations strategy, and an optimized DOT network infrastructure. As budgetary resources have not been requested for these requirements, network assessment activities are not scheduled to finish until the end of the third quarter of FY 2016. Typical lead-times for provisioning new network services are 90 to120 days from the availability of requirements and funding. As a result, our target action date for completing these two recommendations is June 30, 2017.

We appreciate the opportunity to comment on OIG's draft report. If you have any questions or need clarifications, please feel free to contact Andrew Orndorff andrew.orndorff@dot.gov, 202-366-9201 or Sherri Ellis, sherri.ellis@dot.gov, 202-366-1471.