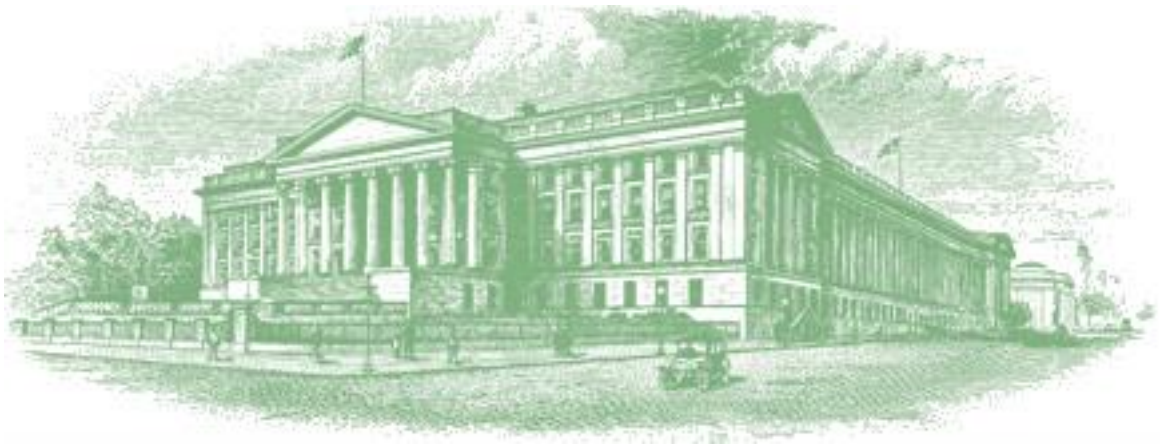
Audit Report



OIG-16-003

INFORMATION TECHNOLOGY: Debit Gateway's Disaster Recovery Exercise Experienced Delays

November 6, 2015

Office of Inspector General

Department of the Treasury

Contents

Audit Report

Appendices

Abbreviations and Acronyms

contingency plan	Debit Gateway Information Technology Contingency Plan
DRE	Disaster Recovery Exercise
Fiscal Service	Bureau of the Fiscal Service
IT	Information Technology
MTD	Maximum Tolerable Downtime
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
RTO	Recovery Time Objective
SP	Special Publication
Treasury	Department of the Treasury
TWAI	Treasury Web Application Infrastructure

This Page Intentionally Left Blank

The Department of the Treasury
Office of Inspector General

November 6, 2015

Sheryl Morrow
Commissioner, Bureau of the Fiscal Service

This report represents the results of our audit of the disaster recovery exercise (DRE) for Debit Gateway conducted jointly by the Bureau of the Fiscal Service (Fiscal Service), Federal Reserve Information Technology,[1] and its contractor, Hewlett-Packard, on February 21, 2015, and March 7, 2015. We performed this audit as part of our ongoing audit oversight of the Department of the Treasury's (Treasury) compliance with the *Federal Information Security Modernization Act of 2014*, which requires each Federal agency to provide information security for information and information systems, including plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. In this regard, we perform periodic audits of DREs and related contingency planning controls at Treasury bureaus and offices. The objectives of this audit were to assess whether Fiscal Service provided adequate contingency planning controls and demonstrated successful recovery of Debit Gateway for operations in the event of a disaster.

To accomplish our audit objectives, we chose Fiscal Service because of the monetary value of transactions it handled. From the list of Fiscal Service's DREs planned for fiscal year 2015, we selected Debit Gateway based on its categorization as a

[1] Federal Reserve Information Technology is a national information technology (IT) service provider within the Federal Reserve System providing a variety of services, including project services, enterprise IT architecture, information security policy, and assurance service.

high-impact system.[2] We observed the DRE at the Federal Reserve Bank of Dallas, Texas, during February 2015 and March 2015. Appendix 1 provides more detail on our objectives, scope, and methodology.

Results in Brief

Fiscal Service provided sufficient contingency planning controls in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34,[3] and demonstrated successful recovery and reconstitution[4] of Debit Gateway for operations in the event of a disaster. However, due to database synchronization failures and memory allocation misconfiguration, neither recovery nor reconstitution met the recovery time objective (RTO) established in the business impact analysis contained in Fiscal Service's *Debit Gateway Information Technology Contingency Plan* (contingency plan).

The root cause for the delays was not identified at the time of the exercise, and therefore, Fiscal Service was not able to document the technical issues in the Plan of Action and Milestones (POA&M). In addition, Fiscal Service established the RTO for specific hours during weekdays only and not for all hours of the day including weekend days or other weekday hours. Furthermore, Fiscal Service did not establish the maximum tolerable downtime (MTD) necessary for establishing the appropriate RTO as required by NIST SP 800-34.

[2] Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004), establishes security categories (high, moderate, low) for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its mission.
[3] NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (May 2010).
[4] Recovery is executing information system contingency plan activities to restore essential missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation including an assessment of the fully restored information system capability and preparing for future disruptions.

We are making two recommendations to management to address the deficiencies identified. First, we recommend that management ensure that the root causes of the automatic database synchronization failures and memory allocation misconfiguration are identified and documented in the POA&M for remediation. We also recommend that management ensure that the MTD is defined so that an appropriate RTO can be established for all hours. Both the MTD and RTO should be documented in the Fiscal Service's contingency plan in accordance with NIST SP 800-34.

In a written response, management agreed with our finding and recommendations and noted that it has developed remediation plans to address each recommendation by January 31, 2016. Overall, management's response meets the intent of our recommendations. We have summarized and evaluated management's response in the recommendation sections of this report. Management's response is provided in appendix 2.

Background

Fiscal Service's mission is to promote the financial integrity and operational efficiency of the Federal government through exceptional accounting, financing, collections, payments, and shared services. Fiscal Service uses Debit Gateway, among other applications in the Treasury Web Application Infrastructure (TWAI) environment, to accomplish this mission.

Fiscal Service is the business owner of Debit Gateway, which is used to process electronic check and Automated Clearing House debit transactions received from other Fiscal Service systems and Federal agencies, and deposit of funds into Treasury. The Debit Gateway production application runs in the TWAI environment that has a primary site at the Dallas Operations Center in the Federal Reserve Bank of Dallas, Texas, and a secondary site at the East Rutherford Operations Center in East Rutherford, New Jersey. In the event of a primary site failure, processing for the Debit Gateway production application is relocated to the secondary site. Data replication of the application and the database, along with additional backups, are used to facilitate the recovery.

The Debit Gateway DRE was conducted in two phases. The recovery phase, conducted on February 21, 2015, simulated a disaster that forced relocation of Debit Gateway processing from its primary site to its secondary site. The reconstitution phase, conducted on March 7, 2015, returned operation back to the primary site.

Results of Audit

Finding 1 Recovery and Reconstitution of Debit Gateway Did Not Meet the Recovery Time Objective

During the DRE of Debit Gateway, both the recovery and the reconstitution did not meet the RTO as specified in Fiscal Service's contingency plan. That is, the recovery was completed in 4 hours 10 minutes, while the reconstitution was completed in 5 hours 20 minutes. According to the RTO defined in the contingency plan, each phase is limited to 2 hours for completion. The root cause of the delays was not identified at the time of the exercise, and therefore, Fiscal Service was not able to document the technical issues in the POA&M. In addition, Fiscal Service defined the RTO in its contingency plan for weekday hours after 4:00 p.m. and did not address the RTO for other weekday hours or weekends. Moreover, Fiscal Service did not define the MTD in the contingency plan, which should have been established in order to determine the appropriate upper limit of the RTO.

As defined by NIST SP 800-34, Revision 1, the RTO is the maximum amount of time a system can be unavailable before there is an unacceptable impact on other system resources, mission and business processes, and the system's MTD. The MTD represents the total amount of outage or disruption time including all impact considerations that the system owner or authorizing official is willing to accept. Determining MTD is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content. Because the RTO must ensure that the MTD is not

exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.

Fiscal Service's management stated that Debit Gateway was not recovered or reconstituted within the RTO because it experienced technical issues with automatic database synchronization and system memory allocation.[5] That is, the automatic synchronization of databases between the primary and secondary processing sites failed, causing the recovery to suspend. After identifying the failure, Fiscal Service staff performed a manual database synchronization allowing the recovery to resume. The recovery then experienced another delay due to insufficient memory allocation for the system that supports Debit Gateway. The system was reconfigured to allocate more memory, which allowed staff to complete recovery of Debit Gateway. Two (2) weeks later, during the reconstitution phase, Fiscal Service experienced yet another delay as a result of the automatic synchronization failure. This failure was also resolved manually. Fiscal Service staff was unable to identify the root cause for the automatic synchronization problem.

In the event of a real disaster, the recovery and reconstitution of Debit Gateway would not have met the RTO, triggering a break in business continuity. As a result, the system would not have been able to process transactions in a timely manner and possibly cause irreversible impact to Fiscal Service's business. Furthermore, if the RTO is only defined for specific hours during weekdays, there is no time limit to recover and reconstitute Debit Gateway in the event of a real disaster during the non-specified times. Without establishing the MTD to determine the appropriate RTO, Fiscal Service management will not know the acceptable outage time for Debit Gateway's business function

[5] Data synchronization is a process of establishing consistency among systems and subsequent continuous updates to maintain consistency. Memory allocation is the process of assigning a block of memory where a program can store its data.

to be unavailable. Finally, management may not be able to track and remediate weaknesses timely since the technical issues causing the DRE delays were not documented in the POA&M.

Recommendations

We recommend that the Commissioner of the Bureau of the Fiscal Service do the following:

1. Ensure that the root causes of the automatic database synchronization failures and memory allocation misconfiguration are identified and documented in the POA&M for remediation.

   Management Response

   In a written response, Fiscal Service management agreed with the recommendation and noted that it has developed a remediation plan to address the root causes of the database synchronization failures and the memory allocation misconfiguration. Management also acknowledged that the failures and misconfiguration caused the Debit Gateway's extended recovery times on February 21, 2015, and March 7, 2015, respectively, but believes the root causes of both issues have now been identified and remediated.

   Debit Gateway scheduled another DRE for August 29, 2015 – September 12, 2015, to validate the effectiveness of the remediation steps taken and saw no recurrence of the issues from the February–March DRE. Management plans to use the final report from the August—September DRE to confirm the results. Management stated that the remediation plan will address this recommendation by January 31, 2016.

   OIG Comment

   Management's response meets the intent of our recommendation.

2. Ensure that the MTD is defined so that an appropriate RTO can be established for all hours of the day. Both the MTD and RTO should be documented in the Fiscal Service's contingency plan in accordance with NIST SP 800-34.

Management Response

Fiscal Service management agreed with the recommendation and noted that it has developed a remediation plan to document in the contingency plan an appropriate MTD for the collection function. According to management, the MTD will reflect the total outage time the Debit Gateway is willing to accept when all impacts are considered within the Fiscal Service chain of collection, settlement, and reporting applications (including impact on upstream collection channels and downstream payment system interfaces).

With respect to the RTO, the contingency plan was updated on August 21, 2015, to define the RTO as 2 hours at all times. This RTO was used to evaluate the August–September DRE.

Management stated that the remediation plan will address this recommendation by January 31, 2016.

OIG Comment

Management's response meets the intent of our recommendation.

* * * * * *

I would like to extend my appreciation to the Fiscal Service staff for the cooperation and courtesies extended to my staff during the audit. If you have any questions, please contact me at 202-927-5171 or Dan Jensen, Audit Manager, at 202-927-8120. Major contributors to this report are listed in appendix 3.

/s/

Tram Jacquelyn Dang
Director, Information Technology Audit

To support our on-going audits of *Federal Information Security Modernization Act of 2014*, we perform periodic audits of disaster recovery exercises (DRE) conducted by the Department of the Treasury's (Treasury) bureaus and offices. In this regard, we initiated an audit of the DRE and related contingency planning controls for the Bureau of the Fiscal Service's (Fiscal Service) Debit Gateway application in December 2014. The objectives of this audit were to assess whether Fiscal Service provided adequate contingency planning controls and demonstrated successful recovery of Debit Gateway for operations in the event of a disaster.

As part of the audit, we chose Fiscal Service because of the monetary value of transactions it handled. From the list of Fiscal Service DREs planned for fiscal year 2015, we selected Debit Gateway based on its categorization as a high-impact system.[6] We observed the DRE, including the recovery and reconstitution of Debit Gateway, at the Federal Reserve Bank of Dallas, Texas. While there, we interviewed key officials and personnel to include, but not limited to, the Treasury Web Application Infrastructure Program Manager at Fiscal Service, a Production Engineer for Treasury Services at Federal Reserve Information Technology, and the Business Continuity Manager at Hewlett-Packard. We also reviewed and analyzed contingency planning documentation, including contingency plans, system security plans, and business impact analyses.

We applied relevant criteria to include, but not limited to, National Institute of Standards and Technology Special Publications as well as Treasury's and Fiscal Service's policies and procedures. We performed our fieldwork primarily at the Federal Reserve Bank of Dallas, Texas, between February 2015 and March 2015.

[6] Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004), establishes security categories for both information and information systems. The security categories are based on the potential impact (high, moderate, or low) on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission.

We conducted this performance 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 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.

DEPARTMENT OF THE TREASURY
BUREAU OF THE FISCAL SERVICE
WASHINGTON, DC 20227

COMMISSIONER

September 15, 2015

Ms. Tram Dang
Director, IT Audit
U.S. Department of the Treasury
Office of the Inspector General
JBAB Building 410/Door 123
250 Murray Lane, SW
Washington, DC 20222

Dear Ms. Dang:

Thank you for the opportunity to respond to the draft audit report "Debit Gateway's Disaster Recovery Exercise Experienced Delays", dated August 21, 2015. Fiscal Service agrees with the finding and its two (2) associated recommendations. Our responses are as follows:

Management Response to Debit Gateway's Disaster Recovery Exercise Experienced Delays

Finding 1: Recovery and Reconstitution of Debit Gateway Did Not Meet the Recovery Time Objective (RTO)

Management Response

Fiscal Service agrees with the finding and has developed a remediation plan to address each recommendation by January 31, 2016.

Recommendation 1: Ensure that the root causes of the automatic database synchronization failures and memory allocation misconfiguration are identified and documented in the POA&M for remediation.

Management Response

Fiscal Service agrees with the recommendation and has developed a remediation plan to address the root causes of the database synchronization failures and the memory allocation misconfiguration. The failures and misconfiguration caused the Debit Gateway's extended recovery times on February 21, 2015 and March 7, 2015 respectively. The Fiscal Service believes the root causes of both issues have now been identified and remediated. Debit Gateway scheduled another disaster recovery exercise (DRE) for August 29, 2015 – September 12, 2015, to validate the effectiveness of the remediation steps taken and saw no recurrence of the issues from the February-March DRE. The final report from the DRE, expected by early-November 2015, will be used to confirm the results.

Recommendation 2: Ensure that the MTD is defined so that an appropriate RTO can be established for all hours of the day. Both the MTD and RTO should be documented in the Debit Gateway contingency plan in accordance with NIST SP 800-34.

Management Response

Fiscal Service agrees with the recommendation and has developed a remediation plan to document in the Debit Gateway's Information System Contingency Plan (ISCP) an appropriate maximum tolerable downtime (MTD) for the collection function, within which Debit Gateway is a critical settlement system. The MTD will reflect the total outage time the Debit Gateway is willing to accept when all impacts are considered within the Fiscal Service chain of collection, settlement and reporting applications (including impact on upstream collection channels and downstream payment system interfaces).

With respect to the Recovery Time Objective (RTO), Debit Gateway's ISCP was updated August 21, 2015, to define the RTO as two (2) hours at all times. This RTO is being used to evaluate the August 29, 2015 – September 12, 2015 DRE, which met the RTO pending confirmation in final reporting.

Sincerely,

for Sheryl R. Morrow
Commissioner

Page 2

Information Technology (IT) Audit

Tram J. Dang, Director
Dan Jensen, Audit Manager
Robert Kohn, Auditor-in-Charge
Jason Beckwith, IT Specialist
Don'te Kelley, IT Specialist
John Tomasetti, Referencer

Department of the Treasury

Deputy Secretary
Assistant Secretary for Management
Deputy Assistant Secretary for Information Systems and Chief Information Officer
Office of Strategic Planning and Performance Management
Office of Deputy Chief Financial Officer, Risk and Control Group

Bureau of the Fiscal Service

Commissioner
Chief Internal Control Officer

Office of Management and Budget

OIG Budget Examiner

Treasury OIG Website

Access Treasury OIG reports and other information online:
http://www.treasury.gov/about/organizational-structure/ig/Pages/default.aspx

Report Waste, Fraud, and Abuse

OIG Hotline for Treasury Programs and Operations – Call toll free: 1-800-359-3898
Gulf Coast Restoration Hotline – Call toll free: 1-855-584.GULF (4853)
Email: Hotline@oig.treas.gov
Submit a complaint using our online form:
https://www.treasury.gov/about/organizational-structure/ig/Pages/OigOnlineHotlineForm.aspx