OFFICE OF INSPECTOR GENERAL

Audit Report 2015-IT-B-001

Audit of Planned Physical and Environmental Controls for the Board's Data Center Relocation

January 30, 2015

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

Report Contributors

Adam Scheps, Project Lead and IT Auditor
Alison Sarfati, IT Audit Intern
Peter Sheridan, Senior OIG Manager for Information Technology Audits
Andrew Patchan Jr., Associate Inspector General for Information Technology

Abbreviations

A/E	architectural and engineering
BISP	*Board Information Security Program*
Board	Board of Governors of the Federal Reserve System
Division of IT	Division of Information Technology
FRB Richmond	Federal Reserve Bank of Richmond
ISO	Information Security Officer
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
PE	physical and environmental
RBOPS	Division of Reserve Bank Operations and Payment Systems
SAFR	*Security Assurance for the Federal Reserve*
SP 800-53	Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

Executive Summary:

Audit of Planned Physical and Environmental Controls for the Board's Data Center Relocation

2015-IT-B-001 January 30, 2015

Purpose

The Board of Governors of the Federal Reserve System (Board) has undertaken a project to relocate its data center from the Board's Martin Building in Washington, DC, to the Baltimore Branch of the Federal Reserve Bank of Richmond. Given the magnitude and significance of the project, we plan to monitor it as the project continues through 2015. We issued our initial report on the data center relocation in February 2014. The objective of this second audit was to review the planned physical and environmental controls for the data center. We also reviewed the change order and procurement processes and followed up on the budget and project schedule recommendations from the initial audit. We plan to issue subsequent reports at key future dates.

Background

The Board's data center relocation is a major element of the third theme in the Board's *Strategic Framework 2012–15*. The Board plans to completely renovate the Martin Building, where the data center currently resides. The multiyear data center project is composed of four overlapping phases, with completion scheduled for December 2015. Construction of the new data center was underway as of the end of our fieldwork. The Board approved an overall budget of $201.5 million for the project and established a high-level timeline for the project.

Findings

Overall, we observed that the Board is continuing to follow a structured approach to planning and executing the relocation of the data center, and Board staff are actively engaged in the planning and decisionmaking for the project. Specifically, we found that the tracking and monitoring of the budget has improved since our previous audit, and the budget has been updated to reflect the information currently available regarding actual costs. The Division of Information Technology has taken steps to monitor the timeline closely and to update the Chief Operating Officer about the project and delays that have occurred.

We found that the Board still needs to ensure that all physical and environmental controls will be implemented in accordance with Board requirements. Prior to the relocation, the Board's data center must be authorized to operate based on a security package that includes a system security plan and risk assessment, in accordance with the *Board Information Security Program*.

Our February 2014 audit report included two recommendations, one regarding the data center relocation project budget and the other regarding the project schedule. As part of this second audit, we followed up on these recommendations and determined that the budget recommendation can be closed but that the schedule recommendation remains open.

Recommendation

We recommend that the Director of the Division of Information Technology compare the Board's control baselines and planned controls for the data center with the Federal Reserve System's requirements and baselines, document the planned controls in a security plan, and conduct a risk assessment to formally accept or facilitate the mitigation of any identified risks or deviations from Board requirements.

The Director of the Division of Information Technology agreed with the recommendation and outlined the actions that the division is taking to address the recommendation. We plan to follow up on the division's actions to ensure that the recommendation is fully addressed.

Summary of Recommendation, OIG Report No. 2015-IT-B-001

Rec. no.	Report page no.	Recommendation	Responsible office
1	5	Compare the Board's control baselines and planned controls for the data center with the Federal Reserve System's requirements and baselines, document the planned controls in a security plan, and conduct a risk assessment to formally accept or facilitate the mitigation of any identified risks or deviations from Board requirements.	Division of Information Technology

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

January 30, 2015

MEMORANDUM

TO: Sharon Mowry
Chief Information Officer and Director, Division of Information Technology
Board of Governors of the Federal Reserve System

FROM: Andrew Patchan Jr.
Associate Inspector General for Information Technology

SUBJECT: OIG Report No. 2015-IT-B-001: *Audit of Planned Physical and Environmental Controls for the Board's Data Center Relocation*

The Office of Inspector General has completed its report on the subject audit. This audit is a follow-on to OIG Report No. 2014-IT-B-002, *Audit of the Board's Data Center Relocation*, February 7, 2014. The objective of this second audit was to review the planned physical and environmental controls for the data center. We also reviewed the change order and procurement processes and followed up on the budget and project schedule recommendations from the February 2014 audit. Given the magnitude and significance of the data center relocation project, we plan to monitor the Board's data center relocation as the project continues through 2015.

We provided a draft of our report for review and comment. In your response, you outlined actions that will be taken to address our recommendation. We have included your response as appendix B to our report.

We appreciate the cooperation that we received from Board personnel during our audit. Please contact me if you would like to discuss this report or any related issues.

cc: Donald Hammond, Chief Operating Officer
William Mitchell, Chief Financial Officer
Michell Clark, Director, Management Division
Raymond Romero, Associate Director, Division of IT
Glenn Eskow, Deputy Associate Director, Division of IT
Jonathan Shrier, Manager, Division of IT
Charles Young, Information Security Officer
J. Anthony Ogden, Deputy Inspector General
Matthew Simber, OIG Manager for Policy, Planning, and Quality Assurance

Contents

Introduction

Objective

The Board of Governors of the Federal Reserve System's (Board) project to relocate its data center is a major element of the third theme in the Board's *Strategic Framework 2012–15*. This multiyear project is composed of four overlapping phases, with completion scheduled for December 2015. Given the project's magnitude and significance, the Office of Inspector General (OIG) plans to monitor the Board's data center relocation as the project continues through 2015. We issued our initial report on the data center relocation in February 2014.[1]

The objective of this second audit was to review the planned physical and environmental (PE) controls identified in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (SP 800-53), for the data center as well as the change order and procurement processes. We also followed up on the budget and project schedule recommendations from the initial report. We plan to issue subsequent reports at key future dates.

Background

The Board's data center provides the infrastructure that makes data and information technology available to the Board and to the Federal Reserve System to support monetary policy, financial supervision, consumer protection, and economic research. The data center currently resides in the Board's Martin Building, which the Board plans to completely renovate. After considering its options, the Board decided to relocate the data center to the Baltimore Branch of the Federal Reserve Bank of Richmond (FRB Richmond). The Board approved the scope and funding for this option in June 2012 as part of the Board's strategic plan.

The approved funding for the project, which is intended to cover all costs associated with building, migrating, and operating the data center for 10 years, is $201.5 million. This amount was allocated into three high-level categories:

- $33.6 million for design and construction
- $28.5 million for transition and migration
- $139.3 for operations[2]

According to the January 2013 memorandum of understanding between the Board and FRB Richmond, FRB Richmond is responsible for the build-out of the data center. The Board also subsequently delegated to FRB Richmond responsibility for designing and implementing PE controls. The Board's PE control requirements are documented in the *Board Information Security*

1. Office of Inspector General, *Audit of the Board's Data Center Relocation*, OIG Report No. 2014-IT-B-002, February 7, 2014. This initial report contains additional background information on the data center relocation project.

2. Figures do not total to $201.5 million due to rounding.

Program (BISP), and PE control requirements for the Federal Reserve Banks, including FRB Richmond, are outlined in the Federal Reserve System's *Security Assurance for the Federal Reserve* (SAFR) program. Construction of the data center was underway as of the end of our fieldwork.

PE controls are measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. FRB Richmond is responsible for providing all the low and moderate controls identified in the NIST SP 800-53 PE control family. Such controls include the following:

- protection of the physical facility housing the system and network components from physical threats, such as fire, roof leaks, and unauthorized access

- protection from the general geographic operating location, including
  - natural threats, such as floods
  - man-made threats, such as burglary
  - damaging nearby activities, such as toxic spills

- controls associated with supporting facilities and services that support operation of the system, such as electricity and heating and air conditioning

The planned PE controls for the data center were designed by the architectural and engineering (A/E) vendor and FRB Richmond, with oversight by the Board.

Finding 1: The Board Needs to Reconcile the PE Controls Provided by FRB Richmond With Board Requirements

The Board is relying on FRB Richmond to provide all low and moderate PE controls for the data center and to provide for their ongoing review; however, the Board has not confirmed that the implementation of the controls provided by FRB Richmond will meet Board requirements. In addition, to meet Board requirements, a security plan must be created for the data center and a risk assessment must be conducted. The BISP states that information system owners are responsible for the development and maintenance of a system security plan and that all Board information systems must undergo a formal risk assessment. Further, the Federal Information Security Management Act of 2002[3] requires agencies to develop, document, and implement an enterprise-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, a contractor, or other source. To meet this requirement, the Board's Information Security Officer (ISO) has signed two memorandums, relying on the Division of Reserve Bank Operations and Payment Systems' (RBOPS) reviews of the Baltimore facility and on FRB Richmond's implementation of the SAFR program's controls. While both the BISP and the SAFR program are built on NIST SP 800-53, implementation of each program's standards can differ. The ISO, who is ultimately responsible for maintaining the appropriate operational security posture, must ensure that the controls meet the Board's own requirements, that compensating controls have been designed, or that the risk has been accepted.

Analysis of Controls Provided Through Reliance Memorandums

In December 2013, the ISO issued a memorandum indicating that he was relying on RBOPS's review of the building and physical security controls associated with the Baltimore Branch of FRB Richmond and that a separate Federal Information Security Management Act of 2002 review would not be required. RBOPS conducts periodic reviews to ensure that the Reserve Banks are complying with the Board's guidelines. While the RBOPS review is not conducted based on NIST SP 800-53, at the request of the Division of Information Technology (Division of IT), RBOPS reconciled its review with the SP 800-53 controls. RBOPS determined that while its review did not cover all PE controls, it did encompass PE protection policy and procedures, physical access authorizations, physical access control, monitoring physical access, and access records (NIST SP 800-53 controls PE-1, 2, 3, 6, and 8, respectively). The ISO's reliance on RBOPS, therefore, was limited to building and physical security controls focused on the current, existing physical structure, current right of ways, visible and nonvisible perimeter security assemblies and barriers, access controls (internal and external), and visitor registration processes.

For assurance that all PE controls will be implemented, in April 2014, the ISO issued a second memorandum indicating that he would rely on FRB Richmond's implementation of SAFR, which includes both the implementation and periodic assessment of the required PE controls. The memorandum states that FRB Richmond is responsible for providing all low and moderate controls identified in the PE control family. However, there are differences between SAFR requirements and BISP requirements. The ISO further stated that the Board reserves the right to

3. Title III, Public Law 107-347 (December 17, 2002).

review FRB Richmond's documentation, including its *Security Plan*, which documents how FRB Richmond supports the PE controls, and its *Security Assessment Reports* regarding the PE controls. As the *Security Assessment Reports* will be conducted using SAFR criteria, SAFR requirements should be reconciled with BISP requirements to ensure that the SAFR review of the controls will also certify compliance with Board criteria.

While both programs are built on NIST SP 800-53, implementation of each program's standards can differ. For example, NIST SP 800-53 includes a control for monitoring physical access, PE-6. This control leaves the frequency of monitoring open to organizationally defined time frames. The BISP's baselines require monthly reviews, but the SAFR program only requires quarterly reviews. While FRB Richmond can implement controls, the ISO must still ensure that the controls meet the Board's own requirements, implement compensating controls, or accept the risk.

Development of a Security Plan

While the PE controls for the data center have been planned, a security plan had not been documented at the close of our fieldwork. Documenting the controls for the data center will assist in comparing BISP requirements with SAFR requirements to ensure that all planned controls will ultimately meet Board requirements.

The BISP requires that system security plans be developed for all information systems that fully describe the security environment of the information system. The security plan acts as the central reference for how information systems implement required and supplemental security controls and for the acceptance of residual risk. The information system owner is responsible for the development and maintenance of a system security plan.

PE controls have been designed for the data center with input from the Board, FRB Richmond, and the A/E firm, but they have not been consolidated into a security plan. In September 2012, the Division of IT issued *Data Center Design Guidelines* to outline potential controls for the new data center. This document was then used by the Board in October 2012 to create the *Data Center High Level Requirements* document. Subsequently, the *Data Center High Level Requirements* document was provided to the A/E firm, which in September 2013 developed the *Facility and Infrastructure Design Criteria Program*. This document contains the specific planned design elements for the new data center.

Completion of a Risk Assessment

The BISP requires that all information systems undergo a formal risk assessment based on NIST standards. This formal risk assessment determines the information security controls that are needed beyond the security control baselines to ensure that the security implemented in the information system is commensurate with the risk and magnitude of harm that can result from the loss, misuse, unauthorized access to, or modification of information generated, stored, or processed by the information system. Each vulnerability must be evaluated to determine whether the risk to the Board can be justifiably accepted or, if the risk is unacceptable, how the risk can be reduced.

As it applies to the data center, the risk assessment should be used to evaluate the planned PE controls and to assess and accept or mitigate risks resulting from differences between SAFR and

BISP requirements. Based on the residual risk, the information owner should decide whether additional controls need to be implemented to lower the residual risk to an acceptable level.

Further, the risk assessment should be used to obtain system owner approval for major security control decisions. For example, the original *Data Center Design Guidelines* called for a gaseous and a water-based fire suppression system, but the A/E firm later recommended installing only a dry-pipe, water-based fire suppression system. This recommendation was discussed at length among the project management personnel from the Board and FRB Richmond and was ultimately accepted. While the decision was discussed among the project team and documented, if the team determined that there is a resulting risk, that risk should be documented in a risk assessment and formally accepted by the system owner.

There are risks associated with a water-based fire suppression system, such as damage to equipment, and we also noted that the system will not be linked with the emergency power-off function to automatically stop the flow of electricity in the event of a fire. The data center project team discussed this issue at length and ultimately decided to maintain the two systems as independent entities. If this selection poses risk, this decision should also be documented in a risk assessment and formally accepted by the system owner.

The ISO stated that the formal system security plan and risk assessment process is planned to be completed prior to signing an authorization to operate. Subsequent to our fieldwork, Board staff began to develop a spreadsheet that identifies how the data center will meet each PE control in the BISP. This spreadsheet includes the BISP PE control baseline and responses from the Board, RBOPS, and FRB Richmond regarding how each individual control will be met. It also lists the artifacts that will be available for corroboration.

Recommendation

We recommend that the Director of the Division of IT

1. Compare the Board's control baselines and planned controls for the data center with the Federal Reserve System's requirements and baselines, document the planned controls in a security plan, and conduct a risk assessment to formally accept or facilitate the mitigation of any identified risks or deviations from Board requirements.

Management's Response

The Director of the Division of IT agreed with our recommendation, outlined corrective actions taken to compare the implementations to the Board's security requirements, and stated that the Board's ISO will work with the 5th District to address identified risks and ensure the controls are appropriately documented in a security plan.

OIG Comment

In our opinion, the actions described by the Director are responsive to our recommendation. We plan to follow up on the division's actions to ensure that the recommendation is fully addressed.

Follow-Up on Prior Audit Recommendations

Our February 2014 audit report included two recommendations, one regarding the data center relocation project budget and the other regarding the project schedule. The Director of the Division of IT agreed with our recommendations and outlined actions to address them. As part of this audit, we followed up on these recommendations and determined that the budget recommendation can be closed but that the schedule recommendation remains open. The results of our follow-up work are below.

Budget Recommendation

In our February 2014 audit report, we recommended that the Director of the Division of IT reevaluate the data center relocation budget, taking into consideration the design changes that have occurred, and implement a process for updating the budget as additional cost information is available. We further recommended that the updated budget clearly separate build-out and operations expenses to allow for separate tracking and monitoring through the duration of the project.

The overall budget remains $201.5 million, as this was the funding amount approved by the Board of Governors. We found that the tracking and monitoring of this budget has improved since our initial report and that figures have been adjusted to reflect updated information regarding actual costs. As a result of actions taken, we are closing this recommendation. We will continue to monitor the budget to ensure appropriate tracking and monitoring through the build-out phase of the project.

Initially, the Management Division was responsible for maintaining the Master Tracker, a document that consolidates all projected expenses to be charged against the total $201.5 million 10-year budget, including design and construction, transition and migration, and operations expenses. Responsibility for this tracker transitioned to the Division of IT, and expenses have been updated to reflect the design changes and the new cost information that has become available, such as the actual cost of the contract with the general contractor and the price of the increased lease space. As of the end of our fieldwork, the Master Tracker showed that both the overall data center relocation project and the design and construction component were under budget.

In addition to the Board's Master Tracker, FRB Richmond is maintaining a project cost estimate tracker to monitor spending toward its allotted build-out budget. This document contains current build-out expenses, including FRB Richmond's project management fees and prepurchased equipment, design and contract administration fees, general contractor fees, commissioning costs, and change order costs. The Board's Management Division also maintains its own tracking of build-out costs and uses data from FRB Richmond to assist in this tracking.

By delegating responsibility for the Master Tracker to the Division of IT, the Management Division's responsibility is reduced to monitoring only costs toward the build-out budget, which

is the sole portion of the budget that the Management Division is responsible for meeting. Further, we found that, separate from the $201.5 million operating budget, the Board also approved a $34.8 million multiyear capital budget. Ten years of depreciation on this $34.8 million flows into and is included as part of the $201.5 million operating budget.

While expense tracking has improved and the Board was under budget at the close of our fieldwork, we noted that change orders have increased expenses and may continue to do so. We found that the project is following an appropriate change order and procurement process, including reviews, approvals, and tracking; however, future change orders will continue to increase expenses and could bring the project over budget.

Project Schedule Recommendation

In our February 2014 audit report, we recommended that the Director of the Division of IT continue to closely monitor data center relocation project schedule risks and identify and analyze possible approaches for responding to potential delays that could affect the Martin Building renovation project.

We observed that the Division of IT has taken steps to monitor the timeline closely and to update the Chief Operating Officer to ensure that interdependencies are known and mitigated; however, we are keeping our recommendation open while the project remains active.

The Chief Operating Officer is provided with a *Capital Construction Update* report every other month, which contains updates on the Martin Building renovation and the 1801 K Street, New York Avenue, and data center relocation projects. This report contains a timeline that compares all four projects and makes specific note of the six-month overlap between the start of the Martin Building construction and the end of the data center relocation.

Despite the enhanced monitoring and progress reporting in place, we remain concerned about the timeline due to (1) the six-month overlap and (2) construction delays that have occurred. The original closeout date for the construction phase was July 14, 2014. However, in March 2014, this date was pushed back to November 2014 due to permitting delays with the Maryland Department of the Environment. In June 2014, the closeout date was delayed to December 2014 due to vendor issues with the chiller equipment. According to Board project management, the overall project schedule still has a projected December 2015 completion date despite these delays because project management had built slack time into subsequent phases of the project. However, project management has noted that further delays could jeopardize this completion date. Such delays could impact the Martin Building renovation project schedule and could also increase costs for the data center relocation project. The Board should continue to closely monitor the status of the timeline as the project continues.

Appendix A
Scope and Methodology

The scope of this second audit of the data center relocation included reviewing the planned PE controls for the data center, reviewing the change order and procurement processes, and following up on the budget and project schedule recommendations from the initial audit.

To accomplish our objective, we reviewed two memorandums that established reliance on FRB Richmond's implementation of SAFR controls and on the RBOPS reviews of the Baltimore branch facility, and we met with the project leader for the RBOPS protection review to review documentation supporting the examination. We also reviewed the data center design guideline documents. We then obtained and reviewed documentation supporting the change order and procurement processes, including policies and tracking logs. We also reviewed the Board's budget documents and supporting documentation relating to cost estimates for the data center, project schedules, and status reports provided to us by the Board's Data Center Relocation Manager.

We interviewed Division of IT and Management Division personnel who are involved in the data center relocation, and we conducted a site visit to the Baltimore Branch of FRB Richmond to observe the construction status and to discuss and observe the planned PE controls. We attended weekly teleconferences with the general contractor to discuss the status of the construction of the data center, and we reviewed meeting minutes and other documents associated with the build-out. Further, we reviewed the contract with the general contractor and the service-level agreement with FRB Richmond. We conducted our fieldwork from April 2014 to July 2014.

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.

Appendix B
Management's Response

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

DIVISION OF
INFORMATION TECHNOLOGY

January 12, 2015

Mr. Mark Bialek
Office of Inspector General
Board of Governors of the Federal Reserve System
Washington DC, 20551

Dear Mark:

We have reviewed your report entitled "Audit of Planned Physical and Environmental Controls for the Board's Data Center Relocation" prepared as part of your office's oversight responsibilities pursuant to the Federal Information Security Management Act of 2002 (FISMA). The report evaluates the planned physical and environmental controls for the Board's data center against the Board's Information Security Program's control requirements. We are pleased that your assessment recognized that the Board is continuing to follow a structured approach to planning and executing the relocation of the data center, and Board staff are actively engaged in the planning and decision making for the project.

We agree with the one recommendation offered in your report. The Board has worked closely with the 5th District to identify the security controls that the Board Data Center will be inheriting from the Bank. The 5th District has provided the SAFR security plans defining how the inherited controls are met and the relevant supporting evidence. The Board ISO has compared the control implementations to the Board's security requirements and identified any risks incurred by relying on SAFR. The Board ISO will work with the 5th District to address identified risks and ensure the controls are appropriately documented in a security plan. Based on the risk assessment performed, the Board ISO is confident in relying on the 5th District for providing the inherited controls under SAFR.

We appreciate the professionalism and courtesies provided by the staff of the Office of the Inspector General and we look forward to working with your office in the future. Thank you for the opportunity to provide comments on this report.

Sincerely,

Sharon Mowry
Director, Information Technology

cc: Mr. Donald Hammond
Mr. Wayne Edmondson
Mr. Andrew Patchan
Mr. Ray Romero
Mr. Charles Young

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

HOTLINE

1-800-827-3340

OIGHotline@frb.gov

Report Fraud, Waste, and Abuse

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, e-mail, fax, or telephone.

Office of Inspector General, c/o Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW, Mail Stop K-300, Washington, DC 20551
Attention: OIG Hotline

Fax: 202-973-5044

Questions about what to report?

Visit the OIG website at www.federalreserve.gov/oig
or
www.consumerfinance.gov/oig