September 27, 2018

Bureau of Consumer Financial Protection

2018 List of Major Management Challenges for the Bureau

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

MEMORANDUM

DATE: September 27, 2018

TO: Mick Mulvaney
Acting Director
Bureau of Consumer Financial Protection

FROM: Mark Bialek
Inspector General

SUBJECT: *2018 List of Major Management Challenges for the Bureau*

We are pleased to provide you with our 2018 list of major management challenges facing the Bureau of Consumer Financial Protection (Bureau). These challenges represent what we believe to be the areas that, if not addressed, are most likely to hamper the Bureau's accomplishment of its strategic objectives.

We identified the Bureau's major management challenges by reviewing our audit and evaluation work, reports issued by the U.S. Government Accountability Office, and Bureau documents. The major management challenges, in order of significance, are as follows:

- Ensuring That an Effective Information Security Program Is in Place
- Managing the Human Capital Program
- Strengthening Controls and Managing Risks

We monitor the Bureau's efforts to address the management challenges we identify each year. Our monitoring work includes following up on open recommendations and conducting related audit and evaluation work. As a result of this monitoring, we did not include the challenge Effectively Managing and Acquiring Workspace in this year's list because the Bureau has substantially completed renovating its headquarters office building and employees have moved in. For additional information on our ongoing and planned work, please see our *Work Plan*.

We appreciate the cooperation that we received from the Bureau during this year's management challenges process. If you would like to discuss any of the challenges, please feel free to contact me.

cc: Brian Johnson, Acting Deputy Director
Kirsten Sutton, Chief of Staff
Katherine Fulton, Acting Chief Operating Officer and Acting Associate Director, Operations Division

Mary McLeod, General Counsel
Eric Blankenstein, Policy Associate Director, Division of Supervision, Enforcement and Fair Lending
Sheila Greenwood, Policy Associate Director, Division of Consumer Education and Engagement
Tom Pahl, Policy Associate Director, Division of Research, Markets and Regulations
Anthony Welcher, Policy Associate Director, Division of External Affairs
Christopher D'Angelo, Associate Director, Division of Supervision, Enforcement and Fair Lending
Gail Hillebrand, Associate Director, Division of Consumer Education and Engagement
Althea Kireilis, Associate Director, Office of Equal Opportunity and Fairness
Zixta Martinez, Associate Director, Division of External Affairs
David Silberman, Associate Director, Division of Research, Markets and Regulations
David Gragan, Chief Procurement Officer and Assistant Director, Office of the Chief Procurement Officer
Jerry Horton, Chief Information Officer
Martin Michalosky, Chief Administrative Officer and Assistant Director, Office of Administrative Operations
Elizabeth Reilly, Chief Financial Officer and Assistant Director, Office of the Chief Financial Officer
Jeffrey Sumberg, Chief Human Capital Officer and Assistant Director, Office of Human Capital
Dana James, Deputy Chief Financial Officer, Office of the Chief Financial Officer

Contents

Ensuring That an Effective Information Security Program Is in Place

The Bureau of Consumer Financial Protection (Bureau) collects and stores sensitive information, including confidential supervisory information and personally identifiable information, to support many of its mission-critical activities. Unauthorized access to or disclosure of this information, through internal or external threats, could undermine the public's trust in the Bureau and limit its ability to accomplish its mission.

Information security continues to be a key risk in the federal government, and as is the case for most federal agencies, the Bureau faces challenges in effectively securing its information technology systems and infrastructures from evolving threats. Although the Bureau continues to mature its information security program, it faces challenges in centralizing and automating processes to better manage insider risks; ensuring that automated feeds from all systems, including contractor-operated systems, feed into the Bureau's security information and event management tool; and aligning its information security program, policies, and procedures with the agency's evolving enterprise risk-management program.

To monitor and protect against the unauthorized transfer of data and other internal and external threats, the Bureau's cyberoperations team coordinates with its network provider, which assists with monitoring and detecting exfiltration and other threats to the agency's external network perimeter. The Bureau also completed an independent penetration test, which found no significant information security issues. However, the Bureau has not fully implemented an insider threat program that includes data loss prevention technologies to better integrate its activities in these areas.

We noted that the Bureau recently reassessed its open-access-within-each-region approach that previously afforded examiners broader access to confidential supervisory information and personally identifiable information than was needed to perform their job duties. We expect that the associated policy change will help to protect this sensitive information going forward; however, we have not assessed the implementation of the new policy or reviewed the Bureau's planned approach for ensuring that it operates in a manner that is consistent with the updated policy.

The prior open-access approach increased the risk of insider abuse of that information. An insider threat program could enable the agency to better prevent and detect unauthorized access to and disclosure of its sensitive information, particularly within its internal network. Likewise, the Bureau is in the process of fully implementing multifactor authentication for its internal system users. Multifactor authentication is in place for remote access and is enabled for privileged access to some cloud environments; however, full adoption would provide greater assurance that only authorized individuals are accessing Bureau systems and data.

The Bureau has also developed and implemented an effective information security continuous monitoring program. For example, the Bureau has implemented a centralized logging information tool for Bureau systems that provides it with enhanced alert capabilities and metrics to gauge effectiveness. However, not all of the Bureau's systems, including those operated by third parties, feed the necessary information

into the tool. Further, the Bureau can ensure that its information security continuous monitoring program remains effective by automating tools for several of its manual processes.

Consistent with the *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, the Bureau is continuing to align its information security program and related policies and procedures to the National Institute of Standards and Technology Cybersecurity Framework. The executive order emphasizes the importance of strengthening information security risk-management processes. In addition, recent federal guidance emphasizes the importance of agencies' implementing enterprise risk-management processes. As the Bureau matures its enterprise risk-management program by developing a risk appetite statement and tolerance levels, it will face challenges in aligning and updating its information security program to enable a consistent view of risks across the agency.

Further, the executive order highlights the importance of building a strong cybersecurity workforce, and the Bureau plans to leverage the National Initiative for Cybersecurity Education framework for determining the training requirements for cybersecurity personnel. The Bureau has experienced turnover in key information technology positions, which may delay its ability to meet the cybersecurity workforce goals of the executive order.

Related OIG Reports

- *2017 Audit of the CFPB's Information Security Program*, OIG Report 2017-IT-C-019, October 31, 2017
- *The CFPB Can Improve Its Examination Workpaper Documentation Practices*, OIG Report 2017-SR-C-016, September 27, 2017

Other Related Information

- *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800, May 11, 2017

Managing the Human Capital Program

An agency's response to changes to its human capital environment have a direct effect on its ability to carry out its mission efficiently and effectively. Since beginning operations in 2011, the Bureau has worked to build its human capital program and develop a diverse, high-performing, and engaged workforce. The Bureau's human capital leadership must adapt to recent changes at the agency, including changes in leadership, strategic direction, and organizational structure, as well as recent Bureau workforce directives, to help ensure that employees' skills are best leveraged.

In February 2018, the Bureau's leadership issued its fiscal years 2018–2022 strategic plan that refocuses the agency's priorities and commits the agency to fulfill only the Bureau's statutory responsibilities as established in the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). As part of the new strategic direction, the Bureau has also updated its mission to more closely align with the Dodd-Frank Act. In addition, the Bureau's leadership has made some organizational changes that will affect the roles and responsibilities of the Bureau's workforce. To address these organizational changes, the Office of the Director established a cross-divisional team of division managers, resource management officers, Office of Human Capital personnel, Legal Division personnel, and other stakeholders. The human capital program will need to remain adaptive and continue to provide the Bureau with support, such as assisting with job description reviews and adjusting workforce resources, to better align with the revised strategic direction at the Bureau.

Guidance issued by the Office of Management and Budget (OMB) to improve management of the federal workforce also has affected the Bureau. OMB Memorandum M-17-22, *Comprehensive Plan for Reforming the Federal Government and Reducing the Federal Civilian Workforce*, directs executive branch departments and agencies to identify and begin taking actions to reduce the federal workforce in order to reduce costs and improve efficiencies. In response to this memorandum, the Bureau established a hiring authorization process for planning and prioritizing hiring across the agency to promote the accomplishment of the Bureau's mission and align with key elements of the memorandum. In addition, the Bureau's leadership instituted an agencywide hiring freeze, with limited exceptions having been approved for those positions deemed critical. To fill vacancies, the Bureau has been reallocating staff resources through reassignments or detail opportunities. As part of the process for reallocating staff resources, human capital management is monitoring reassignments to ensure that they are distributed in such a way as to minimize the effect on the Bureau's ability to meet workload demands. Some of these vacancies are for highly specialized skill sets, and the Bureau may face challenges in identifying the necessary skill sets in its current workforce.

The Office of Human Capital's efforts to establish workforce planning have been affected by the hiring constraints at the Bureau. Workforce planning can help the Bureau better align its human capital resources with its current and emerging mission and programmatic goals. In June 2018, the Bureau internally filled a position to focus on workforce planning, with an emphasis on data analysis to identify trends within the Bureau, including trends in the current skill sets of the workforce and any skill gaps. This workforce-planning position will also be responsible for succession planning. A formal succession-planning program could help the Bureau promote diversity in senior management and mission-critical positions. Having a workforce-planning program in place would help the Bureau respond to evolving

workforce expectations and changes in agency leadership. The Bureau's human capital program will need to remain adaptive as the agency's operational environment changes and to continue to identify strategies to overcome such challenges.

Related OIG Reports

- *The CFPB Can Enhance Its Diversity and Inclusion Efforts*, OIG Report 2015-MO-C-002, March 4, 2015

Other Related Information

- Bureau of Consumer Financial Protection, *Bureau of Consumer Financial Protection Strategic Plan FY 2018–2022* (Goal 3, Foster operational excellence through efficient and effective processes, governance and security of resources and information, page 12)
- Office of Management and Budget, *Comprehensive Plan for Reforming the Federal Government and Reducing the Federal Civilian Workforce*, OMB Memorandum M-17-22, April 12, 2017
- U.S. Government Accountability Office, "Strategic Human Capital Management," *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317, February 15, 2017
- U.S. General Accounting Office, *Recent Government-Wide Hiring Freezes Prove Ineffective in Managing Federal Employment*, FPCD-82-21, March 10, 1982

Strengthening Controls and Managing Risks

Internal control activities serve as the first line of defense in safeguarding assets; preventing impairments to operations; and helping to ensure compliance with provisions of contracts, laws, regulations, and other agreements. Effective internal controls help an organization adapt to shifting environments, evolving demands, changing risks, and new priorities. Over the past year, our office and an independent public accountant continued to identify programs in which the Bureau can further strengthen its internal controls in order to mitigate financial, operational, and reputational risks. The Bureau has taken steps to strengthen its internal controls and manage risk, including implementing an enterprise risk-management program.

The Bureau should continue to strengthen its controls for contract financing and management, offboarding, and its privacy and travel programs. Specifically, we have found the following through our audit and evaluation work:

- The Bureau did not comply with *Federal Acquisition Regulation* requirements concerning contract financing and conducting and documenting annual blanket purchase agreement reviews for one of its largest contracts. In addition, program staff did not verify actual contractor expenses by obtaining and reviewing supporting source documents.
- The Bureau needs to strengthen its offboarding processes for employees and contractors, specifically with respect to returning information technology assets, deactivating building access badges, and preventing the sharing or removing of nonpublic records.
- The Bureau can further strengthen its travel program by ensuring that travelers and approving officials receive proper guidance on documenting multicity trips and personal leave taken during official travel.

In addition to our work, an independent audit identified deficiencies related to controls over budget execution. The report noted that the agency did not establish adequate procedures for reviewing and deobligating unsubstantiated obligations in a timely manner. Another independent audit found that the Bureau needs to strengthen its privacy program, specifically with respect to expanding its inventory of personally identifiable information to include data used by the Office of Human Capital, the Office of Administrative Operations, and the Office of the Chief Financial Officer, and to strengthening its physical controls over its portable media, such as laptops and smartphones.

In addition to our specific audit and evaluation findings and those of independent auditors, we note that the Bureau needs to update its policies to reflect changes to its organizational structure and responsibilities. The Bureau has acknowledged in its strategic and performance plans the importance of being a responsible steward of resources. Further, it has acknowledged that achieving operational excellence requires the Bureau to mature and adapt policies, procedures, tools, and controls to operate more efficiently, effectively, and transparently. Therefore, the Bureau has committed to maintaining effective internal controls and to following appropriate models for internal controls, such as the Federal Managers' Financial Integrity Act of 1982; the objectives on financial reporting as established under the

Dodd-Frank Act; and best practices provided in OMB's *OMB Circular A-123: Management's Responsibility for Enterprise Risk Management and Internal Control.*

The Bureau continues to strengthen internal controls for its various programs, including filling gaps in its policies and implementing new systems to improve operations. It reported several corrective actions it plans to implement to address control weaknesses, including but not limited to the following:

- enhancing policy and associated training to address contract financing and requesting and reviewing supporting documents to verify unliquidated prepayment amounts so that unspent funds can be properly refunded and deobligated
- monitoring the accuracy of separation data, including implementing an additional reconciliation process
- finalizing certified, agency-specific training on travel for approving officials and cardholders
- conducting semiannual reviews of open obligations to determine whether they remain valid, can be deobligated, or need to be adjusted, and refining its contract closeout process
- developing a complete inventory of the personally identifiable information housed at the Bureau and exploring ways to centralize information related to operational datasets

The Bureau has also made additional progress in establishing an agencywide enterprise risk-management program. It recently developed a customized maturity model based on commonly used best practices and is exploring options for an external assessment of its enterprise risk-management program. Finally, the U.S. Government Accountability Office has reported that the Bureau maintained effective internal control over financial reporting. Specifically, during fiscal year 2017, the Bureau took sufficient actions to address the internal control deficiencies related to controls over accounting for property, equipment, and software.

Related OIG Reports

- *The Bureau's Travel Card Program Controls Are Generally Effective but Could Be Further Strengthened*, OIG Report 2018-FMIC-C-014, September 26, 2018
- *The Bureau Could Have Better Managed Its GMMB Contract and Should Strengthen Controls for Contract Financing and Contract Management*, OIG Report 2018-FMIC-C-011, June 20, 2018
- *Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program*, OIG Report 2018-IT-C-003, February 14, 2018
- *The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data*, OIG Report 2018-MO-C-001, January 22, 2018

Other Related Information

- Bureau of Consumer Financial Protection, *Annual Performance Plan and Report*, March 2018
- KPMG LLP, *Consumer Financial Protection Bureau Independent Audit of Selected Operations and Budget, Fiscal Year 2017*, April 18, 2018

- U.S. Government Accountability Office, *Financial Audit: Bureau of Consumer Financial Protection's Fiscal Years 2017 and 2016 Financial Statements*, GAO-18-185R, November 15, 2017
- Office of Management and Budget, *OMB Circular No. A-123: Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Memorandum M-16-17, July 15, 2016
- U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO-14-704G, September 10, 2014

Abbreviations

Bureau	Bureau of Consumer Financial Protection
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
OIG	Office of Inspector General
OMB	Office of Management and Budget

Report Contributors

Jackie Ogle, OIG Manager, Financial Management and Internal Controls
Andrew Gibson, OIG Manager, Information Technology
Matt Simber, OIG Manager for Policy, Planning, and Quality Assurance
Silvia Vizcarra, OIG Manager, Financial Management and Internal Controls
Brenda Rohm, Senior Policy and Planning Analyst
David Horn, Senior Auditor
Ann Wilderman, Auditor
Cynthia Gray, Senior OIG Manager for Financial Management and Internal Controls
Khalid Hasan, Senior OIG Manager for Information Technology
Timothy Rogers, Senior OIG Manager for Management and Operations
Melissa Heist, Associate Inspector General for Audits and Evaluations
Peter Sheridan, Associate Inspector General for Information Technology

Contact Information

General

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551

Phone: 202-973-5000
Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov

OIG

Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, web form, phone, or fax.

OIG Hotline
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551

Phone: 800-827-3340
Fax: 202-973-5044