



OFFICE OF INSPECTOR GENERAL

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

September 30, 2015

MEMORANDUM

TO: Richard Cordray
Director
Consumer Financial Protection Bureau

FROM: Mark Bialek 
Inspector General

SUBJECT: 2015 List of Major Management Challenges for the CFPB

We are pleased to provide you with the Office of Inspector General's 2015 list of major management challenges facing the Consumer Financial Protection Bureau (CFPB). These challenges represent what we believe to be the areas that, if not addressed, are most likely to hamper the CFPB's accomplishment of its strategic objectives.

We used audit and evaluation work performed by our office and audits performed by the U.S. Government Accountability Office (GAO), along with CFPB documents, to identify the CFPB's major management challenges. We removed the challenge "Improving the Operational Efficiency of Supervision" from this year's list because the CFPB has done significant work to reduce the backlog of examination reports and improve the examination process. The following table lists the four management challenges that we have identified, in order of significance.

Management challenge no.	Title	Page no.
1	Ensuring an Effective Information Security Program	2
2	Building and Sustaining a High-Performing and Diverse Workforce	5
3	Strengthening Controls Over Management Operations	7
4	Maintaining Physical Infrastructure	8

Each challenge is detailed below.

Management Challenge 1: Ensuring an Effective Information Security Program

Information security presents a challenge to the Consumer Financial Protection Bureau (CFPB) due to the advanced persistent threat to the government's information technology (IT) infrastructure from outside governments and organized groups. To strengthen its defenses against such attacks, CFPB management should continue improving its information security program, overseeing the security of contractor-operated information systems, transitioning IT resources from the U.S. Department of the Treasury (Treasury), and ensuring that personally identifiable information (PII) is properly protected. The threat of cyberattack is a constant presence in the government IT environment, as exemplified earlier this year when the U.S. Office of Personnel Management reported its detection of cybersecurity incidents affecting its systems and data that compromised the personal information of current and former federal employees, prospective federal employees, and contractors.

Improving the Information Security Program

As the CFPB evolves, it continues to mature and improve its information security program to align with new guidance provided by the National Institute of Standards and Technology. Some improvements that have been noted in our prior audits include enhancements to automation, centralization, and implementation, including in the area of continuous monitoring, to ensure that the requirements of the Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014 (FISMA), are met. While improvements have been made, additional work is needed in four high-priority security risk areas: continuous monitoring, configuration management, security training, and incident response and reporting.

CFPB management faces challenges in implementing a continuous monitoring process for all CFPB systems, establishing metrics to gauge the effectiveness of its continuous monitoring program, and implementing automated tools to more comprehensively assess security controls and system configurations. Management informed us that the underlying challenge has been in adjusting the culture to one in which system owners report information security details, such as information security control testing results for each system, centrally. Further, it has been difficult for the CFPB to correlate information on incident activity because it did not have the capability to analyze security incident information from all relevant sources. Additional challenges exist in developing and implementing an agency-wide configuration management plan and in developing and implementing a role-based security training program to ensure that individuals with significant security responsibilities for CFPB systems are effectively and efficiently implementing the agency's information security program.

GAO continues to include protecting the federal government's information systems and the nation's cybercritical infrastructure as a priority for federal agencies. According to a 2015 GAO report, the White House and senior leaders at the U.S. Department of Homeland Security have committed to securing critical cyberassets. Specifically, the President has signed legislation and issued strategy documents related to this commitment, and the U.S. Department of Homeland Security has committed time and resources to advancing cybersecurity efforts at federal agencies

and to promoting the use of a cybersecurity framework by critical infrastructure sectors. However, securing cyberassets remains a challenge for federal agencies, including the CFPB.

Ensuring the Security of Contractor-Operated Information Systems

FISMA requires agencies to develop, document, and implement an agency-wide information security program for the information and information systems that support the operations and assets of the agency, including those provided by another agency, a contractor, or another source. Our audits of CFPB contractor-operated systems have identified several areas for improvement to ensure that the CFPB's information security requirements are met. These areas include incident response and reporting, configuration management, and personnel security.

The CFPB also continues to face challenges in ensuring that contractors implement information security controls that meet agency requirements. The CFPB relies on a variety of contractor-operated and contractor-maintained systems to meet its mission, including several cloud computing-based systems in which computing resources may be shared with other federal or commercial entities. The risks associated with contractor-provided services can be heightened in cloud computing-based environments because the agency may have limited insight or knowledge of the security processes of contractors. The CFPB should ensure that cloud providers are implementing FISMA requirements for records management, electronic discovery, privacy, and information security.

Transitioning Information Security and IT Resources From Treasury to the CFPB's Infrastructure

Although the CFPB has made significant progress, it still faces challenges in transitioning information security and IT resources from Treasury and building its IT infrastructure. When the CFPB began operations in July 2011, it relied on Treasury's IT systems, IT infrastructure, and information security program. Some of the information security program services and systems that Treasury provided for the CFPB included remote access, security awareness training, and incident reporting. During the course of the migration of IT resources and information security from Treasury, the CFPB has encountered scheduling delays and implementation difficulties in establishing certain components of its own IT infrastructure. The CFPB is still in the process of migrating the wide area network and voice systems to CFPB control. Further, the agency must ensure that its IT infrastructure is built with appropriate security and privacy controls to protect sensitive information.

Protecting Personally Identifiable Information

Protecting PII in federal systems is critical because loss or unauthorized disclosure can lead to serious consequences for individuals. In a 2015 update to its *High Risk List*, GAO expanded the scope of the *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure* risk area to include the federal government's protection of PII due to advances in technology. The CFPB uses a variety of cutting-edge technologies and must continue to ensure

that PII is adequately protected within the systems it owns and maintains and within those maintained on its behalf by contractors and other entities.

In the normal course of carrying out its statutory mandate to protect consumers, ensure regulatory compliance, and monitor the consumer financial marketplace for risks to consumers, the CFPB collects, processes, stores, and shares privacy-related information associated with consumer financial products and services. For example, the CFPB receives information about accounts from consumers who seek the CFPB's help through the Consumer Response function and from the institutions involved in the complaints. The CFPB may share PII to fulfill its enforcement responsibilities or statutory or regulatory requirements. According to the CFPB, it has signed memorandums of understanding with federal, state, and local government entities regarding the potential sharing of data and the treatment of shared data.

GAO conducted an audit of the CFPB in September 2014 and noted that the CFPB has collected consumer financial data on credit card accounts, mortgage loans, and other products. It found that the CFPB lacks written procedures and comprehensive documentation for a number of processes, including data intake and information security risk assessments. GAO also found that the CFPB has not yet fully implemented a number of privacy control steps and information security practices.

Agency Actions

The CFPB has taken steps to develop, document, and implement an information security program. The agency has also made progress in centralizing its information security program by building out its Cybersecurity Program Management Office, which engages with oversight teams to implement the cybersecurity program at the CFPB. The CFPB is also working on centralizing continuous monitoring by making enhancements to its enterprise security logging and security information monitoring systems, which provide security alerts. With the centralization of these security alerts, the CFPB now has the capability to analyze and correlate security incidents. Further, the engineering team has been enhancing the build-out of security controls during the development of systems.

The CFPB has taken several steps to strengthen its oversight processes to ensure that contractor-operated systems meet FISMA and agency information security requirements. Specifically, it has taken steps to promote collaboration among security, IT, and procurement staff to ensure that security requirements for third-party contractors are identified and accounted for during solicitations. Standard contract language has been updated and built into contracts and service-level agreements with third-party providers.

The CFPB developed a phased approach to transitioning IT services from Treasury and developing its IT infrastructure. The CFPB has already transitioned e-mail, file shares, mobile devices, Active Directory, remote access, the wide area network, SharePoint, and laptop images to CFPB-managed infrastructure and is on track to have full technology independence by the end of fiscal year (FY) 2015.

The CFPB hired a Chief Data Officer, who leads a set of teams that work closely with the Chief Information Security Officer to ensure that data are protected. One primary focus of the Chief Data Officer is to provide centralized data governance and management of CFPB data sets. In this role, the Chief Data Officer is also charged with implementing the CFPB's *Information Governance Policy* and addressing many of GAO's findings. Further, the CFPB has a Chief Privacy Officer, who is responsible for the agency's privacy compliance and operational activities. The CFPB is also working on a privacy plan that is scheduled to be completed by the end of FY 2015, and it has conducted some role-based training, with more scheduled for the remainder of 2015.

Management Challenge 2: Building and Sustaining a High-Performing and Diverse Workforce

A key outcome for the CFPB's strategic goal of advancing the agency's performance by maximizing its resource productivity and enhancing its impact is attracting, engaging, and deploying a high-performing and diverse workforce. The CFPB faces challenges in meeting this goal, however, due to competition from other employers for the highly qualified staff with specialized skill sets that the CFPB needs to fulfill its mission. Further, as the agency seeks to build and sustain a high-performing and diverse workforce, it will need to strengthen workforce planning and develop an improved performance management system.

Recruiting and Retaining a Highly Skilled, Diverse Workforce

To effectively carry out its mission, the CFPB strives to hire and retain the best and most capable staff, recruited from a variety of backgrounds. In order to remain competitive with other leading government, commercial, and financial organizations, the CFPB must successfully address evolving expectations regarding diversity, workplace flexibility, career progression, communication, and continuous learning. Another important consideration for the CFPB in recruiting and retaining staff is engaging in workforce planning. The CFPB has established a workforce planning process and identified mission-critical occupations and related competency models. However, a key part of workforce planning—developing a succession plan to ensure continuity of knowledge and leadership in key positions—has not been formally implemented agency-wide. The CFPB's October 2014 *Succession Management Guide* will help to shape the CFPB's succession planning process to ensure that the CFPB is identifying and developing a diverse pool of talent with the potential to be future senior leaders.

The CFPB has reported that it supports the development of a diverse, highly qualified employee base and recognizes that there is an opportunity to increase minority representation, specifically in certain mission-critical positions. The CFPB relies on the Office of Women and Minority Inclusion and also leverages support from leaders across the CFPB to assist in ensuring that its workforce is diverse and inclusive. Although the CFPB has taken steps to enhance its diversity and inclusion practices, our recent audit work noted that opportunities exist for the CFPB to enhance diversity and inclusion efforts, such as implementing an agency diversity and inclusion strategic plan as well as a formal succession planning process. As the CFPB continues to build

and sustain a high-performing and diverse workforce, these challenges should continue to be areas of focus.

Developing and Implementing a New Performance Management System

The CFPB faces challenges in developing and implementing a new performance management system. Our prior audit work noted that there were statistically significant differences in CFPB employees' performance ratings for FY 2012 and FY 2013 based on gender, race/ethnicity, and age. The CFPB has taken several actions to address these differences in its performance ratings. Specifically, the CFPB commissioned an independent third-party review to analyze the potential root causes of the rating disparities and to examine the sufficiency of the CFPB's efforts to understand and address these disparities. Also, the CFPB transitioned to a two-level performance management system for FY 2014 and FY 2015, and it has been working with the National Treasury Employees Union to develop a new performance management system for FY 2016 and beyond. The transition from the interim two-level performance management system to the new performance management system will bring a significant change for the CFPB. Developing the new employee performance management system and ensuring that it is consistently applied across the agency may pose challenges for the CFPB, because it will need to ensure that the new process is effective, fair, and not overly burdensome, while simultaneously maintaining distinctions between high and low performers.

Agency Actions

The CFPB has made a number of improvements to its human capital processes. For example, the CFPB undertook a two-and-a-half-year agency-wide research effort to develop more robust competency models for all CFPB positions. This effort resulted in the development of competency models that help to support a variety of human resource practices and functions, such as the succession planning process and performance management system. In addition, the CFPB has begun the Workforce of the Future initiative, which is intended to ensure that the CFPB has a skilled and productive workforce to fulfill its mission for the long term. This initiative includes an articulation of how the CFPB's practices should evolve to create the workforce experience that enables people to do their best work for sustainable, long-term impact. The CFPB also placed the Office of Minority and Women Inclusion and the Office of Civil Rights under a newly formed Office of Equal Opportunity and Fairness within the Office of the Director.

The CFPB has taken several steps to recruit and retain a highly qualified, diverse workforce. For example, the CFPB recruited applicants from a broad range of geographical areas, continued to review data to identify underrepresentation, and targeted its recruiting to ensure that the agency reaches a diverse pool of talent. To ensure workforce retention, the CFPB has taken a number of steps, including using career ladders, providing opportunities for cross-functional work within and outside the agency, providing training opportunities, and fostering a mission-focused work environment. The CFPB's retention strategy includes employee engagement activities, which encourage headquarters and field office staff members to support a shared workforce commitment to

the CFPB's mission and values. The CFPB has also conducted listening sessions with its employees to identify and respond to perceptions of fairness, equality, diversity, and inclusion.

The CFPB has made progress in developing a new performance management system. In addition to creating new standard operating procedures for performance management program evaluation, compliance, training attendance, and training evaluation, it established a joint labor-management working group with the National Treasury Employees Union. This working group identified a number of key performance management program elements, outlined detailed conditions for successful implementation of the new program, and implemented a streamlined process for FY 2015 performance evaluations and FY 2016 performance plans. Some additional accomplishments of this group include creating management self-assessment and 360-degree feedback instruments on the CFPB's new management competencies and committing to annual mandatory training on performance management for all employees. Further, the working group is developing recommendations for the new performance management system. Those recommendations are expected to be submitted to the Director by September 2015.

Management Challenge 3: Strengthening Controls Over Management Operations

The CFPB continues to implement management processes and controls as it seeks to provide effective oversight of the consumer financial marketplace. Recognizing the importance of internal controls, the CFPB established a team in the Office of the Chief Financial Officer to review, monitor, and improve internal control. As the organization grows and the consumer financial products and services that the CFPB regulates evolve, establishing and monitoring internal controls should continue to be an area of focus across the agency. Our recent work has shown that the CFPB needs to strengthen its controls over contract management. In addition, our recent work noted opportunities for the CFPB to improve its information system security controls and management controls related to the Consumer Complaint Database.

Strengthening Operational Controls

The CFPB should continue to improve its policies and procedures, including establishing clear roles and responsibilities. Our audit work has identified that the CFPB needed to review and revise the policies and procedures governing travel and the Civil Penalty Fund. Our work also has identified that contract management controls and oversight could be improved. The CFPB identified a material weakness and a significant deficiency related to its contracting activities in its 2014 assessment and report on management's controls. Similar findings and control deficiencies related to these activities were also reported in other independent audits of the CFPB. Many of the weaknesses we identified related to contracts awarded by Treasury's Bureau of the Fiscal Service on behalf of the CFPB. The CFPB indicated that managing interagency agreements presents challenges because there are risks associated with relying on third-party providers to help carry out the CFPB's mission.

Strengthening Controls for the Consumer Complaint Database

In June 2012, the CFPB became the first federal regulator to publicly share individual-level consumer financial complaint data. While the Consumer Complaint Database initially contained only credit card complaints, the CFPB has extended the database to other consumer financial products and services. In June 2015, the CFPB enhanced the Consumer Complaint Database to include consumer complaint narratives. Our audit and evaluation work identified opportunities to improve information system security controls and management controls related to the Consumer Complaint Database. Specifically, we found security control deficiencies related to configuration management, access control, and audit logging and review in the Data Team Complaint Database, which supports the Consumer Complaint Database. We also found that the CFPB has implemented some controls to monitor the accuracy of complaint data in the internal case management system from which complaint data are extracted and then uploaded to the Consumer Complaint Database. However, the CFPB has not established separate management controls to ensure the accuracy of the data in the public-facing Consumer Complaint Database.

Agency Actions

The CFPB has made progress in implementing internal controls for its key management operations. For example, in response to the control deficiencies that were identified in the CFPB's contracting activities, the agency has started implementing corrective actions, such as providing additional guidance to contracting officer's representatives and increasing oversight of contract activities. Further, the CFPB identified several areas on which to focus, including the development, review, and revision of policies and procedures for procurement. In addition, the CFPB has taken steps to improve the reliability and timeliness of the data in the Consumer Complaint Database and the related secure information systems.

Management Challenge 4: Maintaining Physical Infrastructure

The CFPB is currently renovating its headquarters building, managing swing space until the renovation is complete, and planning to establish office space in its Southeast region. The renovation of the headquarters building is a multiyear project that poses several challenges and, if delayed, could affect the agency's ability to provide office space for all its staff as well as affect project costs.

Headquarters Renovation

The headquarters building that the CFPB is leasing has not undergone significant renovation since it was constructed in 1976. The CFPB is making workplace and energy-efficiency improvements to its headquarters, including upgrades to the building infrastructure, and is replacing aging mechanical and electrical systems that have reached the end of their life cycle.

The CFPB headquarters renovation is a multiyear project that poses several challenges for the CFPB, including managing and mitigating risks associated with schedule delays, unanticipated expenses, and cost overruns. In recent audit work, we found that the CFPB headquarters construction costs appear reasonable and that controls for approving, managing, and documenting renovation costs and project decisions are designed appropriately. We have not had the opportunity to test the operating effectiveness of those controls, however, because most of the CFPB's construction cost management control activities have not yet begun. The CFPB has partnered with the U.S. General Services Administration (GSA) to assist with the renovation project. The CFPB will need to ensure that management control activities associated with the renovation project are operating effectively.

Space Planning

CFPB employees are currently occupying office space in two locations while the headquarters renovation is ongoing. Once the renovation is complete, the headquarters building will only accommodate a portion of the displaced employees; thus, additional space will still be required. The CFPB will need to determine an optimal location for those employees not returning to the headquarters building. The CFPB's space planning efforts for these employees may be adversely affected if the renovation project encounters schedule delays; in addition, any delays to the project could result in additional rent expenses. The CFPB should continue to ensure that its space needs are managed appropriately as it seeks to obtain office space for its Southeast region.

Agency Actions

The CFPB established a memorandum of understanding with GSA to provide assistance with its renovation needs. GSA awarded a construction management contract in July 2014, as well as a construction contract in December 2014. The construction management contract includes specific controls aimed at managing costs throughout the design and construction phases of the renovation project so that the renovation budget is not exceeded. In addition, the construction contract type and delivery method is expected to help ensure that the budget is not exceeded and to give the CFPB additional control over the design and corresponding costs. The CFPB plans to coordinate with GSA regarding its space needs for personnel at the headquarters location and in the Southeast region.

Closing

We appreciate the cooperation we received from the CFPB regarding this year's major management challenges. Please contact me if you would like to discuss any of the challenges.

cc: Sartaj Alag, Chief Operating Officer and Associate Director, Operations Division
David Bleicken, Acting Associate Director, Division of Supervision, Enforcement, and Fair Lending
Meredith Fuchs, Acting Deputy Director, General Counsel, and Associate Director, Legal Division

Gail Hillebrand, Associate Director, Division of Consumer Education and Engagement

Stuart Ishimaru, Associate Director, Office of Equal Opportunity and Fairness

Zixta Martinez, Associate Director, Division of External Affairs

David Silberman, Associate Director, Research, Markets, and Regulations Division

Stephen Agostini, Chief Financial Officer and Assistant Director, Office of the Chief
Financial Officer

David Gragan, Assistant Director, Office of the Chief Procurement Officer

Christopher Johnson, Acting Assistant Director, Office of Consumer Response

Jeffrey Sumberg, Chief Human Capital Officer and Assistant Director, Office of the Chief
Human Capital Officer

Suzanne Tosini, Chief Administrative Officer and Assistant Director, Office of the Chief
Administrative Officer

Ashwin Vasan, Chief Information Officer and Assistant Director, Office of Technology
and Innovation