

Consumer Financial Protection Bureau

The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data



Office of Inspector General

Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau



Executive Summary, 2018-MO-C-001, January 22, 2018

The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data

Findings

Although we determined that controls related to conflicts of interest are generally in place, we identified opportunities for the Consumer Financial Protection Bureau (CFPB) to strengthen controls for the return of property and records management. Specifically, we found that the CFPB does not have adequate controls for deactivating badges and maintaining badging records. In addition, we found that the CFPB did not consistently maintain information technology asset documentation. We also found that the CFPB did not always conduct records briefings for separating individuals and that the CFPB can enhance its records management guidance for interns and contractors. Further, controls over contractor data should be strengthened so that the CFPB has a complete and accurate accounting of its contractors. We found that the CFPB informed executive employees of postemployment restrictions and requirements and maintained nondisclosure agreements for most contractors.

During the audit, the CFPB took certain actions to improve its offboarding process. For example, the CFPB revised the *Off-Boarding Policy*, identified the Office of Human Capital as the offboarding process owner, and developed standard operating procedures related to offboarding.

Recommendations

Our report contains recommendations designed to strengthen the CFPB's controls over the offboarding processes for the return of property, records management, and maintenance of contractor nondisclosure agreements. Additionally, our report contains recommendations to ensure that the CFPB has an up-to-date list of its contractors as well as current, accurate, and complete separation data for contractors and employees. In its response to our draft report, the CFPB concurs with our recommendations and describes actions that have been or will be taken to address our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Purpose

We conducted this audit to assess the CFPB's controls over the offboarding process for the return of CFPB property, records management, and conflicts of interest. Specifically, we determined whether those controls are operating effectively to mitigate reputational and security risks.

Background

During fiscal year 2016, 188 employees and approximately 175 contractors separated from the CFPB. In April 2013, the CFPB issued its *Off-Boarding Policy*, which establishes the separation processes for CFPB employees and contractors. The policy outlines that prior to separation, employees and contractors are required to return all government-issued property, including badges, and any federal records in their possession. Executive employees should also receive ethics counseling on conflicts of interest, specifically, postemployment restrictions. Although contractors do not receive an ethics briefing, they are required to sign nondisclosure agreements. In June 2016, the Operations Division created a steering committee to review all CFPB policies, procedures, processes, and practices related to offboarding.



Recommendations, 2018-MO-C-001, January 22, 2018

The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data

Finding 1: The CFPB Did Not Deactivate All Badges Timely for Separating Employees and Contractors and Did Not Always Maintain a Record of Badges' Collection Status

Number	Recommendation	Responsible office
1	Develop policies or procedures that meet applicable requirements to ensure the timely deactivation of PIV badges and site badges in the building access system and PIV badges in the USAccess system upon an individual's separation.	Operations Division
2	Finalize the building access system upgrade to ensure that PIV badges and site badges are automatically deactivated in the building access system and that PIV badges are automatically deactivated in the USAccess system upon an individual's separation.	Operations Division
3	Develop a process to maintain <ol style="list-style-type: none"> a. the badge status history for separated employees, interns, and contractors. b. a centralized record of PIV and site badge collection, including the separated individual's name, collection status and date, badge type, and badge number, and periodically reconcile that record with employee and contractor personnel data. 	Operations Division
4	Identify and correct the information for all separated employees and contractors in the building access system and for separated employees in the USAccess system to ensure that all badges are properly deactivated.	Operations Division

Finding 2: The CFPB Did Not Maintain Complete Documentation for IT Assets Assigned to Separating Individuals

Number	Recommendation	Responsible office
5	Develop and implement procedures to ensure that IT assets assigned to individuals and collected from individuals are documented on the respective forms and updated in Remedyforce timely.	Office of Technology and Innovation
6	Maintain a history of IT assets assigned and collected in Remedyforce for all separated employees and contractors in accordance with the applicable National Archives and Records Administration's <i>General Records Schedule</i> .	Office of Technology and Innovation

Finding 3: RMO Did Not Always Perform Its Records Management Responsibilities for Separating Individuals

Number	Recommendation	Responsible office
7	Identify a process for collecting and maintaining all records departure forms for separating employees and interns, and develop a procedure to obtain the signed form electronically.	Office of Administrative Operations
8	Update the <i>Records Management Procedure for Departing Employees</i> to specify RMO's responsibilities with respect to interns, including a requirement to conduct an individual exit interview for those interns with records subject to a litigation hold.	Office of Administrative Operations

Finding 4: The Ethics Office Informed Executive Employees of Postemployment Restrictions and of the Requirement to Submit Public Financial Disclosure Reports Timely

Number	Recommendation	Responsible office
	No recommendations	

Finding 5: The CFPB Maintained NDAs for Most Contractors

Number	Recommendation	Responsible office
9	Review contract files and determine whether NDAs are missing for any of the individuals associated with those files. If so, obtain a signed NDA for each of those individuals.	Office of the Chief Procurement Officer

Finding 6: Certain CFPB Separation and Contractor Data Are Not Accurate and Complete

Number	Recommendation	Responsible office
10	Identify a process for maintaining an accurate contractor personnel list in order to monitor and track contractor information.	Office of the Chief Procurement Officer
11	Once upgrades to the offboarding system have been fully implemented, develop a process to periodically reconcile new separation data in the offboarding system with one of the CFPB's human resources systems to ensure that the separation data are current, accurate, and complete.	Office of Human Capital



Office of Inspector General

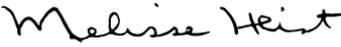
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

MEMORANDUM

DATE: January 22, 2018

TO: Sartaj Alag
Chief Operating Officer and Associate Director, Operations Division
Consumer Financial Protection Bureau

Mary McLeod
General Counsel
Consumer Financial Protection Bureau

FROM: Melissa Heist 
Associate Inspector General for Audits and Evaluations

SUBJECT: OIG Report 2018-MO-C-001, *The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data*

We have completed our report on the subject audit. We conducted this audit to assess the Consumer Financial Protection Bureau's (CFPB) controls over the offboarding process for the return of property, records management, and conflicts of interest and to determine whether those controls are operating effectively to mitigate reputational and security risks.

We provided you with a draft of our report for review and comment. In your response, you concur with our recommendations and outline actions that have been or will be taken to address our recommendations. We have included your response as appendix B to our report.

We appreciate the cooperation that we received from the Operations Division and the Ethics Office. Please contact me if you would like to discuss this report or any related issues.

cc: Sheila Greenwood, Special Advisor, Office of the Director
Martin Michalosky, Chief Administrative Officer and Assistant Director, Office of Administrative Operations
Jerry Horton, Chief Information Officer
David Gagan, Chief Procurement Officer and Assistant Director, Office of the Chief Procurement Officer
Jeffery Sumberg, Chief Human Capital Officer and Assistant Director, Office of Human Capital
Elizabeth Reilly, Chief Financial Officer and Assistant Director, Office of the Chief Financial Officer

Dana James, Deputy Chief Financial Officer, Office of the Chief Financial Officer
Anya Williams, Finance and Policy Analyst, Office of the Chief Financial Officer
Carlos Villa, Finance and Policy Analyst, Office of the Chief Financial Officer



Contents

Introduction	9
Objective	9
Background	9
Overview of the CFPB’s Offboarding Process	9
CFPB Offices That Support Offboarding Activities	11
Commendable Action: The CFPB Has Begun to Revise Its Offboarding Process	13
Finding 1: The CFPB Did Not Deactivate All Badges Timely for Separating Employees and Contractors and Did Not Always Maintain a Record of Badges’ Collection Status	15
The CFPB Did Not Deactivate PIV Badges Timely	15
OSP Did Not Always Maintain a Record of Badges’ Collection Status	17
The CFPB’s Building Access System Was Missing Records and Contained Inaccurate Badging Records	18
Management Actions Taken	19
Recommendations	19
Management’s Response	19
OIG Comment	20
Finding 2: The CFPB Did Not Maintain Complete Documentation for IT Assets Assigned to Separating Individuals	21
T&I Did Not Consistently Maintain IT Asset Documentation	21
Management Actions Taken	22
Recommendations	23
Management’s Response	23
OIG Comment	23
Finding 3: RMO Did Not Always Perform Its Records Management Responsibilities for Separating Individuals	24
RMO Did Not Always Collect Records Departure Forms or Conduct Records Departure Briefings for Nonexecutive and Executive Employees	24
The Records Management Procedure Does Not Specify Guidance for Interns	25
RMO Does Not Provide Guidance to CORs Related to Contractor Separation	25
Management Actions Taken	26

Recommendations	26
Management’s Response	26
OIG Comment	27
Finding 4: The Ethics Office Informed Executive Employees of Postemployment Restrictions and of the Requirement to Submit Public Financial Disclosure Reports Timely	28
Management’s Response	28
Finding 5: The CFPB Maintained NDAs for Most Contractors	29
The CFPB Did Not Have an NDA on File for One Contractor	29
Management Actions Taken	29
Recommendation	30
Management’s Response	30
OIG Comment	30
Finding 6: Certain CFPB Separation and Contractor Data Are Not Accurate and Complete	31
The CFPB Does Not Have a Centralized Contractor List or Accurate Separation Data	31
Management Actions Taken	32
Recommendations	32
Management’s Response	32
OIG Comment	33
Appendix A: Scope and Methodology	34
Appendix B: Management’s Response	37
Abbreviations	41



Introduction

Objective

Recent events at federal agencies have highlighted the importance of an effective employee separation process to mitigate reputational, security, and other risks to federal agencies. We conducted this audit to examine the Consumer Financial Protection Bureau's (CFPB) offboarding process for separating employees and contractors. Our objective was to assess the CFPB's controls over the offboarding process for the return of property,¹ records management, and conflicts of interest and to determine whether those controls are operating effectively to mitigate reputational and security risks.

To achieve this objective, we reviewed the CFPB's policies, procedures, and offboarding practices related to the return of property, records management, and conflicts of interest. We interviewed CFPB officials and reviewed documentation for employees² and contractors who separated from the CFPB during fiscal year (FY) 2016.³ We also interviewed three federal financial regulators to understand their offboarding practices, policies, and overall processes. Details on our scope and methodology are in appendix A.

Background

Overview of the CFPB's Offboarding Process

During FY 2016, 188 employees, including regional and remote employees, separated from the CFPB. Employee separations can occur due to an employee's resignation, retirement, or transfer to another federal agency.⁴ Additionally, approximately 175 contractors separated from the CFPB during FY 2016.⁵ Contractor separations can occur due to contract expiration, voluntary separations, reassignment by the vendor, or performance-related issues.

On April 8, 2013, the CFPB issued its first *Off-Boarding Policy*, which covers the separation process for all CFPB employees and contractors.⁶ The *Off-Boarding Policy* outlines that prior to separation, employees and contractors are required to return all government-issued property, including badges, and any federal records in their possession. Executive employees should also receive ethics counseling on conflicts of interest, specifically, postemployment restrictions. Although contractors do not receive an ethics briefing, they are required to sign nondisclosure agreements (NDAs) before beginning work at the CFPB.

¹ For the purposes of this audit, *property* refers to information technology assets (laptops, BlackBerrys, and IronKeys) and badges.

² Unless otherwise noted, the term *employees* includes nonexecutive employees, executive employees, and interns.

³ For the CFPB, FY 2016 was from October 1, 2015, through September 30, 2016.

⁴ The CFPB informed us that employees who are involuntarily separated are offboarded by the CFPB's Employee Relations Office; these separations are not within the scope of this audit.

⁵ A contractor is an individual who works under a CFPB contract or subcontract.

⁶ We conducted our audit using the CFPB's 2013 *Off-Boarding Policy*. During our audit, the CFPB revised its *Off-Boarding Policy*; the revised policy became effective in April 2017.

Multiple CFPB offices are involved in the offboarding process. The offices that support the areas within our scope include the Office of Human Capital (OHC), the Office of Security Programs (OSP), the Office of Technology and Innovation (T&I), the Records Management Office (RMO), the Ethics Office, and the Office of the Chief Procurement Officer (Procurement). For the purposes of this report, we refer to these offices as *performing offices*. Each performing office is required to complete its offboarding activities on or before the last day of the separating employee's or contractor's employment.

Offboarding requirements may differ depending on whether the separating individual is an employee or a contractor. Additionally, the Ethics Office and RMO have supplemental offboarding procedures for separating executive employees, which differ from nonexecutive employees based on federal requirements.

The Offboarding System

The CFPB inputs employee and contractor departure information into an automated system, referred to as the offboarding system, which is part of a larger information technology (IT) management system called Remedyforce. Departure information includes the individual's name, departure date, duty station, and reason for separation. The system notifies the performing offices of impending employee and contractor separations through automatically generated emails. The larger IT management system also contains an IT asset inventory information database, referred to as the IT asset management system.

The Employee Offboarding Process

The steps for offboarding separating employees are as follows:

1. The supervisor notifies OHC of an employee's impending separation by providing the employee's departure information.
2. OHC enters the employee's departure information into the offboarding system.
3. The system automatically emails the performing offices, signaling them to begin their respective offboarding activities.
4. Each performing office works with the employee to complete all offboarding procedures.

The Contractor Offboarding Process

The steps for offboarding separating contractors are as follows:

1. The contractor notifies his or her contracting officer's representative (COR)⁷ of his or her impending separation date, which may be predetermined by the contract.
2. The COR enters the contractor's departure information into the offboarding system.

⁷ CORs are CFPB employees designated to perform specific technical and administrative functions on individual contracts, including oversight of contractors' performance.

3. The system automatically emails the performing offices, signaling them to begin their respective offboarding activities.
4. The COR works with the performing offices to complete all necessary offboarding actions for the separating contractor.

CFPB Offices That Support Offboarding Activities

Below is a brief description of each performing office and its offboarding roles and responsibilities related to the return of property, records management, and conflicts of interest.

The Office of Human Capital

OHC is responsible for human resources services for the CFPB. With respect to employee separations, OHC is responsible for notifying the other performing offices by entering employee departure information into the offboarding system. In addition to the offboarding system, OHC enters employee separation information into one of its human resources systems, which houses employee personnel data. OHC does not initiate contractor separations.

The Office of Security Programs

OSP, located within the Office of Administrative Operations, is responsible for physical security at the CFPB's headquarters building,⁸ including granting employees, contractors, and visitors access to the headquarters building and administering the building access system. The CFPB's building access system controls access to the headquarters building and maintains badging information for CFPB headquarters staff. OSP also issues personal identity verification (PIV) badges⁹ for employees and site badges¹⁰ for interns and contractors, which allow those individuals access to the headquarters building. The CFPB issues PIV badges in accordance with Homeland Security Presidential Directive 12.¹¹ The U.S. Department of Commerce's National Institutes for Standards and Technology (NIST) provides a standard for agencies to meet Homeland Security Presidential Directive 12 requirements.

On their last day of employment, CFPB employees and interns are responsible for returning their PIV or site badges to OSP. CORs are responsible for collecting contractor site badges on the contractors' last day onsite and returning them to OSP. Upon the separation of an employee, an intern, or a contractor, OSP is responsible for deactivating the associated badge in the building access system. OSP is also responsible

⁸ The CFPB's official headquarters building is located at 1700 G Street NW, Washington, DC. During the scope of our audit, the official headquarters building was being renovated and the CFPB occupied temporary office space at 1275 First Street NE, Washington, DC. For the purposes of this report, we consider the temporary office space to be the CFPB's headquarters building. In addition to its headquarters building, the CFPB leases office space in Washington, DC, and it has regional offices as well.

⁹ PIV badges are a form of federal government identification issued through the U.S. General Services Administration's USAccess program.

¹⁰ Site badges are temporary badges issued to interns and contractors so they may access the CFPB headquarters building.

¹¹ The August 2004 Homeland Security Presidential Directive 12 requires all federal government agencies to adopt the new PIV standard for secure and reliable identification.

for deactivating employee PIV badges in the U.S. General Services Administration's (GSA) USAccess system,¹² which is not connected to the building access system.

The Office of Technology and Innovation

T&I is responsible for maintaining and managing the CFPB's IT assets, including laptops, mobile devices (BlackBerrys), and IronKeys, and documenting all IT asset assignments and returns.¹³ According to the *CFPB Service Desk Asset Management Standard Operating Procedures*, T&I staff perform certain offboarding functions for separating employees, such as collecting and verifying assigned IT assets and entering the IT asset return information into the IT asset management system. For separating contractors, T&I follows the same steps but coordinates with the applicable COR to collect any IT assets issued to contractors.

The following IT asset management forms are used to assist in the assignment and collection of IT assets:

- New Employee IT Asset Request Form: Includes the asset, its serial number/service tag, its barcode number, the individual to whom the asset is assigned, the asset assignment date, and the T&I representative's signature and date.
- IT Asset Property Return/Move Form: Includes the asset returned, its serial number/service tag, its barcode number, the individual who was issued the asset, the signature of the individual who returned the asset, and the T&I representative's signature and date.
- IT Asset Management Equipment Request Form: Includes the asset requested, its serial number/service tag, its barcode number, the individual to whom the asset is assigned, and the T&I representative's signature and date.
- IT Asset Management Equipment Property Replacement Receipt Form: Includes the asset returned and its serial number/service tag, the replacement asset, the replacement asset's serial number/service tag, the individual to whom the replacement asset is assigned, and the T&I representative's signature and date.

The Records Management Office

RMO is located within the Office of Administrative Operations and is responsible for ensuring that federal records created or received remain in the custody of the CFPB and are not removed without the proper approval.¹⁴ RMO is responsible for helping offboarding employees identify any federal records in their possession, conducting records management departure briefings, and obtaining a signed copy of the CFPB's Records Management Departure Form. This form instructs separating employees to not remove, delete, or destroy any federal records or copies upon their separation from the CFPB. Further, RMO is responsible for ensuring that records subject to a litigation hold are properly transferred. Records

¹² GSA's USAccess program enables participating federal government agencies to issue credentials and activate and manage PIV badges through web-based portals.

¹³ An IronKey is a type of encrypted portable storage device.

¹⁴ The Federal Records Act (44 U.S.C. § 3301) defines federal records as "all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under federal law or in connection with the transaction of public business."

become subject to a litigation hold when the employee or contractor is notified that the CFPB has received a threat of a litigation filing or an actual litigation filing, and the employee or contractor is in possession of pertinent records. For separating contractors, RMO informed us that the office communicates with the CORs regarding records management responsibilities.

The Ethics Office

The Ethics Office oversees the CFPB's government ethics program, which includes conflicts of interest that apply to CFPB employees separating from the federal government.¹⁵ As part of its offboarding procedures, the Ethics Office provides guidance on postemployment restrictions to separating executive employees. Specifically, the Ethics Office is responsible for conducting postemployment ethics briefings. The Ethics Office also administers the CFPB's public financial disclosure program and is responsible for notifying CFPB executive employees of their responsibility to submit public financial disclosure reports upon separation.¹⁶ The Ethics Office is not responsible for advising contractors on conflicts of interest (see The Office of the Chief Procurement Officer section below).

The Office of the Chief Procurement Officer

Procurement oversees purchasing for the CFPB in compliance with federal procurement rules and regulations. Procurement is not directly involved in offboarding contractors; however, the office is responsible for designating CORs, who have oversight responsibilities for contractor offboarding. Procurement is ultimately responsible for ensuring that CORs are complying with and completing all associated tasks related to offboarding. Procurement informed us that it has COR advisors who provide CORs with assistance and guidance during the contractor offboarding process. With respect to conflicts of interest, CORs obtain signed NDAs from contractors before they begin work at the CFPB.¹⁷ CORs are responsible for retaining signed NDAs.

Commendable Action: The CFPB Has Begun to Revise Its Offboarding Process

In June 2016, the Operations Division created an agencywide steering committee to conduct a review of the CFPB's offboarding process and, upon completion of its review, recommended eight improvements to the CFPB's process. Some of the improvements include identifying a single owner of the offboarding function, clarifying performing offices' roles and responsibilities, clarifying the roles of Procurement and the CORs, updating the *Off-Boarding Policy*, and documenting standard operating procedures (SOPs).

In April 2017, the CFPB revised its *Off-Boarding Policy* to identify OHC as the policy owner. OHC is responsible for reviewing and coordinating future *Off-Boarding Policy* updates and monitoring the

¹⁵ Title 18, section 207, of the *United States Code* imposes postemployment restrictions on individuals who have separated from federal government service.

¹⁶ Title I of the Ethics in Government Act of 1978, as amended, requires senior officials in the executive, legislative, and judicial branches to file public reports of their finances as well as other interests outside the federal government.

¹⁷ The NDA outlines a contractor's responsibilities when being granted conditional access to certain CFPB documents and records and describes any potential legal actions that could be taken against contractors should they disclose any information that may pose a threat to the security of the CFPB.

program's effectiveness, compliance, and continued improvement. As a result of the policy revision, the *Off-Boarding Policy* defines, for each performing office, the expanded roles and responsibilities for executing all offboarding tasks, maintaining their respective SOPs, and certifying in the offboarding system when an offboarding task is complete. Some additional revisions include updates to instructions, forms, and checklists for separating employees and contractors.

For our specific audit focus areas, the revised *Off-Boarding Policy* requires that separating employees

- return badges no later than the effective separation date
- return IT equipment by arranging a pickup time with T&I
- respond to a request for records management briefing, if required
- ensure receipt of postgovernment ethics briefing materials provided by the Ethics Office

The revised *Off-Boarding Policy* requires that when contractors separate, their offboarding actions have to be coordinated with their COR. Specifically, contractors are required to

- return badges to the COR
- return government property to the COR
- certify that they are leaving all paper records with the COR
- certify that they have saved all electronic records to a specific location as instructed by the COR

In addition to the policy revisions, the CFPB enhanced Remedyforce by designing a workflow system that allows the performing offices to process, monitor, and verify that all offboarding tasks are completed.



Finding 1: The CFPB Did Not Deactivate All Badges Timely for Separating Employees and Contractors and Did Not Always Maintain a Record of Badges' Collection Status

We found that OSP did not deactivate PIV badges timely and did not always maintain a record of the badges' collection status. We also found that OSP's building access system does not contain a complete record of all employees and contractors working in the CFPB's headquarters building. NIST, GSA, and the U.S. Government Accountability Office (GAO) provide agencies with a requirement or guidance related to collecting and deactivating PIV badges, maintaining a record of returned PIV badges, and maintaining complete and accurate information. The CFPB's Building Security Policy does not address collecting and deactivating PIV or site badges from separating employees, interns, and contractors. In addition, OSP has not established consistent practices for deactivating badges and maintaining badging records, including badges' collection status. If these control deficiencies are not corrected, the CFPB risks unauthorized access to its headquarters building.

The CFPB Did Not Deactivate PIV Badges Timely

OSP staff did not deactivate employee PIV badges in the building access and USAccess systems in a timely manner. OSP provided us with employee badge status reports generated by the CFPB's building access system.¹⁸ We reviewed these reports to determine when PIV badges were deactivated in relation to the associated employee's separation.

With respect to the CFPB's building access system, we found the following:

- The PIV badges for 2 of 47 separated headquarters employees¹⁹ (4 percent) were in *active* status in the building access system. We observed OSP staff deactivating the badge for one of these employees; the deactivation occurred almost 8 months after separation. For the other employee, the CFPB confirmed and we verified that the PIV badge was deactivated; this deactivation occurred almost 13 months after separation.

¹⁸ CFPB badge status reports indicate whether PIV and site badges are *activated*, *returned*, or *deactivated* in the building access system.

¹⁹ Remote or regional employees were removed from the employee sample because OSP does not enter their information into the building access system. When remote and regional employees visit the CFPB headquarters building, they are issued a temporary badge.

- The PIV badges for 17 of 47 separated headquarters employees (36 percent) were deactivated in the building access system 1 to 17 months after the employee's separation. The average length of time between separation and deactivation was 7.5 months.

Additionally, OSP provided us with the PIV badge status in GSA's USAccess system for headquarters, regional, and remote employees for our sample. We determined the following:

- The PIV badges for 6 of 54 nonexecutive employees (11 percent) and 1 of 10 executive employees (10 percent) were in *active* status in the USAccess system 9 to 16 months after separation. We observed OSP staff deactivating these 7 PIV badges in the USAccess system.

We noted that the *Building Security Policy* does not address deactivating PIV badges upon an employee's separation from the CFPB. OSP informed us that its practice is to deactivate a separating employee's PIV badge within 24–48 hours of the individual's last day in the building and that OSP is responsible for timely deactivating PIV badges regardless of whether the badges are turned in. NIST's Federal Information Processing Standards Publication 201-2, *Personal Identity Verification of Federal Employees and Contractors*, requires that PIV badges be deactivated when a federal employee separates from federal service and no longer needs access to federal buildings or systems. The requirements also state that deactivation procedures must be in place to ensure that the PIV badge is collected and destroyed. If the badge cannot be collected, deactivation should be completed within 18 hours.

Through our meetings with other federal agencies, we learned that one agency considers PIV badge collection a high priority and requires its security office to collect PIV badges within 24 hours of the employee's exit date to ensure that access to the agency's facilities is timely terminated. Additionally, upon completion of its offboarding tasks, that agency's security office reports the information online in a SharePoint workflow system that centrally tracks the offboarding tasks completed by each performing office.

Another agency uses its human resources system to automatically send two types of employee separation reports to performing offices. One report lists all offboarding employees and contractors separating within 21 days, and the other lists those separating the current day and the next day. That agency's security office uses the reports to ensure that PIV badges are deactivated in the building access and USAccess systems in a timely manner. The agency also performs quarterly reconciliation reviews of separated employees in its building access system with the USAccess system and reviews the status of PIV badges that have been inactive in its building access system for at least 180 days.

OSP staff informed us that they rely on receiving the offboarding system notification or employees physically returning their badge on their last day of employment as the signal to deactivate badges in both the building access and USAccess systems. Additionally, OSP officials stated that they do not reconcile separation information in the building access and USAccess systems with the offboarding system notifications to ensure that PIV badges for all separated employees have been deactivated in both systems.

OSP's reliance on two different deactivation practices puts the CFPB's building security at risk. Separated employees may be able to gain unauthorized access to CFPB facilities and potentially remove federal records, restricted information, or CFPB property.

OSP Did Not Always Maintain a Record of Badges' Collection Status

OSP did not always maintain a record of the collection status for the PIV and site badges of separating employees, interns, and contractors. For PIV badges, OSP's practice was to mark the badge as *destroyed* in the USAccess system to indicate it was collected and destroyed. OSP provided evidence that PIV badges for 36 of 47 separated headquarters employees (77 percent) had been collected and destroyed. We could not determine the collection status for the remaining 11 (23 percent), because their status in the USAccess system was not denoted as *destroyed*, and because OSP does not maintain any in-house documentation of badge collection. Without documentation for the 11 remaining badges, it is unclear whether OSP collected those badges and did not update the USAccess system or whether OSP did not collect those badges.

For site badges, OSP maintains hard-copy site badge application forms; the form includes a *Received Site Badge* field that is initialed and dated when a badge is returned. OSP could not provide the site badge application form for 12 of 25 headquarters contractors and interns (48 percent). Of the remaining 13 separated headquarters contractors and interns, the site badge application *Received Site Badge* field was blank for 10 (40 percent) and did not indicate the collection status. Therefore, it is unclear whether the badges were collected for those individuals whose application form was missing or did not have the *Received Site Badge* field in their application completed. In addition, because site badge documentation is only maintained in hard-copy format, OSP may not be able to effectively monitor badges' collection status.

GSA manages the USAccess program and recommends that agencies use an inventory tool to record when PIV badges are collected and deactivated to ensure that proper inventory controls are maintained throughout the PIV badge life cycle.²⁰ Additionally, Federal Information Processing Standards Publication 201-2, *Personal Identity Verification of Federal Employees and Contractors*, directs agencies to collect PIV badges from separating employees when possible. Through our meetings with other federal agencies, we learned that one agency adds detailed comments in its building access system explaining when changes are made to the individual's account, including when a PIV badge is lost, reissued, or deactivated.

OSP does not have a process to record when PIV badges are not collected from separating employees. Additionally, OSP does not always record when site badges are not collected from separating contractors and interns. OSP officials informed us that the CFPB's building access system does not allow for comments to indicate whether a badge has been returned and, if so, the date of return. By centrally recording the collection status of separated individuals' PIV and site badges and reconciling those records with the offboarding system, the CFPB would improve its ability to ensure that all badges of separated individuals are deactivated. Ensuring deactivation of badges not returned would reduce the risk of unauthorized access to the building and the assets and records therein.

²⁰ GSA regularly communicates information to agencies on USAccess service enhancements, current program events, and recommendations for helping agencies run their USAccess programs.

The CFPB's Building Access System Was Missing Records and Contained Inaccurate Badging Records

OSP does not maintain complete badging records (the individual's name, badge identification number, and badge status) in its building access system for all employees and contractors working at the CFPB's headquarters building.²¹ During our review, OSP showed us the badging records of the separated employees and contractors whose names did not appear in the badge status reports from the building access system. We found that some records for separated individuals were missing or contained incomplete information. Specifically, we found the following:

- Badging records for 4 of 56 separated headquarters employees and interns (7 percent) and 7 of 16 headquarters contractors (44 percent) were missing from the building access system.
- Badging records for 7 of 56 separated headquarters employees and interns (13 percent) and 4 of 16 headquarters contractors (25 percent) were incomplete; they only included the individual's name and did not include information such as the badge identification number or the badge status.

Therefore, we could not determine when these individuals' site badges were deactivated in the building access system.

GAO's *Standards for Internal Control in the Federal Government* identifies the need for management to use and process quality information, which is appropriate, complete, and accurate. GAO also notes that quality information is used by management to make informed decisions while considering the relevant objectives and risks.²²

For the headquarters employees, OSP officials could not explain why the badging records were missing or incomplete in the building access system. For the headquarters interns and contractors, OSP attributed missing or incomplete badging records to a prior practice of deleting badging information. Specifically, OSP deleted separated contractor and intern badging information in the building access system and reassigned those badge numbers to other individuals. By deleting badging information, these separated individuals may appear in the building access system without any associated badge information. In 2016, OSP began directing its staff to modify the site badge status of separating contractors or interns from *active* to *deactive*, rather than deleting them from the system, and then assign those badge numbers to an onboarding contractor or intern.

To help ensure headquarters building security, the badge's deactivation status in the building access system for separated employees, interns, and contractors should align with the individual's actual employment status. Without complete and accurate badging records in the system, separated

²¹ Employees and contractors who do not work in the CFPB's headquarters building were removed from the sample because OSP does not enter their information into the building access system.

²² U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO-14-704G, September 2014.

employees, interns, and contractors, even without a badge, could gain unauthorized access to CFPB headquarters.

Management Actions Taken

OSP reported that the building access system is being upgraded. After the upgrades, the building access system will interface with the USAccess system and one of the CFPB's human resources systems. In addition, once an individual's separation date is entered into that human resources system, the individual's badge should be automatically deactivated in the building access and USAccess systems.

Recommendations

We recommend that the Chief Operating Officer

1. Develop policies or procedures that meet applicable requirements to ensure the timely deactivation of PIV badges and site badges in the building access system and PIV badges in the USAccess system upon an individual's separation.
2. Finalize the building access system upgrade to ensure that PIV badges and site badges are automatically deactivated in the building access system and that PIV badges are automatically deactivated in the USAccess system upon an individual's separation.
3. Develop a process to maintain
 - a. the badge status history for separated employees, interns, and contractors.
 - b. a centralized record of PIV and site badge collection, including the separated individual's name, collection status and date, badge type, and badge number, and periodically reconcile that record with employee and contractor personnel data.
4. Identify and correct the information for all separated employees and contractors in the building access system and for separated employees in the USAccess system to ensure that all badges are properly deactivated.

Management's Response

In its response to our draft report, the CFPB concurs with our recommendations. For recommendation 1, the Chief Operating Officer has designated OSP to manage processes associated with physical security access, including the timely deactivation of site badges and PIV badges. Further, OSP plans to finalize its draft physical security offboarding SOP in March 2018.

For recommendation 2, the Chief Operating Officer will review the roles and responsibilities of the respective offices to ensure that, for separating contractors and employees, building access is deactivated and badges are terminated on the effective separation date. In addition, OSP will continue collaborating with T&I and the Identity, Credential, and Access Management program to explore and implement capabilities to automate badge and building access termination.

For recommendation 3, OSP plans to develop and implement a method to record badge collection. OSP will work with the building access system vendor to enhance the system capabilities to incorporate badge status.

For recommendation 4, OSP will establish an active employee baseline within the building access and USAccess systems.

OIG Comment

We believe the actions described by the CFPB are responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.



Finding 2: The CFPB Did Not Maintain Complete Documentation for IT Assets Assigned to Separating Individuals

T&I did not consistently maintain documentation of IT asset assignment and returns for separated employees and contractors. The *CFPB Service Desk Asset Management Standard Operating Procedures* describes the accountability controls for tracking and recording assets throughout the asset life cycle, including the use of IT asset management forms to assist in the collection of IT assets. The CFPB's controls over IT asset documentation were not designed and operating effectively to ensure that IT asset assignment documentation was maintained for separating employees and contractors. Without complete IT asset documentation, the CFPB may not be able to ensure that separating individuals have returned their IT assets, which increases the risk of data loss or theft.

T&I Did Not Consistently Maintain IT Asset Documentation

We found instances in which T&I did not maintain documentation on the assignment and return of laptops, BlackBerrys, or IronKeys. T&I provided us with asset-related documentation for some employees and contractors who separated during FY 2016; however, T&I could not provide complete documentation for 93 percent of separated employees and 20 percent of separated contractors. As a result, we had limited success in verifying assets returned by separating employees and contractors. Specifically, we found the following:

- For 3 of 76 separated employees (4 percent), we could not determine what assets were assigned and whether any assets were returned. T&I could not provide us with the IT Asset Property Return/Move Form or an IT asset assignment form for these individuals.²³
- For 1 of 76 separated employees (1 percent), we could not determine whether T&I collected the assigned BlackBerry. T&I could not provide us with the IT Asset Property Return/Move Form for the assigned BlackBerry for that individual. In addition, we found that the timing of the laptop collection for that individual was not clear. Specifically, the laptop collection was not recorded in Remedyforce upon separation of the employee; the first entry for the laptop collection in Remedyforce was in December 2016, 5 months after the employee's separation in July 2016.
- For 52 of 76 separated employees (68 percent) and 5 of 25 separated contractors (20 percent), we could not verify whether all IT assets assigned to those individuals were returned. T&I provided us with the IT Asset Property Return/Move Form for those 52 employees and 5 contractors; however, T&I could not provide us with any IT asset assignment forms.

²³ We use the term *IT asset assignment form* to mean any of the following: New Employee IT Asset Request Form, IT Asset Management Equipment Request Form, and IT Asset Management Equipment Property Replacement Receipt Form.

- For 15 of 76 separated employees (20 percent), T&I provided us with IT asset assignment forms; however, T&I could not provide us with the IT Asset Property Return/Move Form. We verified that the assets in question were still at the CFPB by reviewing an asset history log from Remedyforce.

The CFPB's 2013 *Off-Boarding Policy* states that upon separation, all individuals have an obligation to return all government-issued assets. Further, the *CFPB Service Desk Asset Management Standard Operating Procedures* describes the accountability controls for tracking and recording assets throughout the asset life cycle, including the use of IT asset management forms to assist in the collection of IT assets. We learned that one federal agency uses an electronic ticketing system to track IT assets assigned to employees and to ensure that all assigned IT assets are collected from separating employees. In addition, the agency's electronic ticketing system sends the asset management group reminders when someone is separating, and the group generates a list of IT assets assigned to the separating employees.

The CFPB informed us that for 34 of 76 separated employees, it could not provide laptop assignment documentation because the U.S. Department of the Treasury had issued those employees' laptops.²⁴ In December 2015, T&I began importing inventory control information, such as serial numbers and assigned user names, for laptops into Remedyforce. Although T&I is now tracking IT assets in Remedyforce, the system only maintains the history of the asset and does not maintain the history of IT assets assigned to and collected from employees or contractors who have separated from the CFPB. We note that the National Archives and Records Administration has issued a *General Records Schedule* specific to employee general technology management records, which includes the length of time to retain records associated with the return of property.

Because T&I had not entered all IT assets into Remedyforce for the period of our review, we could not verify whether all employees and contractors who separated in FY 2016 returned all their IT assets. Without maintaining documentation of the assignment and return of IT assets, the CFPB may not be able to ensure it is collecting all assigned IT assets upon an individual's separation, which may increase the risk of data loss or theft.

Management Actions Taken

In September 2017, the CFPB informed us that the asset management SOP is in draft and the new offboarding process includes steps to escalate notification and the associated timelines when assets are not returned by separated employees and contractors.

²⁴ Prior to the confirmation of the initial CFPB Director, the Dodd-Frank Wall Street Reform and Consumer Protection Act assigned to the Secretary of the Treasury certain CFPB functional responsibilities, such as IT infrastructure.

Recommendations

We recommend that the Chief Information Officer

5. Develop and implement procedures to ensure that IT assets assigned to individuals and collected from individuals are documented on the respective forms and updated in Remedyforce timely.
6. Maintain a history of IT assets assigned and collected in Remedyforce for all separated employees and contractors in accordance with the applicable National Archives and Records Administration's *General Records Schedule*.

Management's Response

In its response to our draft report, the CFPB concurs with our recommendations. For recommendation 5, T&I is working to finalize its offboarding SOPs. Additionally, T&I plans to update other related SOPs to describe the requirements for tracking assets and assignment forms.

For recommendation 6, T&I has consulted with RMO and plans to implement the record data retention requirements within its asset management tool.

OIG Comment

We believe that the actions described by the CFPB are responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.



Finding 3: RMO Did Not Always Perform Its Records Management Responsibilities for Separating Individuals

RMO did not always collect records departure forms or conduct departure briefings for separating nonexecutive and executive employees as required by RMO's *Records Management Procedure for Departing Employees*. In addition, the procedure does not address interns and contractors; thus, those individuals may not have been aware of their records responsibilities. The CFPB's controls over records management were not designed and operating effectively to ensure that separating individuals were aware of their records responsibilities. As a result, separating employees and contractors may not be aware of the CFPB's records requirements upon separation and may remove information or share nonpublic information.

RMO Did Not Always Collect Records Departure Forms or Conduct Records Departure Briefings for Nonexecutive and Executive Employees

RMO could not provide us with signed copies of the CFPB's Records Management Departure Form for 12 of 54 nonexecutive employees (22 percent) and 4 of 10 executive employees (40 percent). Separately, instead of completing a departure form, 6 of 54 nonexecutives (11 percent) and 1 of 10 executives (10 percent) submitted an email to RMO stating that they received notification of the CFPB's records management procedures. However, some of these emails did not indicate whether the sender had records subject to a litigation hold, which is information included on the departure form. Additionally, we found that RMO did not consistently conduct departure briefings for separating nonexecutives and executives.

The *Records Management Procedure for Departing Employees* states the following:

- Employees will sign departure forms prior to separation, acknowledging that they are aware of their records management responsibilities.
- RMO will conduct departure briefings for all separating employees to ensure the protection and management of all federal records.
- RMO will ensure that records subject to a pending litigation hold are properly transferred.

In addition, the CFPB's *Procedures for Litigation Hold* states that all departing employees with records subject to a litigation hold are obligated to inform RMO about any impending separation so that RMO can arrange for the preservation of potential evidence.

RMO did not adhere to its records policy and procedures to collect departure forms and conduct departure briefings for all separating employees. RMO's records management procedures do not include

guidance on how Records Management Departure Forms should be maintained; further, the procedures do not require RMO to follow up when an employee does not respond to requests to complete the departure form or does not fill out the form in its entirety.

If separating employees do not complete a departure form or receive a briefing, they may not be aware of their records management responsibilities and may remove and possibly share CFPB records, including those subject to a litigation hold. All federal records need to be safeguarded; however, the safeguarding of records subject to a litigation hold is of greater importance due to the records' sensitive nature. Additionally, according to an RMO official, failure to communicate records requirements to executive employees tends to carry a greater risk because of their exposure to sensitive information and because their records contain more historical value. If separating employees are not aware of their records management responsibilities, the agency may be at risk of nonpublic information being improperly shared or removed.

The Records Management Procedure Does Not Specify Guidance for Interns

We found that RMO could not provide us with a signed copy of the Records Management Departure Form for 5 of 12 interns (42 percent) and could not provide documentation that departure briefings were conducted. RMO stated that it conducts mass departure briefings for interns, rather than individual briefings. However, the CFPB could not provide us with documentation to show that any mass departure briefings were conducted in FY 2016.

The CFPB's *Records Management Procedure for Departing Employees* states that RMO will collect departure forms, ensure records subject to a litigation hold are transferred properly, and conduct departure briefings for all separating employees; however, the procedure does not specifically reference interns. RMO stated that it considers interns low risk because they are not exposed to nonpublic records. We learned, however, that one intern in our sample did have records subject to a litigation hold; for this reason, we believe that interns who have records subject to a litigation hold should receive an individual departure briefing.

Without receiving an individual departure briefing, interns may not know that they are obligated to inform RMO of any litigation hold notices. Additionally, without the submitted and signed departure forms, RMO may not be aware that interns have records subject to a litigation hold. In turn, interns may not properly dispose of those records; they may unknowingly remove sensitive materials and share this information inappropriately.

RMO Does Not Provide Guidance to CORs Related to Contractor Separation

For 19 of 25 contractors (76 percent), we could not verify whether RMO had any communication with the COR to verify that separating contractors submitted records associated with the contract prior to their separation. The records management procedure does not provide guidance to the CORs regarding separating contractors and records management.

An RMO official informed us that the office coordinates with CORs on a regular basis to identify pending contractor separations and to ensure that records management is covered as part of contractor offboarding procedures. However, we interviewed three CORs for separating contractors in our sample, and two stated that they did not have any communications with RMO. Those two CORs thought the contractor's program manager was responsible for obtaining all records from the contractor before separation.

If records management procedures do not address roles and responsibilities associated with separating contractors and their CORs, CORs may be unaware that they should provide contractors guidance on records management procedures when separating. Additionally, CORs may not inform RMO when contractors submit contractor records prior to separation. Not informing contractors of their records management responsibilities or collecting contractor-prepared records increases the CFPB's security and reputational risk.

Management Actions Taken

In June 2017, RMO replaced its *Records Management Procedure for Departing Employees* with *Records Management Departing Employees Standard Operating Procedures*. Some updates include

- procedures to guide Records Management Specialists on following up when departing employees are not responsive to a request to set up an interview
- guidance on maintaining signed and submitted departure forms
- guidance to CORs on how to handle contractor separations, which includes conducting annual training and obtaining a signed departure form from contractors
- procedures that address interns and contractors

Recommendations

We recommend that the Chief Administrative Officer

7. Identify a process for collecting and maintaining all records departure forms for separating employees and interns, and develop a procedure to obtain the signed form electronically.
8. Update the *Records Management Procedure for Departing Employees* to specify RMO's responsibilities with respect to interns, including a requirement to conduct an individual exit interview for those interns with records subject to a litigation hold.

Management's Response

In its response to our draft report, the CFPB concurs with our recommendations. With regard to recommendation 7, RMO updated its records management departure SOP in November 2017.

For recommendation 8, RMO is in the process of revising its procedures, forms, and policies to specifically address interns. In addition, RMO plans to conduct individual interviews with those interns who have records subject to a litigation hold.

OIG Comment

We believe that the actions described by the CFPB are responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.



Finding 4: The Ethics Office Informed Executive Employees of Postemployment Restrictions and of the Requirement to Submit Public Financial Disclosure Reports Timely

Based on our testing, we determined that the Ethics Office’s controls over the offboarding process for conflicts of interest, such as informing executive employees of postemployment restrictions and their requirement to complete Office of Government Ethics (OGE) Form 278e, which is a public financial disclosure report, were designed and operating effectively.

We found that the Ethics Office provided an ethics briefing on postemployment restrictions to all executive employees who separated from federal government service in FY 2016. These briefings were conducted by the ethics official, and the briefing documentation was signed by the separating executive employee on or before the separating executive employee’s last day of employment at the CFPB. The postemployment briefing describes the responsibilities of separating executive employees related to compensation for representational services and the disclosure of nonpublic government information. During the briefing, the Ethics Office also informs executive employees of the public financial disclosure reporting requirements, specifically, the requirement to file OGE Form 278e. We confirmed that all the executive employees submitted OGE Form 278e within the required time frame.

Management’s Response

In its response to our draft report, the CFPB notes that it is pleased we found the Ethics Office’s offboarding processes to be designed and operating effectively.



Finding 5: The CFPB Maintained NDAs for Most Contractors

The CFPB provided us with a signed NDA for 24 of 25 contractors; the CFPB was not able to locate one of the NDAs. As a result, we could not determine whether an NDA had been signed by that contractor. The *Federal Acquisition Regulation* outlines that NDAs are obtained to prohibit disclosure of nonpublic information accessed through performance of a government contract.²⁵ If a contractor does not sign an NDA, the CFPB is at risk of having nonpublic information inappropriately disclosed.

The CFPB Did Not Have an NDA on File for One Contractor

The COR is responsible for obtaining signed NDAs from contractors before they begin work for the CFPB. The CFPB informed us that NDAs are maintained in the COR file or are filed with OSP, depending on when the NDA was completed.²⁶ The NDA outlines a contractor's responsibilities when being granted conditional access to certain CFPB documents and records. It also describes any potential legal or other actions that could be taken against contractors should they disclose any information that may pose a threat to the security of the CFPB.

The CFPB could not locate a signed NDA for one contractor. Without a signed NDA for each contractor, the CFPB increases the risk that a contractor is unaware of the trust the U.S. government has placed in him or her to protect sensitive CFPB information from unauthorized disclosure. In addition, without a signed NDA on file, the CFPB may not be able to take any action should the contractor disclose information inappropriately.

Management Actions Taken

In January 2017, the CFPB issued its *Conflicts of Interest Policy and Procedures for Contractors*, which addresses organizational conflicts of interest and NDAs. In August 2017, we learned the CFPB instructed CORs to save NDAs in their COR file and updated contractor NDAs to include contract solicitation and instructional language. This language requires that each contractor or subcontractor who is selected for an award complete, sign, and return the completed form to the COR prior to beginning work. Additionally, effective October 2017, CORs will use an offboarding checklist that enables them to verify receipt of a fully executed and filed NDA for a departing contractor.

²⁵ The *Federal Acquisition Regulation* contains uniform policies and procedures for acquisition by all executive agencies. Although the CFPB has determined that it is not required to follow the *Federal Acquisition Regulation*, the agency has made a policy decision to conduct all its procurements in accordance with the *Federal Acquisition Regulation*.

²⁶ CORs used to send NDAs to OSP as part of the background check process.

Recommendation

We recommend that the Chief Procurement Officer

9. Review contract files and determine whether NDAs are missing for any of the individuals associated with those files. If so, obtain a signed NDA for each of those individuals.

Management's Response

In its response to our draft report, the CFPB concurs with our recommendation. For recommendation 9, Procurement plans to review “a significant sampling of COR files” to confirm whether all contractor personnel have a signed NDA. If an NDA is missing and the individual is still providing support, Procurement will obtain a signed NDA. Procurement also plans to refine its current procedures based on the results of its review and provide training to CORs on the importance of retaining signed NDAs in COR files.

OIG Comment

We believe that the actions described by the CFPB are responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.



Finding 6: Certain CFPB Separation and Contractor Data Are Not Accurate and Complete

When we attempted to validate the CFPB's separation data for its employees and contractors, we found that the data in the CFPB's offboarding system were not accurate and complete. In addition, the CFPB does not maintain a centralized list of its contractors. GAO's *Standards for Internal Control in the Federal Government* states, "Management should use quality information to achieve the entity's objectives." GAO further states that "management should obtain data from reliable sources to ensure the data is reasonably free from error and accurately represented." According to the CFPB, the information in the offboarding system was not being verified. We also learned that the CFPB does not have a process owner or a centralized system to monitor and track contractor information. Therefore, we were unable to verify that all contractors who separated in FY 2016 were in the offboarding system. Without improved controls regarding the accuracy and completeness of separation data, the CFPB may not have assurance that all the separation data in the offboarding system are accurate. In addition, without a centralized list of contractors, the CFPB may not be able to determine the number of contractors working for the agency, the contractors' status, and which contractors may require access to CFPB facilities.

The CFPB Does Not Have a Centralized Contractor List or Accurate Separation Data

To select our contractor audit sample, we requested a list of contractors who separated from the CFPB during FY 2016. We found that the CFPB does not maintain a centralized list of its contractors; in response to our request, the CFPB provided us with separated employee and contractor data from its offboarding system. We encountered some issues when validating these separation data, including finding duplicate entries and inaccurate information, such as employees labeled as contractors. For the period of our review, the CFPB informed us that the offboarding system was not an authoritative source for information because the data were not verified for accuracy. Since the CFPB does not have a unique identifier to differentiate contractors from employees in the offboarding system, we had to manually extract the contractor data from the employee separation data. Despite the offboarding system having inaccurate separation data for employees, the CFPB was able to provide us with separated employee data from one of its human resources systems. We tested the reliability of the separated employee data and determined that the data provided a reasonable level of assurance for sampling purposes.

GAO's *Standards for Internal Control in the Federal Government* states, "Management should use quality information to achieve the entity's objectives." One of the attributes that contributes to this principle is obtaining relevant data from reliable sources. Management should obtain data from reliable sources to ensure the data are reasonably free from error and accurately represented. We met with a federal agency that maintains a contractor personnel list in an electronic database. That agency's contractor personnel list, which includes each contractor's name and contract identification number, enables the agency to report on and identify contractors working at the agency.

We learned that at the time of our review, the CFPB did not have a process owner to centrally monitor and track contractor information or a centralized system to retain contractor information. Thus, we were unable to verify that all contractors who separated in FY 2016 were in the offboarding system. Without improved controls regarding the accuracy and completeness of separation data, the CFPB cannot be assured that separation data in the offboarding system are accurate. In addition, without a centralized list of contractors, the CFPB may not be able to determine the number of contractors working for the agency, the contractors' status, and which contractors may require access to CFPB facilities.

Management Actions Taken

During our audit, the CFPB developed the *Off-boarding of Contractor Personnel SOP*, which identifies Procurement as the process owner, and made updates to the offboarding system to address the mislabeling of personnel type and the misspelling of individuals' names. These updates include adding

- a dropdown box in which OHC staff or the COR can select the personnel type (*contractor or employee*)
- a dropdown box in which OHC staff or the COR can select the employee's or contractor's name from the email system instead of manually entering this information

Recommendations

We recommend that the Chief Procurement Officer

10. Identify a process for maintaining an accurate contractor personnel list in order to monitor and track contractor information.

We recommend that the Chief Human Capital Officer,

11. Once upgrades to the offboarding system have been fully implemented, develop a process to periodically reconcile new separation data in the offboarding system with one of the CFPB's human resources systems to ensure that the separation data are current, accurate, and complete.

Management's Response

In its response to our draft report, the CFPB concurs with our recommendations. For recommendation 10, Procurement created a master contractor roster in FY 2017 and plans to update the roster as contractor personnel are onboarded and offboarded. Procurement also plans to provide additional training to CORs to ensure that the contractor information is accurate. In addition, Procurement plans to benchmark with other federal agencies with regard to their process for maintaining contractor information and refine its process, as appropriate.

For recommendation 11, in FY 2018 OHC plans to begin monitoring the compliance of offboarding tasks in accordance with the revised *Off-Boarding Policy*, including a quarterly reconciliation of opened tickets in Remedyforce with personnel separation reports.

OIG Comment

We believe that the actions described by the CFPB are responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.



Appendix A: Scope and Methodology

Our scope covered the CFPB's controls over the offboarding process for the return of property (laptops, BlackBerrys, IronKeys, and badges), records management, and conflicts of interest for employees and contractors who separated in FY 2016 (October 1, 2015, through September 30, 2016). We define *employees* to include nonexecutives, executives, and interns. Specifically, we focused on the following three areas and the respective performing office's offboarding process:

- For return of property, we determined whether IT assets (laptops, BlackBerrys, IronKeys) and badges (PIV and site badges) were collected from separating employees and contractors.
- For records management, we determined whether separating employees were notified of their federal records management responsibilities. For contractors, we determined whether the CORs notified RMO that the contractors' obligations had been satisfied. We did not assess whether individual divisions developed tailored records procedures for separating employees or contractors.
- For conflicts of interest, we determined whether separating executive employees were informed of postemployment restrictions and the requirement for filing OGE Form 278e, the public financial disclosure report. In addition, we determined whether signed NDAs were maintained for contractors.

To accomplish our audit objective, we reviewed the following CFPB policies and procedures, specifically, the sections applicable to the offboarding process:

- *Off-Boarding Policy* (2013 original policy and 2017 revised policy)
- *Records Management Procedure for Departing Employees* (2012)
- *Policy for Records Management* (2012)
- *Building Security Policy* (2012)
- *CFPB Service Desk Asset Management Standard Operating Procedures* (2014)
- *CFPB Ethics Handbook* (2015)
- *Off-Boarding Standard Operating Procedure* (2016)
- *COR Resources* (2016)

Additionally, we reviewed the CFPB Office of the Chief Financial Officer's *Hiring and Separations: Exploratory Review*; Homeland Security Presidential Directive 12; the Federal Information Processing Standards Publication 201; a related NIST publication; and relevant GAO reports.

During FY 2016, 188 employees separated from the CFPB (10 executives, 109 nonexecutives, and 69 interns). We tested the reliability of the separated employee data and determined that the data provided a reasonable level of assurance. For testing purposes,

- We selected the entire population of 10 executive employees because they pose a greater risk based on their access to sensitive information and public financial disclosure reporting requirements upon separation.
- We statistically selected a random sample of 54 nonexecutive employees. Conclusions in our report that are based on the random sample of 54 can be projected to the population of nonexecutive employees.
- We nonstatistically selected a judgmental sample of 12 interns because we consider interns to be a lower risk. The sample was judgmentally selected based on the interns' location, grade, and date of separation. Because this was a nonstatistical sample, we were unable to project our conclusions to the entire population of interns.

During the same period, approximately 175 contractors separated from the CFPB. Based on our review, we were unable to verify that all contractors who separated in FY 2016 were in the offboarding system. Accordingly, we nonstatistically selected a judgmental sample of 25 contractors, based on their location and type of separation. As a result, we were unable to project our conclusions to the entire population of contractors.

We analyzed and tested internal controls related to the CFPB's offboarding process for the selected employees and contractors. Specifically, we performed testing in the following focus areas:

- Property returned (IT assets, PIV badges, and site badges)
 - 76 employees (10 executive employees, 54 nonexecutive employees, and 12 interns)
 - 25 contractors
- Records management
 - 76 employees (10 executive employees, 54 nonexecutive employees, and 12 interns)
 - 25 contractors
- Conflicts of interest
 - 10 employees (executive employees only)
 - 25 contractors

We interviewed staff in the performing offices who are involved in the offboarding process for employees and contractors. Specifically, we spoke to employees in OHC, RMO, T&I, OSP, Procurement, and the Ethics Office. We discussed their roles and responsibilities in the offboarding process and the controls in place to mitigate reputational and security risks.

We met with officials at three other federal financial regulatory agencies to understand their respective offboarding practices for the return of property, records management, and conflicts of interest.

We conducted our fieldwork from February 2017 through August 2017. Upon receipt of new documentation provided by the CFPB, we conducted additional fieldwork from November 2017 through December 2017. 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 the audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix B: Management's Response



1700 G Street NW, Washington, DC 20552

January 8, 2018

Ms. Melissa Heist
Associate Inspector General for Audits and Evaluations
Board of Governors of the Federal Reserve System &
Consumer Financial Protection Bureau
20th and C Streets, NW
Washington, DC 20551

RE: Evaluation of the CFPB's Off boarding Processes and Data

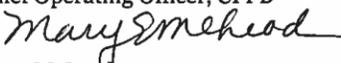
Dear Ms. Heist,

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report titled "*The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data*". We have reviewed the report and appreciate the recommendations provided to CFPB's controls over the offboarding process for the return of property, records management, and conflicts of interest. We are pleased that you found that the Ethics Office's offboarding processes are designed and operating effectively and that our other processes are generally in place. We agree that we need to strengthen controls surrounding the return of property and records management. The Office of Human Capital (OHC), as the new offboarding program owner, will monitor the compliance of the new policy and processes to ensure that all requirements are being met in a timely manner.

We appreciate the OIG's recognizing our commendable actions over the past year to proactively enhance the offboarding process. This was an intensive effort across multiple offices, resulting in a revised offboarding policy, updated processes and an upgraded system designed to promote compliance and accountability throughout the process.

We value your objective, independent viewpoints and appreciate the professionalism and courtesy consistently demonstrated by all OIG personnel throughout this review. We have provided comments for each recommendation.

Sincerely,


Sartaj Alag
Chief Operating Officer, CFPB

Mary McLeod
General Counsel, CFPB

consumerfinance.gov

**Response to recommendations presented in the Draft IG Report,
“The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes
and Data.”**

Recommendation 1: Develop policies or procedures that meet applicable requirements to ensure the timely deactivation of PIV badges and site badges in the building access system and PIV badges in the USAccess system upon an individual’s separation.

Management Response: The Bureau concurs with this recommendation. The Chief Operating Officer has designated the Office of Security Programs (OSP), within the Office of Administrative Operations, to manage processes associated with physical security access. As such, OSP will ensure timely deactivation of site badges and PIV badges as outlined in the Draft Physical Security Offboarding SOP which is expected to be completed in March, 2018.

Recommendation 2: Finalize the building access system upgrade to ensure that PIV badges and site badges are automatically deactivated in the building access system and that PIV badges are automatically deactivated in the USAccess system upon an individual’s separation.

Management Response: The Bureau concurs with this recommendation. The Chief Operating Officer (COO) will review roles and responsibilities of the respective office associated with this process to ensure that building access is deactivated and badges are terminated on the off-board effective dates for contractors and employees. Additionally, OSP will continue collaborating with Technology and Innovation (T&I) and the Identity, Credential, and Access Management (ICAM) program to explore and implement capabilities to automate badge and building access termination. In the interim, OSP will take immediate steps to establish an active employee baseline within the building access system and USAccess.

Recommendation 3: Develop a process to maintain

- a. the badge status history for separated employees, interns, and contractors.
- b. a centralized record of PIV and site badge collection, including separated individual’s name, collection status and date, badge type, and badge number, and periodically reconcile that record with employee and contractor personnel data.

Management Response: The Bureau concurs with this recommendation. The OSP will develop and implement a method to record badge collection. Additionally, OSP will work with the access system vendor to enhance the system capabilities to incorporate badge status. The Bureau is reviewing existing processes to ensure timely deactivation of badges while also ensuring that appropriate artifacts are established at collection and deactivation to meet both system and auditing requirements.

Recommendation 4: Identify and correct the information for separated employees and contractors in the building access system and for separated employees in the USAccess system to ensure that all badges are properly deactivated.

Management Response: The Bureau concurs with this recommendation. OSP will take immediate steps to establish an active employee baseline within the building access system and USAccess. The issue of card reutilization was self-identified by OSP staff and discontinued prior to the audit. While, there is no way to correct or recreate previously deleted information, going forward, OSP has revised processes to ensure accurate and timely deactivation of badges.

consumerfinance.gov

Recommendation 5: Develop and implement procedures to ensure that IT assets assigned to individuals and collected from individuals are documented on the respective forms and updated in Remedyforce timely.

Management Response: The Bureau concurs with this recommendation. The Office of Technology and Innovation (T&I) is working to finalize offboarding SOPs which addresses this recommendation. Additionally, T&I will update the on-boarding and transfer assets SOPs to describe requirements for tracking assets and assignment forms (or electronic signatures in the future).

Recommendation 6: Maintain history of IT assets assigned and collected in Remedyforce for all separated employees and contractors in accordance with the applicable National Archives and Records Administration's *General Records Schedule*.

Management Response: The Bureau concurs with this recommendation. T&I has consulted with the Records Management Office (RMO) and will implement the applicable record data retention requirements within the asset management tool.

Recommendation 7: Identify a process for collecting and maintaining all records departure forms for separating employees and interns, and develop a procedure to obtain the signed form electronically.

Management Response: The Bureau concurs with this recommendation. The RMO has developed a records management departure SOP (Nov. 2017) that fully addresses recommendation 7.

Recommendation 8: Update the *Records Management Procedure for Departing Employees* to specify the RMO's responsibilities with respect to interns, including a requirement to conduct an individual exit interview for those interns with records subject to a litigation hold.

Management Response: The Bureau concurs with this recommendation. The RMO is in the process of revising its procedures, forms, and policies to specifically address interns. The RMO will continue to hold group departure briefings for interns, and will conduct follow-up individual interviews with those interns with records subject to litigation holds.

Recommendation 9: Review contract files to determine whether NDAs are missing for any of the individuals associated with those files. If so, obtain a signed NDA for those individuals.

Management Response: The Bureau concurs with this recommendation. The Office of Procurement will review a significant sampling of COR files to confirm whether all contractor personnel have a signed NDA in the applicable COR file. If an NDA is missing and the contractor personnel is still providing support, Procurement will obtain a signed NDA. Based on the results of this review, the Office of Procurement will refine its current procedures, as required. The Bureau will also provide additional training to CORs to highlight the importance of signed and retained NDAs within COR files.

Recommendation 10: Identify a process for maintaining an accurate contractor personnel list in order to monitor and track contractor information.

Management Response: The Bureau concurs with this recommendation. In FY 2017, the Office of Procurement created a master contractor roster. As contractor personnel are onboarded and

consumerfinance.gov

offboarded, Procurement will update the roster. As a best practice, the Bureau will benchmark with other federal agencies on their process for maintaining contractor information and refine our process, as appropriate. Further, the Bureau will provide additional training to CORs on the Bureau's on-boarding and off-boarding procedures to ensure accurate contractor information.

Recommendation 11: Once upgrades to the offboarding system have been fully implemented, develop a process to periodically reconcile new separation data in the offboarding system with one of the CFPB's human resource systems to ensure the separation data are current, accurate, and complete.

Management Response: The Bureau concurs with this recommendation. As identified in the revised Offboarding Policy, OHC has programmatic oversight for all activities pertaining to offboarding. As of FY18, OHC will begin monitoring the compliance of off boarding tasks in accordance with the policy. This will include a quarterly reconciliation of opened tickets in RemedyForce compared to personnel separation reports to ensure accuracy and consistency in both systems.

consumerfinance.gov



Abbreviations

CFPB	Consumer Financial Protection Bureau
COR	contracting officer's representative
FY	fiscal year
GAO	U.S. Government Accountability Office
GSA	U.S. General Services Administration
IT	information technology
NDA	nondisclosure agreement
NIST	National Institute of Standards and Technology
OGE	Office of Government Ethics
OHC	Office of Human Capital
OIG	Office of Inspector General
OSP	Office of Security Programs
PIV	personal identity verification
Procurement	Office of the Chief Procurement Officer
RMO	Records Management Office
SOP	standard operating procedure
T&I	Office of Technology and Innovation

Report Contributors

Bettye Latimer, Project Lead

Shola Epemolu, Auditor

Shaundace Lewis, Auditor

Nathan Tenor, Auditor

Lindsay Mough, OIG Manager

Timothy Rogers, Senior OIG Manager for Management and Operations

Melissa Heist, Associate Inspector General for Audits and Evaluations

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



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