Office of Inspector General

Office of Program Audits and Evaluations
Report No. EVAL-17-007

Controls over Separating Personnel's Access to Sensitive Information

September 2017

Office of Inspector General

Executive Summary

Controls over Separating Personnel's Access to Sensitive Information

Report No. EVAL-17-007
September 2017

Why We Did the Evaluation

The Federal Deposit Insurance Corporation (FDIC) experienced a number of data breaches in late 2015 and early 2016 that involved employees who were exiting the Corporation. Between February and May 2016, the FDIC notified the Congress of seven major incidents in which departing employees inappropriately took significant quantities of sensitive information. The information taken was associated with financial institutions and their customers, creating the risk of unauthorized disclosure of examination, institution, law enforcement, and customer information and, in turn, identity theft. In response, the Chairman of the Senate Committee on Banking, Housing, and Urban Affairs requested that the FDIC Office of Inspector General examine issues related to the FDIC's policies governing departing employees' access to sensitive financial information.

Our evaluation objective was to determine the extent to which the FDIC has established controls to mitigate the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating personnel. We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Background

The FDIC Division of Administration (DOA) promulgates pre-exit clearance procedures for separating personnel (employees and contractors). These procedures include requiring that separating personnel complete a Pre-Exit Clearance Record to ensure that designated corporate officials have completed check-out activities to confirm, among other things, that their access to the Corporation's network and facilities is disabled. Separating personnel also complete a Data Questionnaire that requires them to identify where they have saved paper and/or electronic records and to certify that they are not removing any information related to the business of the Corporation. Division or office records liaisons are expected to review the Data Questionnaire for completeness and accuracy, and interview the separating individual if warranted. When these activities are completed, the individual's division, office, or contract Oversight Manager clears them for separation.

The FDIC has also taken technological measures to detect or prevent separating personnel from removing sensitive information from the Corporation. The Division of Information Technology uses a data loss prevention (DLP) tool to monitor and inspect FDIC data and flags potential security policy violations, including the unauthorized exfiltration of sensitive data through e-mail, printer activity, and external downloads. In March 2016, the FDIC also began limiting the use of removable media, such as computer disks and thumb drives, on FDIC computer equipment. Further, after June 30, 2017, the FDIC required all of its personnel to use Personal Identity Verification (PIV) cards to access facilities and information systems. Separating personnel surrender their PIV cards as part of the pre-exit clearance process, thereby preventing their access to FDIC facilities and information systems after separation.

Evaluation Results

FDIC Employee Pre-Exit Clearance Process. While the FDIC has established and implemented various control activities, we found that there were weaknesses in the design of certain controls, division and office records liaisons were not always following procedures, and opportunities existed to strengthen the pre-exit clearance process. As designed, the program controls do not provide reasonable assurance that the pre-exit clearance process will timely or effectively identify unauthorized access to or inappropriate removal and disclosure of sensitive information by separating employees.

Our testing of pre-exit clearance controls for a random sample of separating employees showed that most employees completed pre-exit clearance forms before leaving the Corporation. However, we found that division and office records liaisons were not reviewing data questionnaires before employees separated, as required by FDIC procedures, 41 percent of the time.

Based on our evaluation of DOA controls and interviews with other agencies, we identified several opportunities for strengthening the FDIC's pre-exit clearance process for employees, including:

- Designating a pre-exit clearance process owner and increasing program oversight,
- Actively managing the pre-exit clearance process and designating back-up resources,
- Assessing risks presented by individual separating employees,
- Defining policy for DLP use in the pre-exit clearance process,
- Improving pre-exit clearance forms used to identify where sensitive data is located and strengthening acknowledgments and warnings regarding breaches of sensitive information, and
- Continuing automation efforts to develop a centralized pre-exit clearance application.

We also learned that the Legal Division researched potential actions that the FDIC could undertake to minimize future breaches and discourage inappropriate behavior by current and former employees and contractors. The resulting guidance and recommendations had not been completed at the time we performed our work. However, we understand that staff of the various divisions involved (including Legal and DOA) have been working on revisions to the pre-exit clearance forms, and will be considering other process improvements and enhancements aimed at strengthening the FDIC's security posture in relation to separating personnel.

Contractor Pre-Exit Clearance Process. Separating contractor employees (contractors) may present greater risks than separating FDIC employees. We found several differences between the pre-exit clearance process for FDIC employees and contractors that increase risks related to protecting sensitive information when contractors separate. For instance, the Corporation may not know as much about a contractor's personnel history as it does for FDIC employees. In addition, contractors may depart without advance notice and the FDIC would not have sufficient time to complete its pre-exit clearance process. Also, contractor pre-exit clearance is decentralized among contract-specific FDIC oversight managers and is not subject to monitoring at the program level. Further, the priority review of network activity using the DLP tool is not conducted in pre-exit clearance for many contractors. We estimate that at least 43 percent of FDIC contractors that separated between October 1, 2015 and September 30, 2016 were not subject to DLP priority review.

Our testing of pre-exit clearance controls for a random sample of separating contractors showed that the FDIC is not consistently following procedures. For example, we could not locate clearance records for 46 percent of the contractors we sampled or find evidence that oversight managers signed clearance records before contractors separated 71 percent of the time. We also found that records liaisons did not review data questionnaires before contractors separated in 94 percent of the cases we reviewed, as required by FDIC procedures.

Based on our evaluation of DOA controls and interviews with other agencies, we identified several opportunities for strengthening the FDIC's pre-exit clearance process for contractors, including:

- Ensuring consistent controls between employee and contactor pre-exit clearance processes and improving related procedures; and
- Reiterating responsibilities and expectations for oversight managers and records liaisons, and requiring timely notice of separating contractors.

Recommendations

We made 11 recommendations intended to provide the FDIC with greater assurance that its controls mitigate the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating personnel. The FDIC provided a written response dated September 15, 2017 to a draft of this report. FDIC concurred with our recommendations and proposed corrective actions to be completed by September 30, 2018.

Contents

	Page
Background	2
Pre-Exit Clearance Procedures for FDIC Employees	2
Pre-Exit Clearance Procedures for FDIC Contractors	4
Data Loss Prevention Tool (DLP) and Technological Measures to Detect or Prevent the Removal of Sensitive Information	5
Evaluation Results	6
The FDIC's Employee Pre-Exit Clearance Process	6
Pre-Exit Clearance Control Weaknesses Limit Their Effectiveness	6
FDIC Records Liaisons Did Not Always Complete Pre-Exit Clearance Procedures Timely	8
The FDIC Should Strengthen the Employee Pre-Exit Clearance Process	10
The FDIC's Contractor Pre-Exit Clearance Process	14
Contractor Pre-Exit Clearance Controls Also Have Weaknesses	14
FDIC Records Management and Contracting Staff Did Not Always Follow Contractor Pre-Exit Clearance Procedures	15
The FDIC Should Strengthen the Contractor Pre-Exit Clearance Process	16
Recommendations	17
Corporation Comments and OIG Evaluation	18
Appendices	
1. Objective, Scope, and Methodology	19
2. Letter from the Chairman, Senate Committee on Banking, Housing, and Urban Affairs	21
3. October 2016 OIG Memorandum Communicating Preliminary Concerns with the Pre-Exit Clearance Process	23
4. OIG Review of Pre-Exit Clearance Program at Another Federal Agency	25
5. Glossary	26
6. Acronyms and Abbreviations	28
7. Corporation Comments	29
8. Summary of the Corporation's Corrective Actions	36
Tables	
1. Pre-Exit Clearance Controls Assessment for Employees	7
2. Employee Testing Results	9
3. Pre-Exit Clearance Controls Assessment for Contractors	14
4. Contractor Testing Results	16
Figures	
1. The FDIC's Employee Pre-Exit Clearance Process	3
2. The FDIC's Contractor Pre-Exit Clearance Process	5

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, Virginia 22226

Office of Program Audits and Evaluations
Office of Inspector General

DATE: September 18, 2017

MEMORANDUM TO: Arleas Upton Kea, Director
Division of Administration

/Signed/
FROM: E. Marshall Gentry
Assistant Inspector General for Program Audits and Evaluations

SUBJECT: *Controls over Separating Personnel's Access to Sensitive Information* (Report No. EVAL-17-007)

In late 2015 and early 2016, the Federal Deposit Insurance Corporation (FDIC) experienced a number of data breaches. In September 2015, the FDIC learned an employee from the FDIC's Office of Complex Financial Institutions in New York who had abruptly resigned took highly sensitive components of "living will" documents, which large financial institutions are required to produce pursuant to the Dodd–Frank Wall Street Reform and Consumer Protection Act.[1] These living wills, which contain both public and confidential sections, describe how the large financial institution would dissolve itself in a timely and orderly manner under the U.S. Bankruptcy Code[2] in the event of serious financial distress or failure of the company.

In October 2015, the FDIC learned that a former Division of Risk Management Supervision employee copied over 1,200 documents that contained social security numbers from customer bank data and other sensitive FDIC information onto a data storage device. These documents included Suspicious Activity Reports, Currency Transaction Reports, and customer data reports. The OIG determined, in its report entitled, *The FDIC's Process for Identifying and Reporting Major Information Security Incidents*,[3] that the incident should have been characterized as a "major incident" and that the FDIC failed to report it to Congress in accordance with Office of Management and Budget (OMB) guidance and the Federal Information Security Modernization Act.[4]

In total, there were seven major incidents that the FDIC reported to Congress.[5] Each of these incidents involved former FDIC employees inappropriately copying sensitive information, including customer data for 10,000 – 49,000 individuals. The FDIC estimated that approximately 200,000 individuals' information was involved in these incidents related to approximately 380 financial institutions.

---

[1] Public Law 111-203, section 165(d).
[2] See title 11 of the United States Code (U.S.C.).
[3] OIG Report AUD-16-004, dated July 7, 2016.
[4] Public Law 113-283.
[5] FDIC became aware of these incidents during the period from October 2015 through February 2016.

The then-Chairman of the Senate Committee on Banking, Housing, and Urban Affairs requested that the FDIC Office of Inspector General examine issues related to the FDIC's policies governing departing employees' access to sensitive financial information.[6] In response, the then-Acting Inspector General decided to conduct this review.[7]

Our evaluation objective was to determine the extent to which the FDIC has established controls to mitigate the risk of unauthorized access to and inappropriate removal and disclosure of sensitive information by separating personnel.[8] We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Appendix 1 of this report includes additional details on our objective, scope, and methodology. Appendix 2 contains the Senate Committee Chairman's letter. Additional appendices include a glossary, acronyms and abbreviations, the Corporation's comments on a draft of this report and its recommendations, and a summary of the Corporation's corrective actions.

Background

The FDIC provides pre-exit clearance guidance for FDIC employees and contractors in the following: (1) Circular 2150.1, *Pre-Exit Clearance Procedures for FDIC Employees;* (2) sections of the *Acquisition Procedures, Guidance and Information* (PGI); and (3) Standard Operating Procedure (SOP) for *Processing Departing and Transferring Employees and Contractors*.

Pre-Exit Clearance Procedures for FDIC Employees

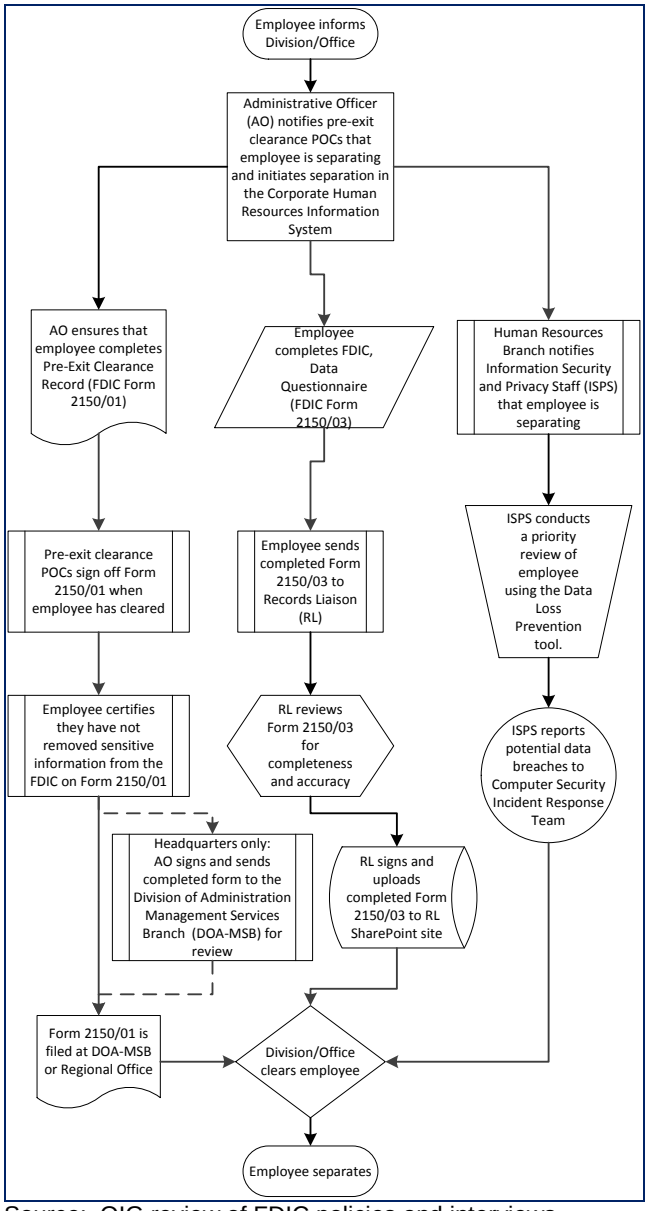
The FDIC policy, *Pre-Exit Clearance Procedures for FDIC Employees* (FDIC Circular 2150.1), establishes procedures for FDIC employees who either are separating from the FDIC or are reassigned to another division or office within the FDIC. The purpose of the procedures is to ensure proper safeguards are in place to protect FDIC-owned property and interests, which includes sensitive information. The circular does not apply to FDIC contractors.[9] Figure 1 illustrates the pre-exit clearance process for employees.

The pre-exit clearance process begins when an employee informs their division or office of their intent to separate from the FDIC. The division or office Administrative Officer (AO) or their

[6] Letter from the Chairman, U. S. Senate Committee on Banking, Housing, and Urban Affairs, to the Acting Inspector General, FDIC, dated June 28, 2016.
[7] Letter from the Acting Inspector General, FDIC, to the Chairman, U. S. Senate Committee on Banking, Housing, and Urban Affairs, dated July 29, 2016.
[8] For this evaluation, the term "personnel" includes FDIC employees and contractors. The evaluation focused on the period starting when the FDIC becomes aware of any personnel that will separate from the Corporation until they separate and established pre-exit clearance procedures are complete. During the course of our evaluation, we decided not to address procedures related to separating outside legal counsel retained by the FDIC because those procedures were distinctly different.
[9] For the purpose of this report, "contractor organization" refers to an entity that the FDIC has contracted with, while "contractor" refers to an individual employee of a contractor organization.

designee is responsible for initiating and controlling the pre-exit clearance process and ensuring that a separating employee is cleared by the appropriate FDIC organizations. These responsibilities include preparing all required notifications, facilitating completion of the process as necessary, and maintaining the documentation required to support the clearance process. The AO sends an email to the relevant points of contact for pre-exit clearance, informing them of the employee's separation and requesting that the points of contact take the necessary steps. The point of contact for each task on the FDIC form 2150/01, *Pre-Exit Clearance Record for Employees* (Employee Pre-Exit Clearance Record in this report) reviews and, if appropriate, verifies satisfactory completion of the task[10] by signing the form or documenting completion by email.

Figure 1: The FDIC's Employee Pre-Exit Clearance Process



Source: OIG review of FDIC policies and interviews.

As part of the pre-exit clearance process, the separating employee's immediate supervisor must ensure that the employee completes the FDIC form 2150/03, *Data Questionnaire for Departing/Transferring Employees/Contractors* (Data Questionnaire in this report).[11] The Data Questionnaire (FDIC Form 2150/03) must be completed at least 1 week, but no more than 30 days, prior to the employee's separation. This form requires the separating employee to identify the location of paper and electronic records in one's possession, access to information technology network shared folders and SharePoint sites, and any email folders that the separating employee shares with other FDIC personnel.

[10] Examples of the most significant pre-exit clearance tasks include the employee (1) turning in their government credit and/or purchase cards, (2) having his/her timekeeper verify leave balances, (3) receiving a post-employment ethics briefing, (4) turning in all FDIC-owned information technology equipment, (5) having access to information systems revoked, and (6) turning in Personal Identity Verification (PIV) cards.

[11] The FDIC updated FDIC Form 2150/03 in January 2017 and then again in April 2017. The form is now called the *Records and Information Management Questionnaire for Departing/Transferring Employees*. The new form added a section for the employee's signature and a requirement to affirm the accuracy of the information on the form.

Upon completing the Data Questionnaire, the employee sends it to their division or office Records Liaison (RL). The RL is the division or office subject-matter expert and point of contact for records and information management activities and helps ensure that divisions and offices comply with records management requirements. According to the SOP, RLs are to review the form for accuracy and completeness and, when necessary, meet with the separating employee, sign the form electronically, and upload it to the RL SharePoint site.

The separating employee signs the Employee Pre-Exit Clearance Record certifying that he/she has not removed or disclosed any confidential information from the FDIC. The AO reviews and, if appropriate, signs the Employee Pre-Exit Clearance Record, sends the form to the Division of Administration (DOA) Management Services Branch (MSB) and provides a copy to the employee.

A DOA-MSB management analyst reviews headquarters employees' pre-exit clearance forms for completeness. The DOA Human Resources Branch (HRB) sends DOA-MSB a report of separating employees for each pay period. The DOA-MSB management analyst verifies receipt of a Pre-Exit Clearance Form for each employee on the separations report. Then, the management analyst adds the name of the separating employee to a control list and files the pre-exit clearance form in a secure file room. Finally, the MSB management analyst also checks the FDIC's global email address list to confirm that the separating employee's access to the network has been disabled. If access has not been disabled, the analyst will send a message to the Chief Information Officer Organization (CIOO) requesting removal of access for the separated employee. The MSB reconciliations are completed for separating headquarters employees only and are completed after the employee separates.

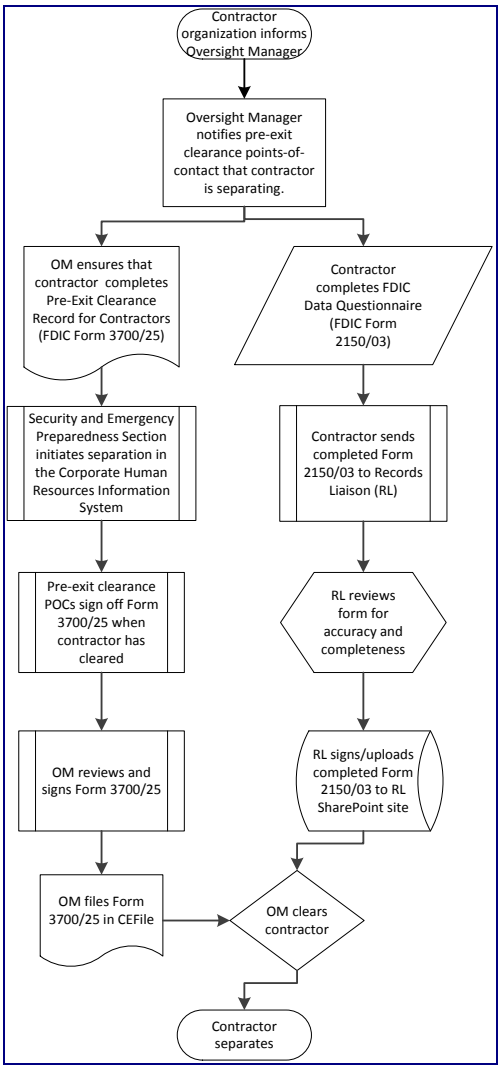
According to DOA-MSB, each regional office manages its own pre-exit clearance process without MSB's oversight, although this distinction is not specified in *Pre-Exit Clearance Procedures for FDIC Employees*. The regional AOs ensure that the Employee Pre-Exit Clearance Record is completed for separating regional office employees. The regional offices indicated that they use corporate guidance and process the Data Questionnaire the same as in headquarters. Five of the six regions had a hyperlink on their DOA regional webpage to the pre-exit clearance process and a list of contacts that assist with pre-exit clearance. During our evaluation, we asked representatives from the sixth region (New York Region) about such a link, and they established a similar hyperlink. The regions process the pre-exit clearances for separating field office employees with assistance from field office personnel. Copies of the forms related to the pre-exit clearance process for employees are generally retained in the region, although for some FDIC divisions, the forms are maintained at headquarters.

Pre-Exit Clearance Procedures for FDIC Contractors

Pre-exit clearance for contractors is governed by the PGI, which provides guidance for internal contract administration as well as the text for standard contract clauses to communicate pre-exit clearance instructions to contractor personnel. For contractors, the contract Oversight Manager (OM) or designee is responsible for initiating and supervising the pre-exit clearance process. Figure 2 illustrates the pre-exit clearance process for contractors.

Contractor organizations whose contractors have access to the FDIC network; receive Personally Identifiable Information; or have been issued an FDIC badge, FDIC property or equipment, parking permits, office keys, access cards, and/or building passes must notify their OM of the contractor's separation no later than the date of separation.[12] Upon notification, the OM must ensure that FDIC Form 3700/25, *Pre-Exit Clearance Record for Contractors* (Contractor Pre-Exit Clearance Record for this report), is completed and filed in DOA's official Contract Electronic File (CEFile) system. The Contractor Pre-Exit Clearance Record requires actions by the OM or designee, CIOO, and the Security Management Section or Field Facility Manager. One of the requirements on the Contractor Pre-Exit Clearance Record is that the OM ensures the separating contractor completes the Data Questionnaire just like separating employees. Upon completion of the Data Questionnaire, the contractor sends the form to the respective division or office RL, who should review it for completeness and accuracy and then upload the form to the RL SharePoint site.

Figure 2: The FDIC's Contractor Pre-Exit Clearance Process



Source: OIG review of FDIC policies and interviews.

Data Loss Prevention Tool (DLP) and Technological Measures to Detect or Prevent the Removal of Sensitive Information

The DLP operates as a guard around the digital perimeter of the FDIC and monitors various electronic ways sensitive information could leave the FDIC. For example, DLP monitors outgoing emails, documents sent to network printers, website uploads, and downloads to external media.

The DLP searches for keywords and network activity that matches a set of business rules intended to protect sensitive information. These business rules are developed by Information Security Managers (ISMs) for each division and office. For example, a division may create a rule that any document attempting to be emailed outside of the FDIC network with the acronym "SIFI," for systemically important financial institution, will be flagged. When DLP identifies activity that meets established criteria, an entry is created in the DLP activity log. An Information Security and Privacy Staff (ISPS) staff member manually reviews all potential incidents in the activity log. If ISPS believes a violation of the rules has occurred, it forwards information about the incident to the Computer Security Incident Response Team (CSIRT) for further investigation. ISPS also provides detailed information about the incident to the division or office ISM for follow-up with the employee.

[12] FDIC standard contract clause 7.5.2-12.

DLP has a detective and preventative mode. The detective mode alerts ISPS staff that potentially sensitive data has already left the FDIC. When the DLP is used in the preventative mode, it prevents the activity associated with the flagged item from being executed. Using the example above, the DLP in preventative mode would have stopped the e-mail containing reference to "SIFI" from being sent outside the FDIC network. The DLP process ends when CSIRT adds the incident to its case management tracker or ISPS reviews the log and determines no violation of the rules occurred.

In response to a number of data breaches and in an effort to improve FDIC network security, in March 2016, the FDIC began limiting most FDIC employees' and contractors' ability to save electronic information to removable media such as computer discs or thumb drives. This action addressed a primary means of carrying out the data breaches and substantially reduced the number of incidents being flagged by the DLP for review.

Further, after June 30, 2017, the FDIC required all of its personnel to use Personal Identity Verification (PIV) cards to access facilities and information systems. Separating personnel surrender their PIV cards as part of the pre-exit clearance process thereby preventing their access to FDIC facilities and information systems after separation.

Evaluation Results

The FDIC's Employee Pre-Exit Clearance Process

The overarching risk to the FDIC is that a data breach, which can include data in electronic and paper format, will occur when employees separate from the FDIC. While the FDIC has established controls over the pre-exit clearance process, we identified certain weaknesses in how those controls were designed, found that the FDIC was not always following its procedures, and identified opportunities to strengthen the pre-exit clearance process for employees.

Pre-Exit Clearance Control Weaknesses Limit Their Effectiveness

Control objectives for the FDIC's pre-exit clearance process include preventing unauthorized access to, and inappropriate removal and inappropriate disclosure of, sensitive data. We evaluated pre-exit clearance policy controls intended to address those control objectives and identified several weaknesses in their design as shown in Table 1.

Table 1: Pre-Exit Clearance Controls Assessment for Employees

Control Objective and Activity	Control Weaknesses
Preventing Unauthorized Access • AO notifies CIOO Access Control to remove employee access to systems and network on employee's separation date. • Supervisor takes employee's PIV card upon exit. • MSB verifies that network access for separating employees has been terminated.	• Access control does not prevent data breach initiated prior to removal of access. • MSB review may not be timely and is only performed for separating headquarters employees.
Preventing Inappropriate Removal or Disclosure • Pre-Exit Clearance Record requires employee to sign an assertion that they have not removed and will not disclose sensitive information. • Data Questionnaire requires employee to identify location of paper/electronic records. • FDIC removed the ability to download data to CDs or external drives. • Priority review of DLP information for separating employees.	• Employees may not be truthful or may be careless in their assertions. • Some FDIC personnel have a business need to download data. • There is currently no policy or procedure for DLP use related to the pre-exit clearance process. • The DLP priority review may not occur until after an employee separates.

Source: OIG-generated based on review of FDIC policies and procedures and interviews with program officials.

As illustrated above, some pre-exit clearance controls are not sufficiently designed to prevent unauthorized access, removal, or disclosure of sensitive data in a timely manner. For example, DOA-MSB does not review Employee Pre-Exit Clearance Records (FDIC Form 2150/01) or determine whether the employee has access to the FDIC network until after the employee has separated. Similarly, the use of the DLP tool to conduct a priority review of separating employee network activity, while an effective control when performed timely, often does not occur until after an employee has separated. As discussed in the next section, we also found that RLs were not always reviewing Data Questionnaires before employees separated. The effectiveness of such controls is limited if they occur after an employee has separated.

In addition, certain controls were not being used for all separating personnel. While DOA-MSB performs a secondary review of pre-exit clearance records and verifies removal of network access for headquarters employees, there is no corresponding secondary review for separating regional office employees. As discussed in the next section, one regional office could not support that RLs consistently or timely reviewed Data Questionnaires.

Further, several controls largely rely upon employee assertions about their handling of sensitive data. Employees certify that they have not disclosed sensitive information by signing a statement in the Employee Pre-Exit Clearance Record (FDIC Form 2150/01). This form cautions that providing knowing and willful false statements can be punished by fine, imprisonment, or both. The Data Questionnaire (FDIC Form 2150/03) also relies on the employees' assertions about their disposition of data and records. However, the employees do not have to sign Form 2150/03 or make certifications about completeness, truthfulness, or accuracy. Also the form contains no warnings against false statements.

In response to the data breaches discussed earlier in this report, the Legal Division researched potential actions that the FDIC could undertake to minimize data breaches and discourage inappropriate behavior by current and former employees and contractors. The Legal Division

identified several legal theories for seeking civil and administrative remedies against employees and contractors who violate FDIC cybersecurity policies and procedures. The Legal Division indicated that none of these theories was found to be compelling or straightforward in pursuing past cases. However, the Legal Division indicated that the FDIC had: (1) taken disciplinary steps, including proposed removal, against current employees for failure to safeguard sensitive government information (and certain contractor organizations had removed contractors from FDIC contracts) and (2) utilized the certification signed by separating personnel in obtaining cooperation from former employees or contractors.

As designed, the program controls do not provide reasonable assurance that the pre-exit clearance process will timely or effectively identify unauthorized access to, or inappropriate removal and disclosure of, sensitive information by separating employees. Further, the FDIC's reliance on employee assertions and the challenges of pursuing an employee or contractor once they have left the Corporation underscores the importance of strong, timely controls and procedures that occur while personnel are still employed.

FDIC Records Liaisons Did Not Always Complete Pre-Exit Clearance Procedures Timely

Our testing showed that division and office records liaisons did not follow or consistently execute timely existing pre-exit clearance procedures. To determine the extent to which the FDIC has established and is following controls that mitigate the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating employees, we tested the timeliness and completeness of pre-exit clearance controls for a random sample of employees that separated from the FDIC between October 1, 2015 and September 30, 2016. Our testing focused on pre-exit clearance controls that were pertinent to the protection of sensitive information. According to FDIC policy, the assertions and reviews required by these controls should be completed prior to the employee's separation.

For separating employees, we were able to locate most of the forms that we reviewed for timeliness and completeness. We located 100 percent of the 49 Employee Pre-Exit Clearance Records that we sampled. In 94 percent of the cases, the employee signed the record before they separated, thereby asserting that they had not removed or disclosed any confidential information from the FDIC.

We located 47 of 49 employee Data Questionnaires that we sampled. However, we found that RLs were not reviewing Data Questionnaires timely as required by the standard operating procedures. The RL is the division or office subject-matter expert and point of contact for records and information management activities and helps ensure that divisions and offices comply with records management requirements. In the sample we tested, RLs did not review the Data Questionnaire before employees separated in 20 of 49 cases or 41 percent of the time. Of the 20 data questionnaires not signed before employees separated, 16 had worked for the

Division of Risk Management Supervision (RMS).[13] Results of employee testing appear in Table 2.

Table 2: Employee Testing Results

Attribute Tested	Results
Clearance Records Located	49 of 49 (100%)
Clearance Records Signed by Employee prior to separation	46 of 49 (94%)
Data Questionnaires Located	47 of 49 (96%)
Data Questionnaires Signed by RL prior to separation	29 of 49 (59%)
Data Questionnaires found on RL SharePoint site	47 of 49 (96%)

Source: OIG testing of a random sample of 49 Employee Pre-Exit Clearance Records (FDIC Form 2150/01) and Data Questionnaires (FDIC Form 2150/03) from a population of 763 employees that separated from the FDIC between October 1, 2015 and September 30, 2016.

Kansas City Regional Office Testing Results. As part of our evaluation, we sent questionnaires about the pre-exit clearance process to the FDIC regional offices. The DOA Corporate Services Branch (CSB) Chief for the Kansas City Regional Office initially responded that the office had not completed Data Questionnaires for separating personnel since January 1, 2016. That date coincides with the departure of the Kansas City Regional Office RL from the FDIC.[14]

After we reported this finding to headquarters DOA management, the Kansas City Regional Office CSB Chief clarified that since February 2016, an administrative assistant in the Kansas City Regional Office had been collecting Data Questionnaires from separating staff in RMS and the Division of Depositor and Consumer Protection, and subsequently uploading the Data Questionnaires to the RL SharePoint site. Separating Kansas City personnel from other divisions and offices were referred to their division or office RL for Data Questionnaire processing.

After receiving the Kansas City Regional Office's amended response, we reviewed data questionnaires for all Kansas City employees that separated between October 1, 2015 and September 30, 2016. For the 43 employees that separated during this time, we located 33 Data Questionnaires, while 10 such questionnaires (23 percent) could not be located. In addition, RLs signed only 16 Data Questionnaires (37 percent) prior to the employee's separation. By comparison, for our overall employee sample, RLs signed Data Questionnaires prior to employee separation 59 percent of the time.

[13] Separating RMS employees represented 39 percent of our sampled items. RMS RLs did not sign 16 of 19 Data Questionnaires that we sampled before employees separated.

[14] The other FDIC regional offices reported that they were using the Data Questionnaire, so we did not follow up with those offices other than for the testing results discussed in Table 2.

The FDIC Should Strengthen the Employee Pre-Exit Clearance Process

Based on our evaluation of FDIC's pre-exit clearance program, testing, and consideration of pre-exit clearance practices from another agency, discussed in Appendix 4 of this report, we identified several opportunities for strengthening the FDIC's pre-exit clearance process for employees.

Designating a Pre-Exit Clearance Process Owner and Increasing Program Oversight. During our initial meetings with DOA, we determined that no single FDIC official is responsible for the overall performance of the Corporation's pre-exit clearance process. Rather, each division and office within the FDIC has certain responsibilities for pre-exit clearance of its employees. DOA reviews pre-exit clearance records for separating headquarters employees only, while each of the regional offices oversees its own pre-exit clearance process.

Establishing a single accountable official or process owner[15] would help the FDIC ensure appropriate management attention to, and accountability for, the pre-exit clearance program. A process owner also will help the FDIC achieve the program goal to ensure proper safeguards are taken to protect FDIC property and interests when personnel separate. A single accountable official also would overcome the challenge of holding multiple divisions and offices accountable for a program in which they only are responsible for a part.

DOA could also increase program oversight. The *Pre-Exit Clearance Procedures for FDIC Employees* provides that DOA-MSB and the Division of Finance (DOF) Corporate Management Control Branch (CMCB) are required to "periodically conduct a review of the Corporate Pre-Exit Clearance Process." DOA-MSB officials told us they had planned to review both employee and contractor pre-exit clearance processes in 2016 but suspended the reviews because of our evaluation. DOA-MSB reviewed portions of the pre-exit clearance program in 2012 and 2014.[16] DOF-CMCB has not reviewed the pre-exit clearance process.

Program Coordinators Should Actively Manage the Pre-Exit Clearance Process and Designate Back-up Resources. The separating individual is responsible for completing pre-exit clearance tasks, and the process largely relies on separating employee assertions about their handling or possession of sensitive information. After the employee completes pre-exit clearance tasks, the division or office AO reviews the Pre-Exit Clearance Record. The FDIC could have greater control over the pre-exit clearance process by having division and office representatives, such as the AO and RL, assume a greater role in actively managing and completing the pre-exit clearance process rather than the separating individual.

FDIC would also benefit from assigning back-up personnel for pre-exit clearance responsibilities to help ensure that tasks are completed. During our testing, we discovered some confusion in one regional office as to who was responsible for reviewing Data Questionnaires for separating

---

[15] The Government Accountability Office (GAO) defines a process owner as "an individual held accountable and responsible for the workings and improvement of one of the organization's defined processes and its related subprocesses." (See GAO's *Business Process Reengineering Assessment Guide*, May 1997, p. 67).

[16] MSB's 2014 review found that oversight managers may not be communicating with DOA's Security and Emergency Preparedness Section when contractor personnel depart.

employees after the assigned RL departed the region. Although this was not a widespread problem, designating back-up personnel for pre-exit clearance responsibilities is a good practice that the FDIC should follow.

Assessing Risks When Individuals Separate. The FDIC currently does not require divisions or offices to assess risks to sensitive information at the time they become aware that individuals are separating from the FDIC. Federal guidelines establish that agency leaders and managers are responsible for implementing management practices that effectively identify, assess, respond, and report on risks.[17]

The FDIC currently has resources and initiatives in place that it could leverage to manage risks associated with separating personnel. We discussed with DOA officials, information that the FDIC could potentially use in developing a risk-assessment process for separating personnel. In designing these risk assessments, DOA should consult with the Legal Division and CIOO regarding the Privacy Act of 1974,[18] the E-Government Act of 2002,[19] and other legal requirements. In particular, the FDIC should ensure that use of these datasets for this purpose complies with the applicable System of Records Notices and other privacy and IT security requirements.

Employing divisions and offices are in the best position to assess those risks when they learn that an employee is separating. A requirement to assess risks specific to separating individuals as the initial step in a pre-exit clearance process would help the FDIC make an informed decision about what controls to exercise or procedures to perform for individual separating personnel.[20]

ISMs could be involved in this assessment along with the separating employee's supervisor, manager, or other key staff in the employing division. Other offices that may be involved include DOA's Labor and Employee Relations Section (LERS) and the FDIC's Office of Minority and Women Inclusion.

The FDIC's Insider Threat and Counterintelligence Program (Program) may also support a personnel-specific risk assessment by helping to identify risks associated with pre-exit clearance and coordinating appropriate responses. The FDIC formally established the Program on September 20, 2016. Currently, the Program, among other things, provides a framework for identifying and responding to insider threats but does not specifically address the pre-exit clearance process. However, the official responsible for developing the Program informed us that the FDIC will deploy user behavior analytics tools to assess personnel-specific risks in the

---

[17] OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. The FDIC has determined that this Circular is not legally binding on the FDIC; however, the FDIC may consider the Circular's enterprise risk management (ERM) provisions as containing "good government" principles that may be useful to the FDIC's own ERM program.

[18] 5 U.S.C. §552a.

[19] Public Law 107-347.

[20] We communicated this issue to the Director, DOA, among other preliminary concerns about the FDIC's pre-exit clearance policy, procedures, and accountability in a memorandum, *Preliminary Concerns Related to the Design of the Corporation's Pre-Exit Clearance Process Controls*, dated October 14, 2016, located at Appendix 3 of this report.

near future. DOA envisions integrating such tools into other FDIC systems and compiling employee activity information (such as PIV card reader information at building entry points and network activity) to inform the risk assessment process. DOA must coordinate with the Legal Division to ensure the program complies with relevant privacy laws and regulations and other requirements.

Defining Policy for DLP Use in the Pre-Exit Clearance Process. DLP provides an electronic means of monitoring network activity that complements manual procedures for pre-exit clearance. The FDIC's current pre-exit clearance guidance for FDIC employees or contractors does not include using DLP. However, over the past year, ISPS has begun to use DLP regularly to conduct a priority review of the network activity of separating employees. After the data breaches by separating employees that occurred in late 2015 and early 2016, DOA-HRB added ISPS to an email distribution for personnel actions that included employee separations. LERS also began to inform ISPS when employees of interest were scheduled to separate from the FDIC.[21]

When ISPS identifies separating employees from either the DOA-HRB personnel email or LERS, ISPS reviews the employee's network activity in DLP. If ISPS discovers potential incidents or data breaches, they report them to the FDIC CSIRT. LERS is working with ISPS and the Legal Division to establish a process that formalizes this arrangement. Further, the OIG recommended the expanded use and refinement of DLP in a July 2016 report.[22] Specifically, we recommended that the FDIC review the implementation of the DLP tool, including the key words and filters used to monitor data, procedures for assessing output (i.e., events that are flagged for review), and resources committed to reviewing the events. This recommendation remained unimplemented at the time that we issued this report.

Improving Pre-Exit Clearance Forms. The Data Questionnaire (FDIC Form 2150/03) requires separating personnel to list data locations where potentially sensitive data may have been stored or sent outside the FDIC, such as portable electronic storage, personal computer, personal email, or filing cabinets for paper records. This form also instructs separating personnel to submit all FDIC business records, files, and information to their supervisor or oversight manager prior to separation.

Although the FDIC revised the Data Questionnaire in March 2016, further improvements are needed. For example, the Data Questionnaire (FDIC Form 2150/03) and related instructions should:

- Include the completion date and employee or contractor certification of the accuracy of the information reported on the form. This form should also include the warning that

[21] Employees of interest include: (1) employees subject to removal actions; (2) employees retiring in less than 2 weeks because they would not appear on the DOA-HRB personnel actions email; and (3) employees involved in suspicious information security practices such as having a family member send an email that contains sensitive information from the employee's home computer to their work email address.
[22] FDIC OIG Report entitled, *The FDIC's Process for Identifying and Reporting Major Information Security Incidents*, July 7, 2016.

providing knowing and willful false statements can be punished by fine, imprisonment, or both under 18 U.S.C. 1001.

- Contain instructions for the division or office ISM to review the information reported on the form.

- Contain steps the RL or ISM should take if the employee or contractor indicates sensitive information has been stored on a portable device or a personal computer or sent to personal email.

- Contain instructions on what to do in situations where the employee or contractor organization does not give a 7-day notice prior to employee/contractor separation.

These improvements could lead to an improved review when separating personnel indicate they have stored information in places at a higher risk of data loss such as portable electronic storage, a personal computer, or personal email.

As discussed earlier, the Legal Division researched potential actions that the FDIC could undertake to minimize future breaches and discourage inappropriate behavior by current and former employees and contractors. The Legal Division contemplated a recommendation aimed at strengthening acknowledgments and warnings in pre-exit clearance forms and non-disclosure agreements regarding breaches of sensitive information and the associated consequences. We also learned that the Legal Division researched potential actions that the FDIC could undertake to minimize future breaches and discourage inappropriate behavior by current and former employees and contractors. The resulting guidance and recommendations had not been completed at the time we performed our work. However, we understand that staff of the various divisions involved (including Legal and DOA) have been working on revisions to the pre-exit clearance forms, and will be considering other process improvements and enhancements aimed at strengthening the FDIC's security posture in relation to separating personnel.

Continuing Automation Efforts. The FDIC would benefit from developing a centralized electronic application to manage pre-exit clearance. Such an application could track exit information for personnel and send automated emails to remind exiting personnel and agency staff of outstanding pre-exit clearance tasks. The application could also include a dashboard[23] to enable the Exit Coordinator to track the progress for each separating individual, with the most important tasks highlighted on the dashboard.

As described earlier in this report, the FDIC's current pre-exit clearance process is manually tracked through the Employee Pre-Exit Clearance Record and by the separating individual's AO. The FDIC plans to develop an automated system to track the progress of pre-exit clearance activities, provide a dashboard view of ongoing exits, and escalate instances of process non-compliance or delays to FDIC leadership, if appropriate, sometime in 2018.

[23] A dashboard is a screen or view that consolidates critical performance metrics all in one place, making it easy for users to stay constantly updated on the information most important to their program or area of responsibility.

The FDIC's Contractor Pre-Exit Clearance Process

Separating contractors may present greater risks than separating FDIC employees because the Corporation may not have as much knowledge about a contractor's personnel history as it does for FDIC employees. In addition, contractors may depart suddenly. As a result, the FDIC would not have sufficient time to conduct its pre-exit clearance process. Again, we identified certain weaknesses in pre-exit clearance controls, found that the FDIC was not always following its procedures, and identified opportunities to strengthen the pre-exit clearance process for contractors.

Contractor Pre-Exit Clearance Controls Also Have Weaknesses

As we did for employees, we analyzed pre-exit clearance process control objectives, control activities, and control weaknesses for separating contractors as shown in Table 3.

Table 3: Pre-Exit Clearance Controls Assessment for Contractors

Control Objective and Activity	Control Weaknesses
Preventing Unauthorized Access • The OM submits a request to terminate network access for separating contractors upon notification they are leaving. • The OM takes the contractor's PIV card upon exit.	• Does not prevent data breach initiated prior to personnel separation. • May not be timely (notification of contractor's separation not required until the day of separation).
Preventing Inappropriate Removal or Disclosure • Confidentiality Agreement for Contractors: contractor will not disclose, release, disseminate or transfer any sensitive information…except as required in contract. • Data Questionnaire requires contractor to identify location of paper/electronic records. • FDIC removed the ability to download data to CDs or external drives. • DLP used to conduct a priority review of activity of selected separating contractors.	• Confidentiality agreements are signed at the beginning of the contract and not reviewed during the pre-exit clearance process. • The Questionnaire relies on contractor assertions, may not be timely, and is not consistently used. • Some FDIC personnel have a business need to download data. • There is no policy or procedure for DLP use related to the pre-exit clearance process. • DLP is not used to conduct priority review for many contractors. • DLP priority review may not occur until after separation.

Source: OIG-generated based on review of FDIC policies and procedures and interviews with program officials.

We identified several differences in the FDIC's pre-exit clearance process for contractors:

- Contractor pre-exit clearance is decentralized and solely managed by individual OMs. There are no oversight or monitoring mechanisms established for contractor pre-exit clearance procedures at the program level. This increases the risk that separating contractors may not be subject to pre-exit clearance procedures and that OMs could implement procedures inconsistently.

- No one is assigned to review Contractor Pre-Exit Clearance Records (FDIC Form 3700/25) or check network access for separating contractors as DOA-MSB does for separating

headquarters employees. This increases the risk that the OM may not follow pre-exit clearance procedures and this lapse would not be detected. The decentralized nature of the OM function makes this second level review even more important.

- Contractors are not required to affirm that they have not removed or disclosed sensitive information at separation. Contractors affirm in Confidentiality Agreements (FDIC Form 3700/46A for individual contractor personnel and FDIC Form 3700/46 for contractor organizations) that they will protect and not disclose sensitive information. Contractors also agree to return or destroy all FDIC information to which they have access upon the conclusion of their duties, association, or support to the FDIC. However, contractors sign Confidentiality Agreements at the beginning of a contract and the Agreement is not revisited during the pre-exit clearance process. Some contractors work at the FDIC for years and may not recall their non-disclosure responsibilities. Accordingly, the Confidentiality Agreement, in our view, is not an effective control for the pre-exit clearance process.

- ISPS does not conduct a DLP priority review for many contractors, which amounted to at least 43 percent of FDIC contractors that separated between October 1, 2015 and September 30, 2016 (252 out of 587 contractors). Further, ISPS is not always notified of separating contractors and, thus, would not conduct a priority DLP review in such cases. Moreover, ISPS usually conducts the DLP review after the contractor has separated. The DLP review is important because it is a way to independently detect unusual activity (such as through e-mail or by printer) involving sensitive information.

These control differences between the employee and contractor pre-exit clearance processes increase risks related to sensitive information when contractors separate.

FDIC Records Management and Contracting Staff Did Not Always Follow Contractor Pre-Exit Clearance Procedures

As we found for FDIC employees, we also determined that those having key roles in the process are not consistently following pre-exit clearance guidance for contractors. Further, the lack of compliance with guidance occurred to a greater degree for contractors than we found for employees.

We tested the timeliness and completeness of pre-exit clearance controls for a random sample of contractors that separated from the FDIC between October 1, 2015 and September 30, 2016, and focused on pre-exit clearance controls that were pertinent to the protection of sensitive information. According to FDIC policy, the assertions and reviews required by these controls should be completed prior to contractor separation. In addition, because the Contractor Pre-Exit Clearance Record (FDIC Form 3700/25) does not require contractors to affirm that they have not removed or disclosed any confidential information from the FDIC, we also tested for the existence of signed confidentiality agreements, which are signed at the beginning of the contract.

According to DOA's PGI, Section 5.203(e), "Termination of Access," OMs are required to file Pre-Exit Clearance Record forms for contractors in the CEFile system. We had difficulty locating most of the forms for separating contractors that we sampled. When we could not locate

the forms in CEFile or the RL SharePoint site, we requested the forms from the contract OM. In our sample of 48 contractors, we were only able to locate 5 Pre-Exit Clearance Records (10 percent) and 12 Confidentiality Agreements (25 percent) in the CEFile system. In other words, the FDIC did not properly maintain Pre-Exit Clearance Records in 90 percent of the cases or Confidentiality Agreements for 75 percent of the contractors. These documents are critical to the security process for departing contractors, because the Pre-Exit Clearance Record documents that the contractor has completed the clearance process and the Confidentiality Agreement affirms the contractor's responsibility for protecting FDIC information.

The DOA's Records and Information Management Unit (RIMU) SOP, *Processing Departing and Transferring Employees and Contractors*, requires the RL to review Data Questionnaires for contractors. However, we could not locate any Data Questionnaires for contractors on the RL SharePoint site. Subsequently, we determined that RIMU did not require RLs to review Data Questionnaires for separating contractors because RIMU and the RLs are not notified when contractors separate. However, RIMU had not communicated to the RLs that they did not have to comply with the RIMU SOP or review Data Questionnaires.

We found that RLs did not review the Data Questionnaire before contractors separated in 94 percent of the cases we reviewed. According to instructions on the Data Questionnaire and the RIMU SOP, the Data Questionnaire should be completed at least 1 week but no more than 30 days prior to an employee's or contractor's separation. As shown below in Table 4, we also could not locate a substantial percentage of clearance records (46 percent), questionnaires (62 percent), and confidentiality agreements (33 percent).

Table 4: Contractor Testing Results

Attribute Tested	Results
Clearance Records Located	26 of 48 (54%)
Clearance Records Signed by OM prior to separation	14 of 48 (29%)
Clearance Records found in the CEFile system	5 of 48 (10%)
Data Questionnaires Located	18 of 48 (38%)
Data Questionnaires Signed by RL prior to separation	3 of 48 (6%)
Data Questionnaires found on RL SharePoint site	0 of 48 (0%)
Confidentiality Agreement Located	32 of 48 (67%)
Confidentiality Agreement found in the CEFile system	12 of 48 (25%)

Source: OIG testing of a random sample of 48 Contractor Pre-Exit Clearance Records (FDIC Form 3700/25), Data Questionnaires (FDIC Form 2150/03), and Confidentiality Agreements (FDIC Form 3700/46 and FDIC Form 3700/46A) from a population of 587 contractors that separated from the FDIC between October 1, 2015 and September 30, 2016.

The FDIC Should Strengthen the Contractor Pre-Exit Clearance Process

Based on our evaluation and testing, we identified several opportunities for strengthening the contractor pre-exit clearance process.

Ensuring Consistent Controls between Employee and Contactor Pre-Exit Clearance Processes and Improving Procedures. The FDIC could strengthen the contractor pre-exit clearance process by addressing the process differences we discussed earlier related to the absence of program level oversight, MSB review of clearance records, contractor affirmation on

the Data Questionnaire, and DLP use. The FDIC should also consider centralizing management of the contractor pre-exit clearance process. The process is currently decentralized among the various contract OMs. Centralizing oversight would increase consistency and assign program accountability for ensuring that contractor pre-exit clearance procedures are completed effectively and timely.

The FDIC should also establish more explicit guidance for separating contractors. FDIC Circular 2150.1 provides guidance for separating FDIC employees only. Pre-exit clearance guidance for separating contractors is covered in various provisions and contract clauses throughout the FDIC's PGI. A single guidance document, ideally covering separating employees and contractors, would eliminate inconsistent direction that currently exists in the pre-exit clearance process and would consolidate program expectations for processing contractor separations.

Reiterating Pre-Exit Clearance Responsibilities and Expectations. During our testing, some OMs indicated that they were not required to complete Data Questionnaires for separating contractors. However, the DOA Acquisition Services Branch (ASB) said that this view is incorrect. Also, RLs were not reviewing Data Questionnaires as required by policy. Communication of responsibilities and expectations would help ensure these functions are performed and would improve consistency.

Requiring Contractors to Provide Timely Notice of Separation. The timing of contractor notification of separation is not consistent with the Data Questionnaire requirements. Per FDIC contract clause 7.5.2-12, the contractor organization is required to notify the OM of a contractor's departure no later than the day of separation, whereas the Data Questionnaire should be completed within 1 week and 30 days prior to separation. Accordingly, should a contractor organization give less than a one-week notice, the contractor will not be able to timely complete the Data Questionnaire, and the OM and records liaison may not have sufficient time to perform pre-exit clearance procedures before the contractor leaves.

According to DOA-ASB, there will be times when a contractor will not be able to comply with that requirement. For example, if a contractor organization does not provide the FDIC sufficient notice, the contractor will not be able to meet the FDIC's 7-day advance notification requirement. Also, if a contractor is removed from the contract because of conduct or performance issues, the FDIC would prefer the individual be removed immediately rather than waiting 7 days to separate. We believe the requirement could be written to allow for such infrequent exceptions.

Recommendations

Based on our evaluation of existing FDIC controls and results of testing, we recommend the Director, DOA:

(1) Designate a pre-exit clearance process owner who will be accountable for the FDIC's pre-exit clearance program.

(2) Incorporate a risk assessment of individual separating employees into the FDIC's pre-exit clearance process.

(3) Work with the FDIC's Chief Information Officer to establish appropriate policy for using DLP to support the FDIC's pre-exit clearance process.

(4) Revise the Data Questionnaire (FDIC Form 2150/03) to improve identification, tracking, and protection of sensitive information for separating personnel.

(5) Work with the General Counsel to strengthen acknowledgments and warnings in pre-exit clearance forms and non-disclosure agreements regarding breaches of sensitive information and the associated consequences.

(6) Reinforce corporate-wide understanding of the significance of, and requirements for, pre-exit clearance policies and procedures among stakeholders in the pre-exit clearance process.

(7) Work with the Director, DOF, to develop a schedule for future CMC program reviews of the pre-exit clearance program.

(8) Establish a comprehensive pre-exit clearance policy for contractors.

(9) Ensure that assigned personnel are reviewing contractor Pre-Exit Clearance Records and Data Questionnaires timely and documenting their work appropriately.

(10) Work with the FDIC's Chief Information Officer to develop an expanded and better defined use of the DLP tool for separating contractors.

(11) Require contractor organizations to provide a reasonable notice of contractor separation in most circumstances, unless there are extenuating circumstances, as defined in the contracts.

Corporation Comments and OIG Evaluation

DOA provided a written response dated September 15, 2017, to a draft of this report. The response is presented in its entirety in Appendix 7. DOA concurred with the report's 11 recommendations, proposed actions in response to the recommendations, and targeted completion dates through September 30, 2018. DOA reported that it had completed action on recommendations 1, 4, 6, and 7. The report recommendations will remain open until we confirm that the planned actions have been completed and are responsive. A summary of the Corporation's corrective actions is presented in Appendix 8.

Objective, Scope, and Methodology

Objective

Our evaluation objective was to determine the extent to which the FDIC has established controls to mitigate the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating personnel.

We performed our work from October 2016 to February 2017 at the FDIC's offices in Arlington, Virginia, in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Scope and Methodology

The scope of this evaluation included a review of the FDIC's pre-exit clearance process from the time the FDIC becomes aware of personnel separating until the process concludes. We evaluated the pre-exit clearance process for FDIC employees and contractors at FDIC headquarters and regional offices. Our testing was limited to personnel separating from October 1, 2015 through September 30, 2016.

To address our evaluation objective, we first gained an understanding of the FDIC's practices for mitigating risk in the pre-exit clearance process. We analyzed FDIC policies and procedures and other guidance on pre-exit clearance for employees and contractors, protecting sensitive information, insider threat and counterintelligence, ERM, and internal controls. We conducted interviews with FDIC personnel including those in:

- The Division of Administration (DOA) Acquisition Services Branch (ASB), Corporate Services Branch (CSB), Human Resources Branch (HRB) and its Labor and Employee Relations Section (LERS), and Management Services Branch (MSB) to verify how the Corporation's pre-exit clearance process is executed in practice;

- The Chief Information Officer Organization (CIOO) Information Security and Privacy Staff (ISPS) on the use of the Data Loss Protection (DLP) tool in the pre-exit clearance process; and

- The Office Corporate Risk Management to understand the consideration of risks from separating personnel in its ERM efforts.

To understand pre-exit clearance practices in the regional offices, we developed, distributed to regional CSB section chiefs, and analyzed the results of questionnaires on regional office pre-exit clearance procedures.

To assess the FDICs practices, we solicited other federal agencies for pre-exit clearance preferred practices. We compared the FDIC's practices to preferred government practices. To evaluate the FDIC's controls, we tested the timeliness and completeness of a sample of Employee and Contractor Pre-Exit Clearance Records (FDIC Form 2150/01 and FDIC Form

3700/25, respectively) and Data Questionnaires (FDIC Form 2150/03). We also assessed the adequacy of those forms. For contractors, we also tested the existence of a Confidentiality Agreement (FDIC Form 3700/46 and FDIC Form 3700/46A) by which recipients agree to protect sensitive information.

Sampling Methodology

We selected a sample of separated employees and contractors to determine the timeliness and completeness of key controls in the pre-exit clearance process. A total of 763 employees and 587 contactors separated from the FDIC during our scope period of October 1, 2015 through September 30, 2016. We used random sampling to obtain a sample population of 49 employees[24] and 48 contractors. Our sampling methodology employed a 90 percent confidence interval, 5 percent desired precision level, and 5 percent expected incidence (error) rate. However, because the error rate for certain attributes that we tested for both the employee and contractor samples was higher than the expected error rate, we cannot project the results of testing to the population with sufficient confidence and precision.

To evaluate the timeliness and completeness of key controls, we tested the following attributes for each sample item:

- Date of separation;
- Date Employee or Contractor Pre-Exit Clearance Record (FDIC Form 2150/01 or FDIC Form 3700/25, respectively) was completed and signed;
- Date Data Questionnaire (FDIC Form 2150/03) was completed and signed;
- Whether the employee or contractor signed the forms and whether the forms were signed by someone else, or not at all;
- Whether contractor forms were posted to the Contract Electronic File (CEFile) system; and
- Whether data questionnaires were uploaded to the RL SharePoint site.[25]

[24] The original sample included one separated Office of Inspector General (OIG) employee. To prevent any threat to the independence of this evaluation, we eliminated the OIG employee sample item and judgmentally selected another sample item outside of the OIG to replace the OIG sample item.

[25] If we did not find documents in the CEFile system or the RL SharePoint site, we asked the contract Oversight Manager or the RL to locate the missing documents.

Letter from the Chairman, Senate Committee on Banking, Housing, and Urban Affairs

RICHARD C. SHELBY, ALABAMA, CHAIRMAN
MICHAEL CRAPO, IDAHO
BOB CORKER, TENNESSEE
DAVID VITTER, LOUISIANA
PATRICK J. TOOMEY, PENNSYLVANIA
MARK KIRK, ILLINOIS
DEAN HELLER, NEVADA
TIM SCOTT, SOUTH CAROLINA
BEN SASSE, NEBRASKA
TOM COTTON, ARKANSAS
MIKE ROUNDS, SOUTH DAKOTA
JERRY MORAN, KANSAS
SHERROD BROWN, OHIO
JACK REED, RHODE ISLAND
CHARLES E. SCHUMER, NEW YORK
ROBERT MENENDEZ, NEW JERSEY
JON TESTER, MONTANA
MARK WARNER, VIRGINIA
JEFF MERKLEY, OREGON
ELIZABETH WARREN, MASSACHUSETTS
HEIDI HEITKAMP, NORTH DAKOTA
JOE DONNELLY, INDIANA
WILLIAM D. DUHNKE III, STAFF DIRECTOR AND COUNSEL
MARK E. POWDEN, DEMOCRATIC STAFF DIRECTOR

United States Senate
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
WASHINGTON, DC 20510–6075

June 28, 2016

Mr. Fred W. Gibson
Acting Inspector General
Federal Deposit Insurance Corporation
Office of Inspector General
3501 Fairfax Avenue
Arlington, VA 22226

Dear Mr. Gibson,

A series of data breaches at the Federal Deposit Insurance Corporation (FDIC) has compromised sensitive financial information in the FDIC's possession, including suspicious activity reports, the resolution plans for some of the largest U.S. banks, and bank customers' social security numbers.

According to a memorandum dated February 19, 2016, your office reviewed the response to one such incident in Gainesville, Florida, and concluded that senior FDIC officials failed to properly classify that incident as "major," did not adequately document their decision-making process, applied factors not authorized by Office of Management and Budget guidance, and failed to timely report the breach to Congress.

The FDIC has since retroactively reported at least six more major incidents, in addition to reports of a criminal investigation of a former employee who removed information related to banks' resolution plans in 2015, and an ongoing investigation into a leak of the most recent living wills results. Furthermore, a former employee is being prosecuted in federal court in Illinois over confidential information taken from the agency in 2012, and recent media reports have revealed to the public for the first time a highly sophisticated attack beginning in 2010 that infected the computers of many top FDIC executives, including former Chairman Sheila Bair.

The Federal Information Security Modernization Act of 2014 requires agencies to promptly report major data breaches to Congress. I understand that your office is currently conducting an audit of the FDIC's controls for major data security incidents. While audits are critical to identifying deficiencies and improving agency performance, the possibility that FDIC officials repeatedly failed to fulfill FDIC's statutory obligations merits additional scrutiny. I request that the scope and depth of your on-going review of each major data security incident be no less thorough than the work undertaken by your office in connection with the Gainesville incident. I further request that your on-going review examine any broader institutional problems at the FDIC related to data security, breach reporting, and policies governing departing

Letter from the Chairman, Senate Committee on Banking, Housing, and Urban Affairs

employees' access to sensitive financial information. Moreover, I request that you consider whether any representations made by FDIC officials are inconsistent with the findings of your review, and whether such representations were fully forthright and complete.

Thank you for attention to this matter.

Sincerely,

Richard Shelby
Chairman

October 2016 OIG Memorandum Communicating Preliminary Concerns with the Pre-Exit Clearance Process

FDIC

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226

Office of Audits and Evaluations
Office of Inspector General

DATE: October 14, 2016

MEMORANDUM TO: Arleas Upton Kea, Director
Division of Administration

/Signed/

FROM: E. Marshall Gentry
Assistant Inspector General for Evaluations

SUBJECT: Preliminary Concerns Related to the Design of the Corporation's Pre-Exit Clearance Process Controls

As we indicated in our memorandum to you dated October 7, 2016, announcing our evaluation of *The FDIC's Controls over Separating Personnel's Access to Sensitive Information* (Assignment No. 2016-038), we have identified several concerns related to the design of the Corporation's pre-exit clearance process controls that we believe warrant immediate attention. Our evaluation will involve additional work to determine the extent to which the FDIC has established controls to mitigate the risk of unauthorized access to and inappropriate removal and disclosure of sensitive information by separating personnel. However, we wanted to communicate the following pre-exit clearance process control concerns that could present risk to the Corporation.

Risk Assessment of Individual Separating. Currently, the FDIC does not assess the specific risks an individual presents at the point the FDIC becomes aware of that individual's impending separation. In our view, this is a fundamental weakness in the Corporation's pre-exit clearance process. We recognize that FDIC's divisions and offices must balance the need for separating personnel to have access to sensitive information to perform their duties with the obligation to protect such information from unauthorized removal and disclosure. We further recognize that the majority of personnel separate under favorable circumstances and may not pose undue risk to the Corporation's sensitive information when they separate. Without assessing specific risk at the initial stage of its pre-exit clearance process, the Corporation cannot consistently and appropriately mitigate threats posed by individual separating personnel.

Pre-Exit Clearance Policy. Another issue we identified in planning our evaluation is that the FDIC does not have a single policy for pre-exit clearance that covers all personnel who are separating from the FDIC. FDIC Circular 2150.1, *Pre-Exit Clearance Procedures for FDIC Employees*, provides guidance for FDIC employees only. Various provisions of the FDIC's Acquisition Procedures, Guidance and Information (PGI) and FDIC contract clauses address the pre-exit clearance process for separating contractors. Neither the FDIC Circular nor the PGI address Legal Division outside counsel.[1] A single guidance document for pre-exit clearance

[1] For our evaluation, we are including Legal Division outside counsel among FDIC personnel that includes employees and contractors.

October 2016 OIG Memorandum Communicating Preliminary Concerns with the Pre-Exit Clearance Process

would clarify the pre-exit clearance program goals and facilitate uniform oversight. A single guidance document also would eliminate contradictory direction that currently exists in which contract clauses do not align with corporate pre-exit clearance guidance.

Timing of Contractor Notification of Separation. Separating contractors are required to complete FDIC Form 2150/03, *Data Questionnaire for Departing/Transferring Employees/Contractors*. The instructions for the data questionnaire require that the contractor complete the form at least one week, but not greater than 30 days prior to departure. However, contractors who have been issued an FDIC badge, access to the network, or issued other FDIC property or information, must notify their oversight manager of their departure no later than the date of departure.[2] Fulfilling this requirement is not possible if the contractor waits until his or her date of separation to inform the FDIC they are departing. This contradiction weakens the preventive effect of the data questionnaire to mitigate the risk of a data breach when personnel separate from the FDIC.

Program Accountability. Finally, there appears to be no single FDIC official accountable for the pre-exit clearance program. This situation could be a contributing cause to the pre-exit clearance process control weaknesses that we have identified to date. At a September 1, 2016 evaluation planning meeting with the Division of Administration (DOA), we were told that no single office is responsible for the overall performance of the pre-exit clearance process. The Government Accountability Office's (GAO's) *Standards for Internal Control in the Federal Government*[3] state that "management should evaluate performance and hold individuals accountable for their internal control responsibilities." The FDIC should designate a pre-exit clearance "process owner"[4] to ensure the pre-exit clearance process's overarching goal—to ensure that proper safeguards are taken for the protection of FDIC-owned property and interests (including sensitive information) when personnel separate—is met.

We will continue to engage with you on these concerns throughout our evaluation so we can recognize responsive management actions when we report on the assignment.

If you would like to discuss these concerns further, please contact me at (703) 562-6378, or Michael Stevens at (703) 562-6381.

cc: Charles Yi, General Counsel
Lawrence Gross, Jr., Chief Information Officer
Russell G. Pittman, DIT
Noreen Padilla, ISPS
Ronald T. Bell, DOA
Ira W. Kitmacher, DOA
Daniel H. Bendler, DOA
Rack D. Campbell, DIT
Stephen M. Hanas, Legal Division
André M. Douek, Legal Division
James H. Angel, Jr., DOF

[2] PGI Chapter 7.1, FDIC Contract Provision and Clauses, Section 7.103 Text of Provisions and Clauses, Clause 7.5.2-12 Contractor Notification of Departing Employee (August 2012).
[3] GAO-14-704G, September 2014, p. 32.
[4] GAO defines a process owner as "an individual held accountable and responsible for the workings and improvement of one of the organization's defined processes and its related subprocesses." (See GAO's *Business Process Reengineering Assessment Guide*, May 1997, p. 67).

2

OIG Review of Pre-Exit Clearance Program at Another Federal Agency

We canvassed several federal agencies to identify leading pre-exit clearance program practices. We discovered one agency that had developed pre-exit clearance policies and procedures covering that agency's employees that we determined were worthy of the FDIC's consideration for improving the Corporation's program. Leading practices include:

- Designating a single agency official, the Exit Coordinator, responsible for the pre-exit clearance process.
- Designating back-up personnel for each responsibility so that tasks do not go uncompleted.
- Avoiding overreliance on employee assertions by making an Exit Coordinator and the divisions and offices responsible for managing the pre-exit clearance process.
- Implementing a centralized electronic application, to include headquarters and field locations, to track exits for employees and contractors and send automated emails to remind exiting employees and agency staff of outstanding items.
- Establishing an electronic dashboard to allow the Exit Coordinator a status view of all exit requests and outstanding pre-exit clearance steps.
- Highlighting within the electronic application the most important documents and steps to be completed.
- Holding supervisors and human resources staff accountable, through performance ratings, for meeting requirements through system-generated reports and metrics that are sent to agency leaders.
- Including contractors in the pre-exit clearance application and taking additional steps to ensure the agency is aware of contractor separations.

We used that agency's program to help identify practices for strengthening the FDIC's pre-exit clearance process discussed in our report.

Glossary

Term	Definition
Breach	OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, dated January 3, 2017, defines a breach as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.
Computer Security Incident Response Team	An FDIC team that is responsible for collecting facts and documenting all incidents involving loss or compromise of sensitive information and notifying appropriate officials so that prompt action may be taken.
Contract Electronic File (CEFile)	A component of the FDIC's Consolidated Document Information System that Contracting Officers and Oversight Managers use to organize and file contract-related documents from the point the ASB receives an approved requisition through contract closeout. The system is designed to contain documents such as contractor proposals, technical evaluations, the contract and any modifications, confidentiality agreements, and pre-exit clearance records for contractors. The CEFile system is the official contract file.
Currency Transaction Report	A form that financial institutions are required to file with the United States Department of the Treasury Financial Crimes Enforcement Network (FinCEN) for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to the financial institution that involves a transaction in currency of more than $10,000.
Data Loss Prevention Tool	An FDIC tool that monitors outbound emails sent by employees and contractors to help to ensure they comply with FDIC's privacy and security policies.
Information Security Manager	An FDIC employee assigned by each division or office to be responsible for risk management of FDIC automated information systems and assist in the enforcement of FDIC security and privacy policies and procedures.
Insider Threat and Counterintelligence Program	An FDIC program designed to provide an integrated framework for FDIC personnel to affirmatively protect the FDIC by using a defensive program to address internal and external threats posed to its personnel, facilities, assets, resources, and classified and sensitive information, by insider threats and foreign entities.
Major Incident	According to Office of Management and Budget Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirement*, dated October 30, 2015, a major incident will be characterized by a combination of the following factors: (1) involves information that is Classified, Controlled Unclassified Information (CUI) proprietary, CUI Privacy, or CUI Other; and (2) is not recoverable, not recoverable within a specified amount of time, or is recoverable only with supplemental resources; and (3) has a high or medium functional impact to the mission of an agency; or (4) involves the exfiltration, modification, deletion or unauthorized access or lack of availability to information or systems within certain parameters to include either: (a) a specific threshold of number of records or users affected; or (b) any record of special importance. This definition, which the FDIC determined was legally binding on the FDIC, was in effect for most of the period covered by this evaluation. Subsequently, on November 4, 2016, OMB issued Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and*

Glossary

Term	Definition
	Privacy Management Requirements, which contains a different definition of a Major Incident.
Personally Identifiable Information	Any information about an individual that can be used to distinguish or trace that individual's identity, such as their full name, home address, Email address (non-work), telephone numbers (non-work), Social Security Number, driver's license or state identification number, employee identification number, date and place of birth, mother's maiden name, photograph, biometric records (e.g., fingerprint, voice print), etc. This also includes, but is not limited to, education, financial information (e.g., account number, access or security code, password, personal identification number), medical information, investigation report or database, criminal or employment history or information, or any other personal information which is linked or linkable to an individual.
Records and Information Management Unit	The Division of Administration organizational component that develops policy and procedures to govern the lifecycle (creation, management, use, and disposition) of business records and information created or received by the FDIC in the course of conducting business, and which assists FDIC employees and contractors with their records management responsibilities.
Records Liaison	An employee designated by each division or office to be responsible for providing training and guidance to ensure that records and information activities are consistent with applicable records management policy and guidance.
Risk Designation	Per FDIC Circulars 1610.2, *Personnel Security Policy and Procedures for FDIC Contractors*, and 2120.1, *Personnel Suitability Program*, employee and contractor positions are designated as High Risk, Moderate Risk, or Low Risk, commensurate with the responsibilities and attributes of the position.
Sensitive Information	Any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interest of the FDIC in carrying out its programs or the privacy to which individuals are entitled.
Suspicious Activity Report	A document that financial institutions must file with FinCEN following a suspected incident of money laundering or fraud.
User Behavior Analytics (UBA)	The tracking, collecting and assessing of user data and activities using monitoring systems and modeling to determine a baseline of normal activities specific to the organization and its users and then identify deviations from normal. Large financial and manufacturing companies currently use UBA tools to assess personnel risks. Some government agencies are also adopting this technology.

Acronyms and Abbreviations

Acronym / Abbreviation	Explanation
AO	Administrative Officer
ASB	Acquisition Services Branch
BSA	Bank Secrecy Act
CEFile	Contract Electronic File
CIOO	Chief Information Officer Organization
CMCB	Corporate Management Control Branch
CSB	Corporate Services Branch
CSIRT	Computer Security Incident Response Team
CUI	Controlled Unclassified Information
DLP	Data Loss Prevention
DOA	Division of Administration
DOF	Division of Finance
ERM	Enterprise Risk Management
eWORKS	Enterprise Workforce Solution
FDIC	Federal Deposit Insurance Corporation
FinCEN	United States Department of the Treasury Financial Crimes Enforcement Network
GAO	Government Accountability Office
HRB	Human Resources Branch
ISM	Information Security Manager
ISPS	Information Security and Privacy Staff
ITCIP	Insider Threat and Counterintelligence Program
LERS	Labor and Employee Relations Section
MSB	Management Services Branch
OIG	Office of Inspector General
OM	Oversight Manager
OMB	Office of Management and Budget
PGI	Procedures, Guidance, and Information
PIV	Personal Identity Verification
RIMU	Records and Information Management Unit
RL	Records Liaison
RMS	Division of Risk Management Supervision
SOP	Standard Operating Procedure
UBA	User Behavior Analytics
USB	Universal Serial Bus
U.S.C.	United States Code

Corporation Comments

FDIC
Federal Deposit Insurance Corporation
3501Fairfax Drive, Arlington, VA 22226
Division of Administration

DATE: September 15, 2017

MEMORANDUM TO: E. Marshall Gentry, Assistant Inspector General for Program Audits and Evaluations

FROM: /**Signed**/
Arleas Upton Kea, Director
Division of Administration

SUBJECT: Management Response to the OIG Draft Report Entitled, *Controls over Separating Personnel's Access to Sensitive Information* (Assignment No. 2016-038)

The Federal Deposit Insurance Corporation (FDIC) has completed its review of the Office of Inspector General's (OIG) draft audit report entitled Controls over Separating Personnel's Access to Sensitive Information (Assignment No. 2016-038), dated August 2, 2017.

We appreciate the OIG's analysis and findings regarding the FDIC's employee and contractor separation process. We particularly appreciate the OIG's recognition of the procedures already in place and the new technological measures taken to detect and prevent separating personnel from removing information from the Corporation. FDIC's senior leadership considers the protection of sensitive information and assets (both physical and informational) among its highest priorities. The Agency's continuous attention to preventative, detective, and corrective controls in this area is designed to provide ongoing assurance that access to sensitive information is monitored, restricted, and acted upon when attempts to violate policy are detected.

To that end, the FDIC has made, and continues to make, great strides in protecting sensitive information on an ongoing basis, and with respect to potentially high risk events such as when personnel separate from the Agency. For example, the Agency has implemented a number of mitigating technical controls which address risks associated with departing FDIC employees and contractors. The FDIC has restricted (with limited exceptions) the ability of network users to copy information to removable media to reduce the risk of unauthorized exfiltration of sensitive information. Further, in the last year, the FDIC has implemented the use of PIV cards as a key control for logical and physical access of FDIC employees and contractors. Capture of the PIV cards at the time of departure for FDIC employees and contractors helps to ensure that the departing individual no longer has physical access to FDIC buildings or access to the FDIC network. In addition, the FDIC has established an Insider Threat Program to affirmatively protect the FDIC using a defensive program to address internal and external threats and risks posed to the agency's personnel, facilities, assets, resources, and classified and sensitive information.

Corporation Comments

We recognize the need to address remaining risks and implement improvements to the pre-exit clearance process going forward. As such, we appreciate the OIG's helpful observations and recommendations contained throughout the subject draft report.

The audit report identifies eleven recommendations to strengthen information security. FDIC management concurs with the report's findings and is committed to addressing each of the OIG's recommendations to further strengthen the FDIC's controls over the process for separating personnel. Our responses below contain actions already completed, planned or in process.

Recommendation 1: The OIG recommends that the Director, Division of Administration (DOA), designate a pre-exit clearance process owner who will be accountable for the FDIC's pre-exit clearance program.

Management Decision: DOA management concurs with this recommendation.

Corrective Actions: The Director of DOA accepts full responsibility and accountability for the FDIC's pre-exit clearance program. In a May 17, 2017, email to all FDIC Division and Office Directors, the Director of DOA reminded her colleagues that DOA has overall responsibility for the pre-exit clearance process under the provisions of Circular 2150.1 entitled *Pre-Exit Clearance Procedures for FDIC Employees*. In that email, DOA's Director stated that DOA's Management Services Branch (MSB) would be reaching out to Administrative Officers (AOs) to reinforce several important requirements of the FDIC's pre-exit clearance directive. The email further explained that DOA is pursuing this important effort to better ensure that we collectively take proper safeguards for the protection of FDIC-owned property and information when employees separate from the Agency. DOA's message emphasized that security at the FDIC (both physical and informational) is of the highest priority, and we will continue to raise staff's awareness to their role in protecting that security. It should be noted that the DOA Director's message emphasizing her overall responsibility for the pre-exit clearance process was issued with the knowledge and approval of the Chairman.

Estimated Completion Date: Completed May 17, 2017.

Recommendation 2: The OIG recommends that the Director DOA incorporate a risk assessment of individual separating employees into the FDIC's pre-exit clearance process.

Management Decision: DOA management concurs with this recommendation.

Corrective Action: DOA's executive leadership team and senior officials from the Chief Information Officer Organization (CIOO) have been collaborating to identify a viable approach for incorporating risk assessments into the pre-exit clearance process. A number of factors are being evaluated as potential indicators of risk when an employee announces his/her intention to leave the Agency. These factors include:

Corporation Comments

- The risk designation of the employee's position (as determined by the Agency's Risk Level Designation Process).
- Personal financial issues revealed through background investigations.
- Signs of disgruntlement such as repeated disputes with FDIC management.
- Performance concerns, such as evidence of poor judgment and lack of accountability for actions.
- Prior disciplinary actions to address performance or behavior issues.
- Prior violations of FDIC security policies.
- Attempts to obtain unauthorized access to sensitive information.
- Excessive copying or reproduction of sensitive information.

The FDIC acknowledges that immediate supervisors within divisions and offices are in the best position to evaluate the risks associated with separating employees. Division and office Information Security Managers (ISMs) and DOA's Labor and Employee Relations (LER) officials are also well-positioned to assess certain risks associated with separating employees.

The FDIC will also rely on the Agency's evolving Insider Threat and Counterintelligence Program to support personnel-specific risk assessments to help identify risks associated with pre-exit clearance. Among other initiatives, the FDIC's Insider Threat Program is considering the merits and feasibility of deploying a "user behavior analytics" (UBA) tool to help assess personnel risks in an automated comprehensive manner. UBA could help the FDIC identify what population of personnel poses the most risk, the types of data associated with various threat events, and the FDIC systems/applications that contain the data needed for analysis. DOA and CIOO officials are currently evaluating UBA tools already in place and how such tools could be leveraged to support the pre-exit clearance process.

DOA will continue to collaborate with Division and Office officials to establish specific procedures and protocols for incorporating a fundamental risk assessment as part of the pre-exit clearance process. These procedures and protocols will be vetted through the Legal Division, Labor and Employee Relations, the National Treasury Employees Union, and the Office of Inspector General to ensure that new procedures comply with relevant privacy laws and regulations and other requirements.

Estimated Completion Date: February 28, 2018.

Recommendation 3: The OIG recommends that the Director DOA work with the FDIC's Chief Information Officer to establish appropriate policy for using DLP to support the FDIC's pre-exit clearance process.

Management Decision: DOA management concurs with this recommendation.

Corrective Action: DOA will coordinate with the FDIC's CIOO and the Chief Information Security Officer to establish formal policy for using the appropriate security controls/monitoring

3

Corporation Comments

tools, including Data Loss Prevention (DLP), to support the FDIC's pre-exit clearance process. The FDIC directive for the pre-exit clearance process will be revised and published with this information by June 1, 2018.

Estimated Completion Dates: June 1, 2018.

Recommendation 4: The OIG recommends that the Director DOA revise the Data Questionnaire (FDIC Form 2150/03) to improve identification, tracking, and protection of sensitive information for separating personnel.

Management Decision: DOA management concurs with this recommendation.

Corrective Action: DOA's Records and Information Management Unit (RIMU) has revised the Data Questionnaire (FDIC Form 2150/03). The revised Form 2150/03 incorporates changes that will strengthen the identification, tracking, and protection of corporate records. Changes include employee signature with specific acknowledgements regarding preservation of records; records removal; use of nonpublic information for private interests; and the legal remedies available to the FDIC should the employee breach the agreements specified on Form 2150/03.

Estimated Completion Date: Completed August 24, 2017.

Recommendation 5: The OIG recommends that the Director DOA work with the General Counsel to strengthen acknowledgments and warnings in pre-exit clearance forms and non-disclosure agreements regarding breaches of sensitive information and the associated consequences.

Management Decision: DOA management concurs with this recommendation.

Corrective Action: DOA RIMU has coordinated with the General Counsel's Office to incorporate new and stronger acknowledgements and warnings into the revised Data Questionnaire – Form 2150/03 that protects the FDIC should an employee breach any of the acknowledgements detailed in the 2150/03. Additionally, with the introduction of this revised form, employees are now required to sign the form to acknowledge their understanding. Regarding the pre-exit clearance Form 2150.01, DOA will continue working with the Legal Division to strengthen acknowledgments and warnings regarding breaches of sensitive information and associated consequences and revise the Form 2150.1 accordingly.

Estimated Completion Date: Completed Form 2150/03 revision on August 24, 2017; Revised Form 2150/01 estimated by January 15, 2018.

Corporation Comments

Recommendation 6: The OIG recommends that the Director DOA reinforce corporate-wide understanding of the significance of and requirements for pre-exit clearance policies and procedures among stakeholders in the pre-exit clearance process.

Management Decision: DOA management concurs with this recommendation.

Corrective Actions: On June 14, 2017, DOA's Management Services Branch (MSB) provided guidance to all division and office Administrative Officers (AO's) to reinforce the corporate-wide requirements for the pre-exit clearance process. MSB's guidance referenced Director Kea's May 17, 2017 message to all division and office Directors and provided additional clarity regarding newly implemented improvements to the pre-exit clearance process. In particular, MSB informed division and office AO's that, effective June 25, 2017 (pay period 13), all FDIC regional and field offices would be required to send completed FDIC pre-exit clearance forms (Form 2150/01) including supporting documentation to DOA's MSB. It was further communicated that MSB would review every form to ensure that all steps have been followed and would retain the forms in accordance with Circular 2150.1, entitled *Pre-Exit Clearance Procedures for FDIC Employees*. To help ensure proper accountability and responsiveness, MSB required every division and office to designate a point-of-contact who will be responsible for collecting and sending employees' pre-exit forms to MSB as well as researching incomplete information. As an added internal control, MSB verifies that every separating employee's access to FDIC's network has been deactivated.

Given the importance of its role in the pre-exit clearance process, in June 2017, MSB developed comprehensive Standard Operating Procedures (SOPs) to ensure consistency and clarity in administering the program. The SOP's describe the program's purpose, responsibilities of key stakeholders, specific step-by-step procedures, operating examples, and mandatory compensating controls to help ensure full compliance with FDIC Circular 2150.1. Management believes that these new procedures and controls, which became effective on June 25, help to reinforce a corporate-wide understanding of the significance of and requirements for pre-exit clearance policies and procedures among stakeholders in the pre-exit clearance process.

Estimated Completion Date: Completed June 25, 2017.

Recommendation 7: The OIG recommends that the Director DOA work with the Director, DOF, to develop a schedule for future CMC program reviews of the pre-exit clearance program.

Management Decision: DOA Management concurs with this recommendation.

Corrective Action: DOA's MSB has included in its annual internal review plan specific reviews of the pre-exit clearance program. MSB will include personnel from DOF's Corporate Management Control Branch to participate on these internal reviews as appropriate.

Estimated Completion Date: Completed August 24, 2017.

Corporation Comments

Recommendation 8: The OIG recommends that the Director DOA establish a comprehensive pre-exit clearance policy for contractors.

Management Decision: DOA management concurs with this recommendation.

Corrective Action: In June 2017, DOA formed an inter-divisional working group consisting of officials from DOA, the Legal Division, Division of Finance, and the CIOO. The working group developed an Action Plan to improve the overall process for managing, tracking, and reporting on the status of FDIC contractors. A number of action items are underway that will help ensure that:

- Official systems of record contain accurate contractor data.
- Contractor employees who are no longer working under FDIC contracts do not have network or physical access.
- Procedures are developed to continuously monitor and update FDIC systems that contain contractor employee information.
- New written procedures covering all aspects of the contractor pre-exit clearance process are fully developed.
- Oversight Managers and other FDIC staff who play a critical role in the contractor pre-exit clearance process receive proper training.

Recently, a dedicated Project Manager was assigned to help oversee and manage the working group's Action Plan. All Action Plan tasks including the development of comprehensive pre-exit clearance procedures for contractors will be completed by January 31, 2018.

Estimated Completion Date: January 31, 2018.

Recommendation 9: The OIG recommends that the Director DOA ensure that assigned personnel are reviewing contractor Pre-Exit Clearance Records and Data Questionnaires timely and documenting their work appropriately.

Management Decision: DOA management concurs with this recommendation.

Corrective Action: DOA MSB will continue to conduct periodic compliance reviews of the contractor pre-exit process. Currently, DOA MSB is performing a review of the contractor pre-exit process that will be completed by the end of this year.

Estimated Completion Date: December 31, 2017.

Recommendation 10: The OIG recommends that the Director DOA work with the FDIC's Chief Information Officer (CIO) to develop an expanded and better defined use of the DLP tool for separating contractors.

Corporation Comments

Management Decision: DOA management concurs with this recommendation.

Corrective Action: DOA will coordinate with the FDIC's CIOO and the Chief Information Security Officer to develop an expanded and better defined use of the appropriate security controls/monitoring tools for separating contractor employees. We will identify and implement the appropriate security controls/tools to meet this requirement by June 1, 2018.

Estimated Completion Date: September 30, 2018.

Recommendation 11: The OIG recommends that the Director DOA require contractor organizations to provide a reasonable notice of separation in most circumstances, unless there are extenuating circumstances, as defined in the contracts.

Management Decision: DOA management concurs with this recommendation.

Corrective Action: DOA will develop contract clauses to be used in all future contract awards and will modify existing contracts (where security and information privacy/sensitivity is particularly relevant) that will require contractors to: (1) periodically validate the population of all contractor employees assigned to their contract; and (2) provide reasonable advance notice when contractor employees are scheduled to depart.

Estimated Completion Date: January 15, 2018.

If you have any questions regarding this response, our point of contact for this matter is Dan Bendler at (703) 562-2123.

Summary of the Corporation's Corrective Actions

This table presents the corrective actions taken or planned by the Corporation in response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The DOA Director sent a May 17, 2017 email to all FDIC division and office directors reiterating that DOA has overall responsibility for the pre-exit clearance process and that MSB would be reinforcing important pre-exit clearance requirements with division and office AOs.	May 17, 2017	No	Yes	Open
2	DOA and CIOO representatives are collaborating to identify a viable approach for incorporating risk assessments into the pre-exit clearance process. The FDIC will also leverage the evolving ITCIP to support personnel-specific risk assessments. DOA will ultimately establish specific procedures and protocols for incorporating a fundamental risk assessment as part of the pre-exit clearance process.	February 28, 2018	No	Yes	Open
3	DOA will coordinate with the FDIC's CIOO and the Chief Information Security Officer to establish formal policy for using appropriate security controls and monitoring tools, including the DLP, to support the FDIC's pre-exit clearance process and will revise the pre-exit clearance directive accordingly.	June 1, 2018	No	Yes	Open
4	RIMU revised the Data Questionnaire (FDIC Form 2150/03) to strengthen the identification, tracking, and protection of corporate records. Changes include requiring an employee signature with specific acknowledgements regarding the preservation of records and legal remedies available to the FDIC should the employee breach the agreements specified on the form.	August 24, 2017	No	Yes	Open
5	RIMU coordinated with the General Counsel's Office to incorporate new and stronger acknowledgements and warnings into the revised Data Questionnaire. Employees are now	January 15, 2018	No	Yes	Open

Summary of the Corporation's Corrective Actions

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
	required to sign the form to acknowledge their understanding. DOA will continue working with the Legal Division to strengthen acknowledgments and warnings regarding breaches of sensitive information and associated consequences and will revise the form accordingly.				
6	On June 14, 2017, MSB provided guidance to all division and office AOs to reinforce the corporate-wide requirements for the pre-exit clearance process. MSB began requiring all AOs to send pre-exit clearance forms for MSB review. MSB also required each division and office to designate a point-of-contact for collecting and sending pre-exit clearance forms to MSB.	June 25, 2017	No	Yes	Open
7	MSB included in its annual internal review plan specific reviews of the pre-exit clearance program. MSB will include CMCB personnel to participate on these internal reviews as appropriate.	August 24, 2017	No	Yes	Open
8	In June 2017, DOA formed an inter-divisional working group and developed an Action Plan to improve the overall process for managing, tracking, and reporting on the status of FDIC contractors.	January 31, 2018	No	Yes	Open
9	MSB will continue to conduct periodic compliance reviews of the contractor pre-exit process. As discussed in management's response to recommendation 1, MSB also reinforced important pre-exit clearance requirements with division and office AOs.	December 31, 2017	No	Yes	Open
10	DOA will coordinate with the FDIC's CIOO and the Chief Information Security Officer to develop an expanded and better defined use of the appropriate security controls and monitoring tools for separating contractor employees and will implement such controls and tools.	September 30, 2018	No	Yes	Open
11	DOA will develop contract clauses to be used in all future contract awards	January 15, 2018	No	Yes	Open

Summary of the Corporation's Corrective Actions

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
	and will modify existing contracts (where security and information privacy/sensitivity is particularly relevant) that will require contractors to: (1) periodically validate the population of all contractor employees assigned to their contract; and (2) provide reasonable advance notice when contractor employees are scheduled to depart.				

[a] Resolved – (1) Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Recommendations will be closed when the OIG confirms that corrective actions have been completed and are responsive.