The FDIC's Personnel Security and Suitability Program

January 2021 **EVAL-21-001**

Evaluation Report

Program Audits and Evaluations

☆☆☆☆☆☆☆☆

REDACTED VERSION

PUBLICLY AVAILABLE

Portions of this report containing sensitive information have been redacted and are marked accordingly.

Office of Inspector General

Executive Summary

The FDIC's Personnel Security and Suitability Program

Before individuals can be hired by the Federal Deposit Insurance Corporation (FDIC), they must meet minimum standards for employment with the FDIC. Contractor personnel must meet minimum standards of integrity and fitness. Collectively, these standards ensure that individuals working for or on behalf of the FDIC have not been convicted of a felony, demonstrated a pattern or practice of defaulting on obligations to insured depository institutions, been removed from banking, or caused significant loss to deposit insurance funds. In this report, we refer to the determination of whether an individual meets these standards as a Preliminary Background Investigation (PBI). Federal regulations also require that a background investigation (BI) be conducted on each Federal employee and contractor personnel.

According to the Defense Counterintelligence Security Agency (DCSA), which is responsible for conducting BIs for the Federal Government, "[i]n the interest of safeguarding the welfare of the American people, it is required that all persons privileged to be employed in the departments and agencies of the United States Government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States." Some BIs are done for the purpose of a "suitability" determination. Suitability refers to a person's character or conduct that may have an impact on the integrity or efficiency of the individual's government service. Other BIs are done to determine whether an individual can obtain access to classified national security information. Additionally, employees and contractors are subject to periodic reinvestigations, which are conducted as a means to ensure the ongoing trustworthiness of an individual.

According to the U.S. Government Accountability Office, "[a] high-quality personnel security clearance process minimizes the risks of unauthorized disclosures of classified information and helps ensure that information about individuals with criminal histories or other questionable behavior is identified and assessed."

The FDIC's Personnel Security and Suitability Program (PSSP) is designed to ensure that its employees and contractor personnel meet applicable Federal security and suitability requirements and do not jeopardize the accomplishment of the FDIC's mission. The effectiveness of the FDIC's PSSP is critically important to ensure that FDIC employees and contractor personnel are properly screened and investigated before being granted access to systems and entrusted with sensitive, confidential, or, in some cases, classified information.

Our evaluation objective was to determine whether the FDIC has an effective program to: (1) complete PBIs in a timely manner before hiring individuals; (2) order and adjudicate BIs commensurate with position risk designations and reciprocity rules; and (3) order reinvestigations within required timeframes.

Results

We determined that the FDIC's PSSP was not fully effective in ensuring that: (1) PBIs were completed in a timely manner; (2) BIs were ordered and adjudicated commensurate with position risk designations; and (3) re-investigations were ordered within required timeframes. Specifically, through our analysis of PSSP-related data for all employees and contractor personnel with access to the FDIC's information technology systems as of December 2, 2019, we found that:

- The FDIC did not remove multiple contractors with unfavorable background investigation adjudications in a timely manner;
- The FDIC did not follow its Insider Threat protocols and conducted limited risk assessments for the contractors with unfavorable adjudications;
- The FDIC did not initiate and order numerous required periodic reinvestigations in a timely manner;
- Data on contractor position risks were unreliable;
- Employee background investigations were sometimes not commensurate with position risk;
- Some of the FDIC files were missing certain PBI data; and
- The FDIC was not meeting its goals for completing PBIs within a specified timeframe.

We did find, however, that the FDIC was adhering to reciprocity requirements.

In 2018, the FDIC began working to implement process changes, including implementing a business process management system and addressing data quality issues. The FDIC also increased SEPS staffing. However, some of the process changes, including the implementation of the business process management system, were envisioned in 2014, more than 6 years ago. In addition, some issues we identified in this present report (2021) were similar to those identified in several prior reports, including our OIG evaluation of the FDIC's PSSP in 2014. Specifically, a number of issues—timeliness of PBIs; missing documentation; BIs not being consistent with position risk; and the reliability of PSSP-related data—were identified previously by the OIG, but still do not appear to be corrected.

"Security – Personnel and Physical" is among the risk areas identified as part of the FDIC's Enterprise Risk Management (ERM) Program. However, the results of our

evaluation led us to conclude that the risks within the FDIC's PSSP were not fully reflected in the FDIC's Risk Inventory, which informs the Risk Profile. The FDIC's Operating Committee, as the Risk Management Council, must ensure that the Division of Administration is satisfactorily addressing the risks associated with the PSSP.

This risk analysis is particularly important now as the FDIC begins contingency planning for potential surge staffing in case its workload increases as a result of the current pandemic situation negatively impacting the banking sector. The FDIC anticipates the potential for increased hiring to ensure readiness for any increase in supervisory workload, bank failure activity, and administrative support. The FDIC's Operating Budget for 2021 rose by $261 million (12.9 percent), largely due to "contingency reserves to address a potential increase during 2021 in supervision or resolution workload resulting from the ongoing pandemic." Implementation of a surge staffing scenario will dramatically increase the number of suitability screenings and BIs processed through the PSSP.

Recommendations

The report includes 21 recommendations aimed at strengthening the PSSP's controls and ensuring that the FDIC is in full compliance with Federal requirements. We recommended that the FDIC re-evaluate enterprise-level risks to reflect the weaknesses highlighted in this report (and prior reports) and communicate any changes to the Operating Committee. We also recommended that the FDIC update policies and procedures, conduct additional training, and establish monitoring techniques to ensure that individuals deemed unfavorable are removed. In addition, we recommended that the FDIC: (1) develop and implement a plan to ensure that it completes periodic reinvestigations in a timely manner; (2) correct system data and position risk inaccuracies; and (3) address PBI weaknesses, including the development of metrics, reports, and monitoring for compliance with statutory requirements. The FDIC concurred with all 21 recommendations.

Contents

Background **3**

Evaluation Results **13**

The FDIC Has Not Fully Recognized the Level of Risk Within Its Personnel Security and Suitability Program 15
Removal of FDIC Contractor Personnel with Unfavorable Adjudications Delayed 20
The FDIC Conducted Limited Risk Assessments for Insider Threats 27
The FDIC Did Not Initiate and Order Required Periodic Reinvestigations 30
Contractor Risk Level Recorded in CHRIS Not Accurate 34
Employee Background Investigations Not Commensurate with Position Risk Designations 36
CHRIS Missing Data on PBI Completion Dates 38
The FDIC Not Meeting Goal Established to Complete PBIs 40
The FDIC Is Adhering to Reciprocity Requirements 41

FDIC Comments and OIG Evaluation **41**

Appendices

1. Objective, Scope, Methodology 43
2. List of Executive Orders 47
3. Acronyms 49
4. FDIC Comments 50
5. Summary of the FDIC's Corrective Action 61

Tables

1. FDIC Directives Associated with the PSSP 6
2. Public Trust Risk Levels and Investigation Requirements 8
3. National Security Positions and Investigation Requirements 9
4. Contractors with Unfavorable Adjudications Removed Based on OIG Evaluation Results 21
5. Delays in Removal of Seven Contractors with Unfavorable Adjudications 23
6. Reinvestigation Requirements for Public Trust and National Security Positions 30
7. OIG Analysis of Selected PR Cases 31
8. OIG Analysis of Missing PBI Completion Dates in CHRIS 39
9. OIG Analysis of PBI Timeliness 40

January 19, 2021

Subject ***The FDIC's Personnel Security and Suitability Program***

Before individuals can be hired by the Federal Deposit Insurance Corporation (FDIC), they must meet minimum standards for employment with the FDIC.[1] Contractor personnel must meet minimum standards of integrity and fitness.[2] Collectively these standards ensure that individuals working for or on behalf of the FDIC have not been convicted of a felony, demonstrated a pattern or practice of defaulting on obligations to insured depository institutions, been removed from banking, or caused significant loss to deposit insurance funds.[3] Federal regulations also require a background investigation (BI) be conducted on each Federal employee and contractor.[4] The type of BI varies based on the degree of risk and sensitivity of the position for which the individual is being considered.

According to the Defense Counterintelligence Security Agency (DCSA), which is responsible for conducting BIs for the Federal Government,[5] "[i]n the interest of safeguarding the welfare of the American people, it is required that all persons privileged to be employed in the departments and agencies of the United States Government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States."[6] Some BIs are done for the purpose of a "suitability" determination. Suitability refers to a person's character or conduct that may have an impact on the integrity or efficiency of the individual's government service.[7] Other BIs are done to determine whether an individual can obtain access to classified national security information. Additionally, employees and contractors are subject to periodic reinvestigations (PR), which are conducted as a means to ensure the ongoing trustworthiness of an individual.

The Security Clearance, Suitability, and Credentialing Performance Accountability Council (PAC) is responsible for leading the Government-wide implementation of security, suitability, and credentialing reform. The principal agencies of the PAC are

---

[1] 12 U.S.C. § 1822(f).
[2] *Id*.
[3] In this report we refer to the determination of whether an individual meets the FDIC's minimum employment or integrity and fitness standards as a Preliminary Background Investigation (PBI).
[4] The authority for determining suitability for federal employment in the competitive service is vested in 5 U.S.C. §§ 3301, 3302, and 7301 and 5 C.F.R. parts 5, 731, and 736. Authority for National Security Positions is found in 5 C.F.R. pt. 732.
[5] On April 24, 2019, Executive Order 13869 was signed shifting primary responsibility for conducting background investigations for the Federal government from the Office of Personnel Management to DCSA, effective October 1, 2019.
[6] DCSA Website (https://www.dcsa.mil/mc/pv/mbi/).
[7] Suitability determinations apply to employees. The equivalent for contractors is referred to as a fitness determination.

the Office of Management and Budget, Office of the Director of National Intelligence, Office of Personnel Management, and the Department of Defense. The PAC stated that "[o]ur world is changing at a pace that requires the security, suitability/fitness, and credentialing community to anticipate, detect, and counter both internal and external threats, such as those posed by trusted insiders who may seek to do harm to the Federal Government's policies, processes, and information systems."[8] The U.S. Government Accountability Office (GAO) reported that "[a] high-quality personnel security clearance process minimizes the risks of unauthorized disclosures of classified information and helps ensure that information about individuals with criminal histories or other questionable behavior is identified and assessed."[9]

The FDIC's Personnel Security and Suitability Program (PSSP) is designed to ensure that its employees and contractor personnel[10] meet applicable Federal security and suitability requirements and do not jeopardize the accomplishment of the FDIC's mission. To avoid duplication of work, Federal reciprocity guidelines require the FDIC to accept background investigations, suitability decisions, and security clearance determinations conducted by other authorized agencies, provided that they are within defined timeframes and risk parameters. The effectiveness of the FDIC's PSSP is critically important to ensure that FDIC employees and contractor personnel are properly screened and investigated before being granted access to systems and entrusted with sensitive, confidential, or, in some cases, classified information.

The FDIC OIG previously evaluated the FDIC's PSSP in 2014.[11] At that time, we reported that the FDIC's PSSP was in a state of transition with various aspects of the program still evolving. The report included 10 recommendations to strengthen controls in the following areas: (1) overall program administration; (2) the FDIC's oversight of contractor personnel who support the PSSP; (3) records management; and (4) information systems. The FDIC closed the recommendations without further review by the OIG.[12] Notably, we found that the FDIC was still working to implement process changes envisioned in 2014, more than 6 years ago. In addition, some issues we identified in this present report (2021) were similar to those identified in several prior reports, including our OIG evaluation of the FDIC's PSSP in 2014.

[8] President's Management Agenda, Mission Priority Issue, *Security Clearance, Suitability, and Credentialing Reform, Cross-Agency Priority Goal Action Plan* (September 2020).
[9] U.S. GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas* (GAO-19-157SP) (March 2019).
[10] All employees of a contractor or subcontractor who work under an FDIC contract. For the purposes of this report, all references to contractor, contractor personnel, and contractor employee refer to the employees of a company with whom the FDIC has established a services contract.
[11] OIG Report, *The FDIC's Personnel Security and Suitability Program* (EVAL-14-003) (August 2014).
[12] The FDIC closed recommendations without OIG review of the corrective actions. At the time, the OIG did not review all corrective actions before recommendations were closed. The OIG has since revised its processes, and the OIG now reviews all corrective actions to determine whether the FDIC's actions satisfy the recommendation and therefore can be considered closed.

Specifically, a number of issues—timeliness of PBIs; missing documentation; BIs not being consistent with position risk; and the reliability of PSSP-related data—were identified previously by the OIG but still do not appear to be corrected.

Our evaluation objective was to determine whether the FDIC has an effective program to: (1) complete PBIs in a timely manner before hiring individuals; (2) order and adjudicate BIs commensurate with position risk designations and reciprocity rules; and (3) order reinvestigations within required timeframes.

To answer our objective, we reviewed PSSP-related data in the FDIC's Corporate Human Resource Information System (CHRIS) for all employees and contractor personnel with access to the FDIC's information technology (IT) systems as of December 2, 2019.[13] The population included 7,254 individuals consisting of 5,744 FDIC employees and 1,510 FDIC contractor personnel. We used data analytics to identify anomalies within the population. We then reviewed case file documentation in order to substantiate and draw conclusions on our test results. Appendix 1 of this report includes details about our objective, scope, and methodology.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation. We conducted this evaluation from June 2019 to September 2020. We performed our work at the FDIC's offices at Virginia Square in Arlington, Virginia.

BACKGROUND

PSSP Roles and Responsibilities at the FDIC

The Deputy to the Chairman and Chief Operating Officer provides day-to-day management and supervision of the Division of Administration (DOA). Within DOA, the Deputy Director, Corporate Services Branch, oversees the Assistant Director, Security and Emergency Preparedness Section (SEPS). The Assistant Director, SEPS is responsible for the administration of the PSSP.

Within SEPS, the Chief, Security Operations Unit, is responsible for the day-to-day management of the FDIC's PSSP, including:

[13] In addition to serving as the authoritative source for employee data, CHRIS maintains background investigation submission/clearance dates for FDIC employees. CHRIS is also used to record the BI results of FDIC contractors and non-FDIC government employees.

- Validating position risk designations for all positions at the FDIC;
- Ensuring reciprocity is applied in accordance with Federal requirements and guidance;
- Initiating appropriate BIs corresponding to position risk designation levels;
- Reviewing the results of BIs;
- Granting adjudicative decisions; such as, but not limited to approval, denial, revocation, and removal;
- Ensuring security/suitability adjudications of persons employed by the FDIC are completed in a timely manner;
- Coordinating with DOA's Labor and Employee Relations officials and management as appropriate; and
- Complying with the Personnel Suitability Program administration and reporting requirements.

The Personnel Security Group (PSG) supports the Chief, Security Operations, in executing these responsibilities. To assist in processing PBIs and BIs, SEPS relies on approximately 29 contractor personnel, who are overseen by FDIC Personnel Security Specialists in the PSG.

Others within the FDIC also fulfill key responsibilities related to the PSSP. For example:

- Division/Office Directors (or designee) are responsible for adhering to the FDIC's PSSP;
- Administrative Officers (AO) facilitate the position designation process and ensure newly created or amended position descriptions are submitted to the specific Division or Office Information Security Managers and the Human Resource Branch and submit personnel security documents and forms to SEPS; and
- Oversight Managers (OM) and Technical Monitors (TM) are responsible for managing all aspects of contractor security, including establishing contractor position risk level designations, requesting contractor access to FDIC facilities and IT resources, and ensuring contractor removal. In addition, OMs and TMs must perform quality control on all security requests[14] to ensure accuracy, completeness, and legibility of the forms prior to submitting them to the PSG.

SEPS personnel are responsible for communicating adjudication decisions to Division or Office AOs (for employees), or OMs (for contractor personnel), so that these officials take appropriate action to remove individuals when an unfavorable adjudication determination is rendered.

[14] FDIC Form 1600/13, *Personnel Security Action Request*.

Overview of the the FDIC's PSSP Policies

The FDIC vets all employees and contractor personnel performing any service for or on behalf of the FDIC by implementing the security eligibility and suitability requirements found within Federal regulations, various Executive Orders (EO),[15] and guidance from the United States Office of Personnel Management (OPM) and Office of the Director of National Intelligence (ODNI).[16] To meet these requirements, the FDIC has established procedures to ensure that any individual who is performing, directly or indirectly, any function or service on behalf of the Agency meets minimum standards of integrity and fitness.[17] In this regard, the FDIC prohibits any person from performing any service on behalf of the agency who has:

a) Been convicted of any felony;
b) Been removed from, or prohibited from participating in the affairs of, any insured depository institution pursuant to any final enforcement action by any appropriate Federal banking agency;
c) Demonstrated a pattern or practice of defalcation[18] regarding obligations to insured depository institutions; or
d) Caused a substantial loss to Federal deposit insurance funds.[19]

All applicants, employees, and contractor personnel who have or may have access to FDIC facilities, information technology systems, and sensitive or classified information for longer than 6 months must first meet the FDIC minimum standards for integrity and fitness. FDIC procedures provide that applicants, employees, and contractor personnel may be subjected to modified vetting if they will have access for less than 6 months.[20] Table 1 outlines the FDIC Policy Directives associated with the PSSP.

[15] Various Presidential EOs govern the personnel suitability and security clearance process. Appendix 2 includes a brief description of relevant EOs.
[16] The Director, OPM, serves as the Suitability Executive Agent, and the Director of National Intelligence serves as the Security Executive Agent. In that role, the Directors have responsibility for developing uniform and consistent policies and procedures to ensure effective, efficient, and timely completion of investigations relating to suitability and security determinations, respectively.
[17] 12 U.S.C. § 1822; Directive 2120.5, *Minimum Standards for Employment with the Federal Deposit Insurance Corporation as Mandated by the Resolution Trust Corporation Completion Act* dated February 2013.
[18] Patterns or Practice of Defalcation is defined in 12 C.F.R. § 336.3(i) to include a history of financial irresponsibility with regard to debts owed to insured depository institutions, which are in default in excess of $50,000 in the aggregate and wrongful refusal to fulfill duties and obligations to depository institutions.
[19] A substantial loss is defined to be a loan or advance or final judgment that is delinquent for 90 or more days in excess of $50,000.
[20] 5 C.F.R. 732.202(b)(1)(i) permits exceptions to certain positions. These positions are intermittent, seasonal, per-diem, or temporary not to exceed an aggregate of 180 days either in a single continuous appointment or a series of appointments.

Table 1: FDIC Directives Associated with the PSSP

Directive No.	Title	Purpose
Directive 2150.5 **February 22, 2013**	***Minimum Standards for Employment with the Federal Deposit Insurance Corporation ("Corporation") as Mandated by the Resolution Trust Corporation Completion Act ("RTCCA")*** **(PBI Directive)**	Prohibits any person who does not meet the statutorily imposed minimum standards of integrity and fitness from becoming employed or otherwise performing any service for or on behalf of the FDIC.
Directive 2120.2 **January 15, 2020***	***Personnel Security and Suitability Program for Applicants and Employees*** **(PSSP Employee Directive)**	Provides FDIC policy relating to applicant and employee personnel security and suitability in accordance with Federal directives and authorities.
Directive 1610.2 **January 15, 2020***	***Personnel Security and Suitability Program for Contractors and Contractor Personnel*** **(PSSP Contractor Directive)**	Provides policy relating to contractors and contractor personnel security and fitness in accordance with Federal directives and authorities.
Directive 1600.3 **September 24, 2001**	***National Security Program*** **(National Security Directive)**	Establishes policy and implements guidance for the FDIC's National Security Program outlining the process for determining National Security Position sensitivity, the investigative requirements for a position, and the process for granting security clearances.

Source: FDIC Directives as noted.
*These Directives superseded prior versions reviewed and considered during our fieldwork, as discussed in Appendix 1.

The FDIC also maintains two internal guides with detailed procedures and guidance for FDIC officials with PSSP responsibilities: *Personnel Security Guide for FDIC Employee Background Investigations* and *Personnel Security Procedures Guide for Contracting Officers and Oversight Managers*.

In 2018, the PAC began the process of creating the Trusted Workforce 2.0 Framework. According to ODNI's website, the Framework is "the start of a wide-ranging effort to overhaul how background investigations are conducted." The Trusted Workforce 2.0 Framework includes plans for reducing the number of levels in the security clearance process from five to three and aligning investigative criteria for security, suitability, and credentialing requirements at each stage. As the implementation of the Trusted Workforce 2.0 Framework continues, the FDIC will need to ensure that its policies and procedures are kept up-to-date.

Overview of the FDIC's PBI and BI Process Steps

PBI Process. To evaluate whether an individual meets the FDIC's minimum requirements, as part of the PBI process, the FDIC reviews information about the individual's criminal, employment, and financial history to verify whether the individual has any delinquent Federal debt or caused substantial loss to the Federal deposit insurance funds. After reviewing this information, PSG officials decide whether individuals can begin working for or on behalf of the FDIC. Absent any disqualifying issues, the FDIC's goal is to complete the PBI process within 5 days.[21]

BI Process. SEPS initiates a background investigation based on the individual's position risk and sensitivity designation. The FDIC assigns a risk designation for all employee positions. For positions that require access to Classified National Security Information (CNSI), the FDIC assigns a sensitivity designation. Risk and sensitivity designations are specific to the duties and responsibilities of a position, and are not related to a particular individual. OMs are responsible for identifying the risk and sensitivity for contractor personnel based on contract labor categories or functions.[22] Accurate position risk designations are the foundation of an effective and consistent suitability and personnel security program.

To determine the appropriate risk designations, the FDIC adopted the Risk Designation System established by OPM. According to SEPS's *Personnel Security Guide for Employee Background Investigations*, the FDIC has three position risk and sensitivity designations:

- **Low Risk/Non-Sensitive Positions.** Positions that are neither Public Trust nor National Security Positions.
- **Public Trust Positions**. Public Trust Positions have the potential for affecting the integrity, efficiency, and effectiveness of the FDIC's mission, and when misused, may diminish public confidence in the Nation's banking system.

[21] The FDIC's goal is included in its contract with Global Resource Solutions, Inc. and is predicated upon conditions that are under the control of the contractor and there being no potentially disqualifying issues. Global Resources Solutions, Inc. supports SEPS with resources in conducting key background investigation-related activities.
[22] Contracts, Basic Ordering Agreements (BOA), Receivership BOAs (RBOA), Blanket Purchase Agreements (BPA) and task orders will no longer receive an overall risk category designation. In lieu of such designation, each contract, BOA, RBOA, or BPA will set forth separately designated risk levels for each established labor category. In the absence of labor categories, separately designated risk levels for each defined area of functional responsibility are identified on Form 1600/17, *Contract Risk Level Record* (Revised June 2019). Contractors working in multiple labor categories or functional areas must be designated based on the highest risk level.

- **National Security Positions**. Sensitive positions, designated as Non-Critical Sensitive or Critical Sensitive, and Special Sensitive in which the incumbent's duties and responsibilities involve access to classified national security information at the Confidential, Secret, Top Secret, or Secret Compartmented Information level, or other restricted information relating to the security of our nation.

These three position risk and sensitivity designations correlate with five investigative tier levels (Levels 1 through 5).[23] These tiers determine the type of investigation to be conducted by the DCSA. Tier 1 positions involve low-risk, non-sensitive, and non-national security program responsibilities. Public Trust positions require a higher degree of integrity in the individual occupying the position. The FDIC has determined that most of its positions are Public Trust positions and require Tier 2 or Tier 4 investigations depending on the position risk level determination. Table 2 defines the risk levels for Public Trust positions.

Table 2: Public Trust Risk Levels and Investigation Requirements

Risk Level	Minimum Investigation Required
Moderate Risk **These positions have the potential for moderate to serious impact involving duties of considerable importance to the FDIC or program mission with significant program responsibilities and delivery of customer services to the public.**	Tier 2
High Risk **These positions have the potential for exceptionally serious impact involving duties especially critical to the FDIC with broad scope of policy or program authority.**	Tier 4

Source: SEPS *Personnel Security Guide for Employee Background Investigations.*

National Security Positions are those in which the position duties require the regular use of, or access to, CNSI. Table 3 defines the sensitivity level and background investigation required for National Security Positions.

[23] The investigative tiers align with Federal Investigative Standards (FIS) called for by EO 13467. OPM and ODNI approved implementation of FIS in 2017.

Table 3: National Security Positions and Investigation Requirements

Access Level	Sensitivity Level	Minimum Investigation Required
Secret or Confidential	**Non-Critical Sensitive** These positions have the potential to cause damage to the national security, up to and including damage at the significant or serious level.	Tier 3
Top Secret – Sensitive Compartmented Information	**Critical-Sensitive or Special Sensitive** Critical Sensitive positions have the potential for exceptionally grave damage to the national security. Special Sensitive positions have the potential to cause inestimable damage to the national security.	Tier 5

Source: SEPS *Personnel Security Guide for Employee Background Investigations.*

Before ordering an investigation, SEPS checks the OPM's Central Verification System (CVS)[24] to determine whether reciprocity should be applied. SEPS determines whether any other Federal organization previously investigated the individual and the date and type of investigation, adjudication determination, and, if applicable, the clearance status. Federal guidance requires agencies to grant reciprocity unless one of the exceptions shown in the adjacent text box is apparent. If reciprocity is not applicable, SEPS initiates the appropriate level background investigation. The FDIC's goal is to submit BI requests to DCSA within 14 days of receiving completed forms from employees or contractor personnel.

Reciprocity Exceptions

1. The new position requires a higher level of investigation than previously conducted for that individual;
2. The gaining organization obtains new information that calls into question the individual's fitness based on character or conduct; or
3. The individual's investigative record shows conduct that is incompatible with the core duties of the new position.

Once DCSA completes the investigation, SEPs officials have 90 days to review associated reports of investigation and make a final adjudication determination. The final adjudicative process consists of a review of all relevant documentation and the

[24] CVS is designated as the primary tool for facilitating reciprocal decisions, as required by EOs, regulations, and policies. CVS contains information on security clearance, suitability, fitness, and Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) credentialing determinations.

completed background investigation. If SEPS identifies any potentially disqualifying issues, the individual will be sent a Letter of Issues (LOI) to obtain further information and/or related documentation. A final adjudicative determination results in either a favorable or unfavorable determination.[25]

All employees and contractor personnel except those in non-sensitive low-risk positions are subject to Government-wide reinvestigation requirements or PRs every 5 years.[26] Some individuals in sensitive positions are also subject to "continuous evaluation (CE)."[27] According to ODNI, "CE" is a personnel security investigative process that leverages automated record checks of commercial records, U.S. Government databases, and other information lawfully available to security officials, to continuously review the background of individuals who have been determined to be eligible for access to classified information or eligible to hold a sensitive position.

PSSP Records and Systems

During our evaluation, the FDIC was in the midst of transitioning the location where PSSP documents and data will be retained. In July 2018, more than 2 years ago, the FDIC deployed Enterprise Workforce Solution (eWorks), which is a web-based tool that automates the processes for "on-boarding" and "off-boarding" FDIC employees and contractor personnel. The FDIC's implementation of eWorks involved a phased approach. According to the OIG's Evaluation Report in 2014, SEPS planned to deploy eWorks in 2015. Because the implementation of eWorks took longer than expected, the FDIC remained dependent during the scope of our review on legacy systems, including Documentum (an FDIC-owned storage system),[28] CHRIS, and a SEPS SharePoint site[29] to manage processes and records. The FDIC also remained dependent on manual data entry to update data in CHRIS. However, DOA officials advised that on June 20, 2020, eWorks became the official system of record for SEPS-related records. DOA officials also stated that the FDIC continues to make enhancements to eWorks.

[25] According to OPM, if an unfavorable suitability determination is made, the following actions may be applicable: cancellation of eligibility; removal; cancellation of reinstatement eligibility; and debarment.
[26] Federal reinvestigation requirements were changed in June 2018, allowing for temporary deferment of the 5-year reinvestigation period pending the completion of minimum background and criminal history checks. The allowance for temporary deferments expired in June 2020.
[27] CE is a key component of security clearance reform efforts to modernize personnel security practices and increase the timeliness of information reviewed between periodic reinvestigation cycles.
[28] Documentum included scanned forms and case files for employees and contractor personnel.
[29] The SharePoint site includes spreadsheets used to track and assign cases within SEPS.

Prior Reviews of the PSSP

In addition to the OIG's Evaluation completed in 2014, we identified three other reviews of the FDIC's PSSP completed between April 2013 and June 2015. The following summarizes the relevant information from each of these reviews:

OPM Federal Investigative Services PSSP Review Report | April 2013

The OPM-Federal Investigative Services program evaluation confirmed that the FDIC was validating the need for an investigation through OPM's CVS.[30] However, this OPM review made several findings and recommendations for improvements at the FDIC, including the following:

- Calculating accurate annual investigation projections;
- Using the e-QIP system;
- Reporting adjudication determinations to OPM;
- Making timely adjudication decisions;
- Sharing CVS data monthly with OPM;
- Appropriately designating position risk and sensitivity; and
- Requesting correct investigations and reinvestigations.

The FDIC took action to address the OPM recommendations in 2013.

Personnel Security & Operations As-Is Process Analysis | July 2013

The FDIC engaged a contractor to assess the current state of its security processes and identify areas of improvements. The contractor's findings showed that:

> [T]he paper-based manual work flow process that results in slow processing times, lost and misplaced data and cases, slow management approval, and customer dissatisfaction. [PSSP Staff] used multiple systems operating in silos to input and withdraw data manually. All too often the staff had to manually stop operations and search for cases to address inquiries. In addition, OMs and others were unable to determine the status of their requests so they flooded the [unit] with calls and emails, which slow the process down even more.

[30] This is a suitability and security automation performance goal that OPM monitors and reports to the Performance Accountability Council established by EO 13467, dated June 30, 2008, *Reforming Processes Related to Suitability for Government Employees, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information.*

The contractor made five recommendations. The first two recommendations focused on digitizing records and instituting an electronic record system and a security and HR-web-based system. The other recommendations dealt with instituting the use of Electronic Questionnaire for Security Processing (eQIP) for contractors, mandating the use of digital fingerprints, and developing training and standard operating procedures. According to SEPS officials, all recommendations from the report have been implemented.

OIG's Evaluation of the FDIC's PSSP | August 2014

The objective of the OIG's evaluation was to determine whether the FDIC was carrying out its PSSP efficiently and effectively. The report included the following key findings:

Overall Program Administration. The OIG found that:

- Some PBIs and adjudication decisions were questionable and lacked support;
- Not all background investigations performed were commensurate with a position's risk level designation;
- Some background investigations were not timely; and
- Many investigation case files were missing key documentation.

Contract Oversight. Contract oversight could be strengthened by SEPS establishing better criteria for measuring contractor production and performance.

Records Management. Records management controls over the PSSP needed improvement. At that time, we observed that file rooms were overloaded and disorganized and contained boxes of unfiled BI documents. The report cautioned that digitizing and automating PSSP processes would not ensure or negate the need for strong, comprehensive records management controls in the PSSP's future environment.

Information System. Because SEPS manually input relevant data into the system, BI data were not reliable in the DOA systems used to capture preliminary clearance data and provide management reporting.

The OIG made 10 recommendations in this report to enhance the FDIC's PSSP. The FDIC determined that it had completed corrective action and closed the recommendations without any further review by the OIG.[31]

[31] As noted earlier, in 2014, the FDIC could close OIG recommendations without further review by the OIG of the corrective actions. The OIG has since revised its processes and now reviews all corrective actions to determine whether the FDIC's actions satisfy the recommendation and therefore can be considered as closed.

DOA's Management Services Branch PSSP Review | June 2015

The Management Services Branch within DOA initiated this review to determine whether SEPS had taken steps to improve the program administration activities to address issues raised in the OIG's Evaluation Report in 2014. This internal DOA report found that the FDIC had made improvements in case file documentation and OPM reporting. The DOA report, however, made five additional recommendations aimed at improving file review and documentation controls to ensure all key documents for PBIs existed and were filed appropriately; PBI decisions were appropriately approved; and key activities, issues, and milestones were uniformly captured to immediately ascertain the status of background investigations. DOA officials asserted that these recommendations had been addressed.

As noted in the Evaluation Results section of this current report, we identified similar weaknesses in the FDIC's PSSP to those previously noted in these four prior reviews.

EVALUATION RESULTS

We determined that the FDIC's PSSP was not fully effective in ensuring that preliminary suitability screenings were completed in a timely manner; background investigations were ordered and adjudicated commensurate with position risk designations; and reinvestigations were ordered within required timeframes. Specifically, through our analysis of PSSP-related data for all employees and contractor personnel with access to the FDIC's information technology systems as of December 2, 2019, (5,744 FDIC employees and 1,510 FDIC contractor personnel), we found that the FDIC did not:

- Remove multiple contractors with unfavorable adjudications in a timely manner;
- Sufficiently evaluate the contractors for insider threat risks when they were removed as a result of unfavorable adjudications;
- Initiate and order periodic reinvestigations of all contractors and employees in a timely manner;
- Order background investigations commensurate with position risk designations in some cases;[32]
- Maintain complete and accurate PBI records in some cases; and

[32] We were unable to assess whether background investigations ordered for contractors were commensurate with position risk designations because we determined that contractor risk designation information in CHRIS was unreliable.

- Achieve established goals for completing PBIs in a timely manner.

We also found that the FDIC adhered to its reciprocity guidelines.

In 2018, the FDIC began working to implement process changes, including implementing a business process management system and addressing data quality issues. The FDIC also increased SEPS staffing. However, some of the process changes, including the implementation of the business process management system, were envisioned in 2014, more than 6 years ago. In addition, some issues we identified in this present report (2021) were similar to those identified in several prior reports, including our OIG evaluation of the FDIC's PSSP in 2014. Specifically, a number of issues—timeliness of PBIs; missing documentation; BIs not being consistent with position risk; and the reliability of PSSP-related data—were identified previously by the OIG, but still do not appear to be corrected.

While "Security – Personnel and Physical" is among the risk areas identified as part of the FDIC's Enterprise Risk Management (ERM) Program, the results of our evaluation led us to conclude that the risks within the FDIC's PSSP were not fully reflected in the FDIC's Risk Inventory, which informs the FDIC's Risk Profile. The FDIC validated its Risk Inventory in July 2020, [redacted] In our view, DOA's risk assessment did not fully reflect the operational, compliance, reporting, and reputational risk presented in our Evaluation Results. Further, while DOA considers eWorks to be a significant mitigating factor, it was unclear how ongoing data validation efforts and other planned system enhancements were factored into the assessment of risk. Although the minutes from the meeting of the Operating Committee in August 2020 reflect consideration and discussion about the FDIC's Risk Profile, there was no indication that the risks associated with the PSSP had been discussed.

According to DOA, the FDIC is preparing for potential surge hiring in the event the uncertain economic conditions due to the pandemic cause an increase in the FDIC's workload.[33] The FDIC may be required to increase hiring to ensure readiness for any potential increase in supervisory workload, bank failure activity, and administrative support. In December 2020, the FDIC Board approved an increase in the agency's Operating Budget of $261 million (12.9 percent). This expansion was largely due to the establishment of contingency reserves in order to address "a potential increase during 2021 in supervision or resolution workload resulting from the ongoing pandemic."

[33] Many banking and economic experts have predicted the potential for an increase in bank failures due to the economic impacts resulting from the pandemic. Congressional Research Service, *COVID-19 and the Banking Industry: Risks and Policy Responses* (June 18, 2020); USA Today, *Two Small banks failed in October. They won't be the last if COVID leaves some businesses struggling to pay loans.* (November 20, 2020); International Banker*, Is COVID-19 About To Trigger a 2008-Style Banking Collapse?* (October 12, 2020).

The contingency reserve could be used to add a significant amount of new personnel at the FDIC, both employees and contractors. For example, the reserve would be "sufficient to add an estimated 280 additional temporary employees and substantially increase contractual resources in [the Division of Resolutions and Receiverships]." In addition, the FDIC Budget for 2021 includes:

- $39.6 million for overhiring in [the Division of Risk Management Supervision] to ensure readiness to address any potential increase in supervisory workload, including an estimated 275 risk management examiners in excess of the Division of Risk Management Supervision's 2021 examiner staffing authorization; and
- $11.1 million for targeted overhiring in other divisions, including 24 additional full-time equivalent positions (FTE) in DOA to enhance readiness to address projected temporary workload.
- $11.9 million to fill existing vacancies as well as 43 new authorized positions to address skill gaps in the Division of Complex Institution Supervision and Resolution.

A significant hiring surge will increase the number of suitability screenings and background investigations processed through the PSSP. Therefore, FDIC leadership must be assured that the PSSP has both the resources and the controls needed to ensure all new employees and contractors are properly screened and investigated without compromising efforts to complete PRs for those already working for or performing services on behalf of the FDIC.

The FDIC Has Not Fully Recognized the Level of Risk Within Its Personnel Security and Suitability Program

ERM is a way to anticipate, prioritize, and manage risks across an agency. At the FDIC, the ERM program aims to address the full spectrum of significant internal and external risks facing the Agency and the combined impact of those risks as an interrelated portfolio. According to FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program* (ERM Directive), each Division/Office identifies its key activities and determines what risks may threaten its or the FDIC's ability to achieve success. The Directive states that based on the criticality of each activity and the perceived impact and likelihood of risks, management takes actions to address the risks, including escalation of the risks up the chain of command and/or to the appropriate committees. The FDIC's Operating Committee serves as its Risk Management Council tasked with overseeing the establishment of the Agency's Risk Profile, regular assessment of risk, and development of appropriate risk response. The FDIC's Chief Risk Officer is charged with maintaining the FDIC's ERM components, such as the Risk Appetite Statement, Risk Inventory, and Risk Profile.

The FDIC issued its Risk Appetite Statement in May 2019. The Risk Appetite Statement communicates the FDIC's views about the level of risk taking that is acceptable in pursuit of its strategic goals and objectives. According to its Risk Appetite Statement, the FDIC has a "very low" appetite for risks that could threaten its ability to protect the safety and security of its personnel and facilities and identify and prevent insider threats.[34] The FDIC also has a "very low" appetite for risks that threaten the FDIC's ability to comply with a required law or regulation. The FDIC's designation of "very low" indicates areas in which the FDIC seeks to avoid, minimize, or eliminate risks, because the potential downside costs are intolerable.

The FDIC's Risk Inventory is a detailed list of risks that could affect the FDIC's ability to meet its strategic objectives.[35] Senior officials within Divisions/Offices retain first-line responsibility and ownership for risk identification, assessment, escalation, management, monitoring, and mitigation. The Risk Inventory includes an assessment of risk impact and likelihood, and is prioritized and summarized into the FDIC's Risk Profile. The Risk Profile is a prioritized inventory of "the most significant" risks facing the FDIC. The primary purpose of a Risk Profile is to provide analysis of the risks that might interfere with an agency's ability to achieve its strategic objectives. The adjacent text box highlights how risk associated with the PSSP is factored into the FDIC's Risk Inventory and Risk Profile.

Risk Inventory

Security – Personnel and Physical Risk [redacted]

[redacted]

The risk, along with other related risks, are integrated into the FDIC's Risk Profile.

Risk Profile

Physical Security and Employee Health [redacted]

[redacted]

Source: FDIC Risk Inventory and Risk Profile [September 2020].

[34] See FDIC Risk Appetite Statement.
[35] As of September 8, 2020, the FDIC maintained 99 individual risks within its Risk Inventory.

According to the *ERM Standard Operating Procedure* (SOP) (May 2020), the FDIC identifies risks through Division/Office risk assessments, audits and evaluations conducted by the OIG and GAO, the FDIC's risk committees, and the Office of Risk Management and Internal Controls (ORMIC)[36] research and risk assessments. The FDIC's Divisions and Offices updated their Risk Inventory items throughout the year and validated them on July 1, 2020. Based on the validated Risk Inventory, ORMIC officials also updated the Risk Profile in coordination with the FDIC's Divisions and Offices.

DOA officials stated that they had reviewed the "Security – Personnel and Physical" risk within the FDIC's Risk Inventory in July 2020 and [redacted][38] In drawing this conclusion, DOA documented existing controls and mitigations for personnel suitability to include Federal adjudication guidelines; experienced FDIC staff and contractors; and a system for managing background investigations (eWorks). As a result, as of September 14, 2020, the FDIC considered this risk related to the PSSP [redacted][39]

However, we determined that DOA's risk assessment and the assigned risk rating did not fully reflect the risks associated with the PSSP that we observed during this evaluation. Specifically, although the FDIC considered its centralized system for managing background investigations to be a mitigating factor for this risk, eWorks had not become the official system for SEPS-related records until June 2020 and SEPS officials informed us that they were still enhancing eWorks to help monitor the program on a go-forward basis. Further, the FDIC had not completed other necessary process improvements, including data correction, position risk reviews, and case file migration.

[36] On December 15, 2020, the Deputy to the Chairman and Chief Financial Officer announced an orgranizational change. Effective January 1, 2021, the Risk Management and Internal Controls Branch within the Division of Finance was reorganized and elevated to a separate, independent office known as ORMIC.
[37] According to the FDIC's ERM SOP, an unlikely risk event is one that has a 25 percent or less chance of occurring within 3 years. A risk event that has between a 26 percent and 50 percent chance of occurring within the next 3 years is considered possible. A risk event that has occurred in the last 24 months or has between a 51 percent and 75 percent chance of occurring within the next 3 years is likely, and a risk event that has occurred within the last 12 months or has a greater than 75 percent chance of occurring in the next 3 years is considered probable.
[38] Moderate impacts include those that could moderately affect the FDIC's ability to achieve its mission or strategic goals, or could result in breaches of legal, regulatory, or contractual obligations that are confined to isolated incidents. Significant impacts include those that could significantly affect the FDIC's ability to achieve its mission or strategic goals, or could result in regular breaches of legal, regulatory, or contractual obligations. Critical impacts are those that could preclude or highly affect the FDIC's ability to achieve its mission or strategic goals and objectives, or could result in continuous breaches of legal, regulatory, or contractual obligations.
[39] [redacted].

Based on the findings of this report, we do not believe that DOA's risk assessment fully considered the various risks identified in our Evaluation Results. For example, in February 2020 and March 2020 (prior to the update of the Risk Inventory and Risk Profile), we informed the FDIC of our findings regarding four contractor personnel with unfavorable adjudications that remained on board for periods ranging from nearly 8 months to almost 5 years after the FDIC made the unfavorable adjudication determinations. This presents a breakdown of existing controls that should have been reflected within the FDIC's risk assessment.[40] Further, three of these four contractor personnel held High-Risk positions, including two IT administrators and an armed security guard. At the time of the Risk Profile update (July 2020), the FDIC (including DOA personnel) was also aware of documentation, record keeping, and data quality issues in its PSSP as well as its non-compliance with reinvestigation requirements, which should have impacted the risk assessment.

As discussed in detail below, we also found that:

- Another seven contractor personnel worked at the FDIC for periods ranging from 83 days to 421 days before receiving unfavorable adjudications.[41] Upon adjudicating these individuals as unfavorable, the FDIC took between 3 days and 118 days to execute the removal actions.
- SEPS did not refer any of the contractor personnel with unfavorable adjudications to the Insider Threat and Counterintelligence Program (ITCIP) Program Manager for further evaluation of the insider threat risk they posed to the FDIC.
- In four cases, FDIC employees did not receive BIs at a sufficiently high level commensurate with their position risk level. Three of these employees operated in High-Risk Public Trust Positions with another operating in a Special Sensitive National Security Position.

SEPS officials stated that they considered the implementation of eWorks, including its automated interfaces with CHRIS and its enhanced monitoring capabilities as a significant factor in both mitigating the risks highlighted within this report and in support of their risk determination. However, we do not agree with this proposition. As discussed above, eWorks had not become the official system for SEPS-related records until June 2020 and SEPS informed us that it was still enhancing eWorks to help it monitor the program on a go-forward basis. Further, the FDIC had not completed other necessary process improvements, including data correction, position risk reviews, and case file migration.

[40] These events should have been factored in the FDIC's likelihood rating for the Security – Personnel and Physical risk.
[41] This was allowable since the FDIC cleared these individuals during the PBI process before coming on board. Nevertheless, these situations create risk – particularly for contractor personnel in certain High-Risk positions.

According to the ERM Directive, if risks are not effectively identified, assessed, and addressed, such failure could negatively affect the FDIC's ability to achieve its goals and objectives. Risk management practices must be forward-looking and designed to help leaders make better decisions, alleviate threats, and identify previously unknown opportunities to improve government operations. The FDIC should ensure that its risk assessments fully reflect the likelihood, impact, and mitigations for existing risks. This acknowledgement will ensure transparency to senior leadership in the FDIC's ERM program as they assess and evaluate the risks for the entire enterprise and formulate appropriate mitigation approaches.

In August 2020, the Operating Committee affirmed the updated Risk Profile. In approving the Risk Profile, the Operating Committee confirmed that the "Physical Security and Employee Health" risk, which integrates the risks associated with the PSSP, [redacted] based on the underlying risks. According to ORMIC's Risk Profile analysis, three underlying risks from the Risk Inventory, including the "Physical Security and Employee Health risk," [redacted] and one underlying risk from Risk Inventory entitled "Health and Safety" was [redacted] (due to the recent COVID-19 pandemic). However, based upon the minutes from this Operating Committee meeting, there was no indication that the "Physical Security and Employee Health" risk was discussed or that its associated rating was evaluated by the Operating Committee. According to the meeting minutes, the FDIC Chief of Staff reiterated the importance for Divisions and Offices to accurately reflect residual risk on their ERM responses. Had the FDIC's Operating Committee given full consideration to the risks associated with the Agency's PSSP and questioned the "Security – Personnel and Physical" risk rating, the FDIC may have adjusted the overall "Physical Security and Employee Health" risk to a higher level.

As reflected in our recent report on the FDIC's Implementation of Enterprise Risk Management,[42] having the Operating Committee, as the FDIC's designated Risk Management Council for ERM, make the final determinations of the approaches and actions to address risks included in FDIC's Risk Profile helps to ensure that risks that have significant impact on the mission outcomes of the Agency and the banking sector are addressed. This designation also ensures mitigation strategies are prioritized and overseen at the enterprise level. As stated in the FDIC's ERM SOP, through adequate risk management, the FDIC can concentrate its efforts towards key points of failure and reduce or eliminate the potential for disruptive events.

Recommendations

We recommend that the Deputy to the Chairman and Chief Operating Officer:

[42] OIG Report, *The FDIC's Implementation of Enterprise Risk Management* (EVAL-20-005) (July 2020).

1. Coordinate with the Chief Risk Officer and review the Risk Assessment associated with the "Security - Personnel and Physical" risk to ensure it fully reflects all risks, known weaknesses within the program, and the findings communicated in this report.

2. Communicate the results of the updated Risk Assessment to the Operating Committee and update the FDIC's Risk Profile as necessary.

Removal of FDIC Contractor Personnel with Unfavorable Adjudications Delayed

The FDIC continues to increase the Agency's reliance on outside contractor personnel. The FDIC devoted more than 16 percent of its annual budget for 2020 to contracted services personnel -- $308 million out of its total budget of $1.9 billion. This figure in the FDIC's budget for 2020 represents a 19-percent increase over the amount for contract services in the FDIC's previous budget in 2019.

The FDIC's PSSP Contractor Directive 1610.2 governs security requirements for contractor personnel. According to this Directive, contractor personnel may begin work at the FDIC after meeting PBI requirements. The FDIC considers the results of the PBI to be an "interim" suitability determination until a BI is completed and adjudicated by the FDIC. Contractor personnel who meet PBI requirements may subsequently receive an unfavorable BI adjudication because of the differing criteria and depth of review.

SEPS makes suitability adjudication decisions by assessing a contractor's background investigation report and information against OPM criteria found in 5 C.F.R. § 731.202. That criteria includes, for example, an assessment of misconduct or negligence in employment, criminal or dishonest conduct, and abuse of alcohol or illegal drug use. The FDIC has 90 days[43] after receiving a BI report from DCSA to make a final adjudication of the contractor's suitability for employment with the FDIC.

When SEPS adjudicates a contractor to be unfavorable for employment, SEPS must notify the responsible OM in writing by email. The OM then notifies the contractor's Program Manager and initiates the FDIC's Pre-Exit Clearance Process to remove the contractor.[44] OMs must initiate the FDIC's Pre-Exit Clearance Process to remove a contractor who has access to the FDIC's network, facilities, sensitive information, or has had a background investigation completed by SEPS. The Pre-Exit Clearance

[43] 5 C.F.R. § 731.203(g).
[44] The Pre-Exit Clearance Process is outlined in the *FDIC's Acquisition Procedures, Guidance and Information* guide and the *FDIC Pre-Exit Clearance Procedures.*

Process and Division of Information Technology (DIT) internal procedures[45] require that the contractor return all FDIC property, including Personal Identity Verification (PIV) cards and laptops; provides 18 hours for DOA to disable building access and DIT 24 hours to disable systems access; and requires that the OM account for the location of all records and information in the contractor's possession.

The FDIC Failed to Remove Four Contractor Personnel After Unfavorable Adjudications

In February and March 2020, we identified four contractors—from our total evaluation population of 1,510 contractor personnel—who had received an unfavorable adjudication and were still working on behalf of the FDIC. We immediately notified the FDIC of these cases.[46] These contractors had worked on behalf of the FDIC for periods ranging from nearly 8 months (232 days) to nearly 5 years (1,715 days) after the FDIC had already made its unfavorable adjudication determinations. When we raised this issue with SEPS in February and March 2020, SEPS stated that it was unaware that these contractors continued to work at the FDIC after their unfavorable adjudication dates. The FDIC removed these contractors shortly after we notified FDIC officials that these contractors continued to provide services to the FDIC. The FDIC processes an average of 20 unfavorable adjudications for contractors per year.[47] Table 4 summarizes information about the four contractors, including their risk level and the amount of time they worked at the FDIC.

Table 4: Contractors with Unfavorable Adjudications Removed Based on OIG Evaluation Results

Contractor	Division/Position	Risk Level	Days Before Unfavorable Adjudication*	Days After Unfavorable Adjudication**	Total Days	Month & Year of Adjudication
1	DIT - Systems Administrator [redacted]	High	346	1,715	2,061	[redacted] 2015
2	DIT - Systems Administrator [redacted]	High	808	766	1,574	[redacted] 2018
3	DOA - Armed Guard	High	132	232	364	[redacted] 2019
4	DRR - [redacted]	Moderate	436	274	710	[redacted] 2019

Source: OIG analysis of SEPS-related documentation and data.

* Days before unfavorable adjudication includes time required for OPM (now DCSA) to complete a background investigation.

**For our analysis, we considered the contractor's termination to be the later of physical removal, disabling of building access, or disabling of systems access. The FDIC faces risk from these contractors until all access is removed.

[45] FDIC, *Operational Security Framework*, Version 7.0 (July 23, 2020).

[46] We identified these contractors by reviewing all 1,510 contractors working for the FDIC as of December 2, 2019. See Appendix 1 – Objective, Scope and Methodology.

[47] This average is based on SEPS contractor unfavorable adjudications between the years 2015 and 2019.

In total, the period of time these contractor personnel worked at the FDIC ranged from 364 days (nearly 1 year) to 2,061 days (more than 5-1/2 years). These contractors included two high-risk level[48] DIT Systems Administrators,[49] a high-risk level armed security guard, and a moderate-risk[50] level [redacted] contractor.

One Systems Administrator [redacted] was adjudicated to be unfavorable because of an interim security clearance revocation as a result of a classified Federal Bureau of Investigation (FBI) report and dishonesty. The other Systems Administrator [redacted] was adjudicated to be unfavorable for causing a major IT incident at a prior employer that involved the compromise of Personally Identifiable Information (PII).[53]

The armed security guard [redacted] was adjudicated to be unfavorable for failing to disclose mental health consultation, misconduct at a prior employer, and dishonesty. Finally, the [redacted] contractor [redacted] and was found to be unfavorable for falsifying hours and dishonesty concerning a separation from a prior employer.

We determined that these contractors were not removed for two primary reasons. First, SEPS had not established a control to detect whether individuals with unfavorable adjudications remained employed at the FDIC. Such a control would allow SEPS to ensure appropriate action was taken to remove these individuals. Second, existing process steps to remove contractors were not executed by SEPS and OM personnel. Specifically:

[48] FDIC Directive 1610.2 defines high-risk positions as those reflecting the potential for exceptionally serious impact to the mission, integrity, or efficiency of the FDIC.
[49] According to the FDIC's *Policy on Administrator Account Naming and Password Length*, Administrator accounts have "elevated access rights to resources such as operating systems, network devices, databases, and applications to perform IT functions such as controlling, monitoring, and maintaining applications and systems."
[50] FDIC Directive 1610.2 defines a moderate risk positons as reflecting the potential for moderate to serious impact to the mission, integrity, or efficiency of the FDIC.
[51] [redacted]
[52] [redacted]
[53] PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

- In three instances, SEPS officials did not notify the responsible OM of the contractors' unfavorable adjudication. As a result, the OM could not notify the Contracting Officer to remove the contractor or initiate the Pre-Exit Clearance Process to remove the contractor's building and systems access. SEPS relied on its contracted staff to send unfavorable adjudication notices to OMs and did not monitor the contractor staff to ensure that the notices were sent.
- In one instance, the transition from one OM to another OM resulted in a miscommunication with each OM believing the other had informed the Contracting Officer and initiated the Pre-Exit Clearance Process.

The FDIC Did Not TImely Remove Seven Other Contractor Personnel with Unfavorable Adjudications

In February and March 2020, we identified another seven contractor personnel with access to FDIC systems that SEPS adjudicated to be unfavorable during our evaluation fieldwork. The FDIC removed these contractors but did not execute notification and removal procedures in a timely manner. The FDIC took from 3 days to 118 days to execute these removal actions. Table 5 summarizes information about each of these contractors, including their risk level and our analysis of the contractor's time with the FDIC.

Table 5: Delays in Removal of Seven Contractors with Unfavorable Adjudications[54]

Contractor	Division/Position	Risk Level	Days Before Unfavorable Adjudication*	Days After Unfavorable Adjudication**	Total Days	Month & Year of Adjudication
1	DIT- Systems Administrator [redacted]	High	418	3	421	[redacted] 2020
2	DIT- Systems Administrator [redacted]	High	306	41	347	[redacted] 2019
3	DIT- Systems Administrator [redacted]	High	207	49	256	[redacted] 2019
4	DOA - Armed Guard	High	307	21	328	[redacted] 2019
5	DOA - Armed Guard	High	244	77	321	[redacted] 2020
6	DOA - Armed Guard	High	219	118	337	[redacted] 2019
7	DOA - Cafeteria Services	Moderate	79	4	83	[redacted] 2019

Source: OIG analysis of SEPS-related documentation and data.
* Days before unfavorable adjudication includes time required for OPM (now DCSA) to complete a background investigation.
**For our analysis, we considered the contractor's termination to be the later of physical removal, disabling of building access, or disabling of systems access. The FDIC faces risk from these contractors until all access is removed.

These contractors included three high-risk level DIT Systems Administrators, three high-risk level armed guards, and one moderate-risk level cafeteria employee. These contractors were found to be unfavorable for reasons including: illegal drug

[54] An additional unfavorable contractor working at the FDIC on December 2, 2019 departed the FDIC after a BI was completed but before the FDIC rendered its unfavorable adjudication.

use, omitting terminations from prior employment, falsification of time records, and performance issues.

The circumstances associated with the removal of these contractors included:

- In one instance, SEPS did not notify the OM of the contractor's unfavorable adjudication timely, causing removal action to be delayed by 41 days.
- In three instances, the OM did not initiate removal action timely under the FDIC's Pre-Exit Clearance Process, causing delays of 3 days, 4 days, and 77 days, respectively.
- In one instance, the OM completed some of the Pre-Exit Clearance processes but took 21 days to initiate disabling the contractor's IT access.
- In two instances, the PSG did not deactivate the contractor's PIV Card for 49 and 118 days, respectively.

The FDIC's procedures do not establish timeframes for SEPS to notify an OM of a contractor's unfavorable adjudication. As a result, these individuals were allowed to continue working in the FDIC facilities, with access to the FDIC's systems and personnel, and in some cases, for extended periods of time.

Also, there were no established timeframes for an OM to notify the Contracting Officer of a contractor's unfavorable adjudication or for the OM to initiate the Pre-Exit Clearance process. Further, the FDIC did not have mechanisms in place to monitor the background adjudications for these individuals, in order to ensure the execution of all process steps to remove unfavorable contractors in a timely manner. Given the risk posed to the FDIC by unfavorable contractors, SEPS and OM personnel should take immediate action to remove individuals with unfavorable adjudications.[55]

Similar weaknesses were identified in previous OIG reports:

- In our OIG evaluation report, *The FDIC's Personnel Security and Suitability Program* (August 2014),[56] we concluded that policies and procedures in key control, process, and reporting areas were not in place, well understood, nor consistently practiced by federal or contractor employees. We recommended that DOA establish and implement standard operating procedures for SEPS personnel. SEPS did update its procedures, but the updated procedures did not establish timeframes for SEPS to notify OMs or include monitoring processes to ensure that OMs removed contractor personnel who had unfavorable adjudication determinations.

[55] See, for example, the Pension Benefit Guaranty Corporation Personnel Security and Suitability Program, Directive PM 05-17, requiring that its security group directly contact the contractor's employer for immediate removal upon an unfavorable adjudication.
[56] OIG Report, *The FDIC's Personnel Security and Suitability Program* (EVAL-14-003) (August 2014).

- In our OIG report, *Controls over Separating Personnel's Access to Sensitive Information* (September 2017),[57] we identified the need to monitor OMs' responsibilities for contractors' Pre-Exit Clearance Process. We found that for our random sample of 48 cases, 90 percent (43 of 48) of OMs were not able to provide pre-exit clearance forms for departing contractors.[58] We recommended that the FDIC designate a Pre-Exit Clearance Process owner who would be accountable for the FDIC's pre-exit clearance program.

  In response to our recommendation, the then-Director, DOA,[59] was identified as the process owner and it was represented that this individual "would personally remain accountable for the pre-exit clearance process to centralize oversight and demonstrate the Agency's commitment to this important business process." However, as discussed above, Pre-Exit Clearance oversight processes failed to identify that OMs did not take action to remove unfavorable contractors.

- In our OIG report, *Contract Oversight Management* (October 2019),[60] we found that OMs within DIT had workloads that were 67 percent higher than another FDIC Division with similar-sized contract portfolios. These workloads reduce the capacity of DIT OMs to effectively oversee contractors. We recommended that DIT determine the appropriate number of OMs needed to oversee DIT contractors' workloads and ensure appropriate staffing. DIT contractors accounted for nearly half of the 11 contractors with unfavorable adjudications who were not removed timely.

Delays in removing unfavorable contractor personnel put FDIC information, systems, personnel, and facilities at risk. As discussed above, some of these contractors had access to sensitive FDIC information, including bank closing and supervisory information and the PII of FDIC employees, contractors, visitors, and parties to receivership loans. Specifically:

[57] OIG Report, *Controls over Separating Personnel's Access to Sensitive Information* (EVAL-17-007) (September 2017).
[58] A total of 763 employees and 587 contactors separated from the FDIC during the scope period of the evaluation October 1, 2015 through September 30, 2016. We used random sampling to obtain a sample population of 49 employees and 48 contractors. Our sampling methodology employed a 90-percent confidence interval, 5-percent desired precision level, and 5-percent expected incidence (error) rate.
[59] In September 2018, the FDIC Chairman eliminated this position and transitioned the day-to-day management and supervision of DOA to the Deputy to the Chairman and Chief Operating Officer.
[60] OIG Report, *Contract Oversight Management* (EVAL-20-001) (October 2019).

- Five contractors had Systems Administrator accounts that posed significant risk to the Agency given their elevated privileges. These contractors had the potential to imbed malware or inappropriately remove sensitive information or PII. Such actions could severely impact the mission, integrity, or efficiency of the FDIC and harm FDIC personnel, contractors, and parties to receivership loans. The potential for harm is especially acute when contractors are informed of their removal, but their systems and building access remain active.
- Ten contractors had access to FDIC facilities. These included four armed security guards who worked at the FDIC's Virginia Square facility and had interactions with nearly 1,500 FDIC employees and contractors assigned to that facility as well as visitors to the Virginia Square daycare center, student residence, corporate training center, and cafeteria.

Examples from other agencies demonstrate that the actions of one contractor can cause significant harm to an organization and its personnel. For example, in 2018, a Government contractor was sentenced for inserting malicious code known as a "logic bomb" into the US Army reserve's pay and personnel action system.[61] That event cost the military about $2.6 million to fix the damage.[62]

Our findings also highlight the risk of the FDIC's policy to allow contractors to begin working at the FDIC before completion of the BI adjudication process. This policy allows contractors to have access to FDIC systems and facilities for long periods of time before the FDIC makes an adjudication decision. SEPS officials informed us that this allows the FDIC to on-board staff more quickly and this practice is followed by other agencies. Further, DCSA is working to reduce processing times for completing BIs thereby reducing the period of risk to the FDIC. Nonetheless, as shown in Tables 4 and 5 above, contractors worked at the FDIC for periods of more than 2-1/2 months (79 days) to over 2 years (808 days) before the FDIC made its unfavorable adjudication decision. In our view, the positions these contractors occupied created significant risk to the FDIC. As such, the FDIC should evaluate whether its policy to allow contractors in certain high-risk positions, such as Systems Administrators and armed Security Guards, to work at the FDIC before being favorably adjudicated continues to be an acceptable risk.

The number of FDIC adjudications will likely grow with the FDIC's increasing budget for contractor services. As mentioned previously, $308 million (more than 16 percent) of the FDIC's total budget of $1.9 billion for 2020 was for contracted services personnel, which represents a 19-percent increase over the previous budget in 2019.

[61] Georgia Man Sentenced for Compromising U.S. Army Computer Program, U.S. Attorney's Office, Eastern District of North Carolina, U.S. Department of Justice (September 11, 2018).
[62] Atlanta Man Ordered to Pay $1.5M for Putting "logic bomb" in Army Computer, The Atlanta Journal-Constitution (September 21, 2018).

Further, in the event of a crisis, the FDIC may need to quickly employ contractor personnel. For example, according to an FDIC internal study, during the 2008-2011 period of the financial crisis, the FDIC awarded over 6,000 contracts totaling nearly $8 billion. The FDIC must take action to strengthen controls surrounding the timely removal of personnel adjudicated to be unfavorable for FDIC employment.

Recommendations

We recommend that the Deputy to the Chairman and Chief Operating Officer:

3. Formally define key process steps for removing contractors SEPS adjudicated to be unfavorable and establish timeframes for executing those process steps.

4. Provide training to program offices officials with responsibilities under the PSSP on process steps and timeframes for removal action of contractors SEPS adjudicates to be unfavorable.

5. Monitor and confirm that contractors adjudicated unfavorably are removed within established timeframes.

6. Evaluate and document the Risk Assessment of completing Background Investigations for contractor personnel in high-risk positions before they begin work at the FDIC.

The FDIC Conducted Limited Risk Assessments for Insider Threats

In September 2016, FDIC Directive 1600.7, *FDIC Insider Threat and Counterintelligence Program* (ITCIP Directive),[63] established an Insider Threat and Counterintelligence Program intended to detect and mitigate risks and vulnerabilities to the FDIC's operational mission, personnel, assets, and facilities. The ITCIP Directive states that all FDIC personnel have a responsibility to report activities that pose risks to the FDIC's mission or assets. According to the ITCIP Information Sharing Protocols,[64] the ITCIP Program Office "expects to receive information to support insider threat and counterintelligence assessments." This information should include personnel departures and separations, and any adverse actions. Specific referrals should be made to the ITCIP Program Office for "adverse findings in

[63] The FDIC defines an insider threat as a **"**threat posed to the FDIC or U.S. national security by someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to any USG [United States Government] resource. This threat can include damage through espionage, terrorism, sabotage, unauthorized disclosure of classified information or unclassified sensitive information, or through the loss or degradation of FDIC resources or capabilities."
[64] ITCIP Information Sharing Protocols (November 21, 2019).

background investigations and post-appointment background concerns."[65] SEPS internal procedures[66] also state that in instances where Personnel Security Specialists detect potential areas of concern or insider threat indicators, such information shall be referred to the ITCIP for further review.

The FDIC also uses a Data Loss Prevention (DLP) tool to assess potential information breach activities for departing contractors. The DLP tool monitors the movement of FDIC information to identify potential information breaches. 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 for each Division and Office.

When the DLP identifies activity that meets established criteria, an event is created in the DLP activity log. According to the FDIC's *Data Loss Prevention Concept of Operations*, the DLP tool monitors all FDIC user activities 24 hours a day and 7 days a week. When a contractor departs the FDIC, DIT reviews the DLP log for any incidents associated with the contractor for a 30-day lookback period beginning on the date the OM requested removal of the contractor's IT access.

SEPS did not refer any of the 11 contractor personnel removed for unfavorable adjudications to the ITCIP Program Manager. According to SEPS personnel, they do not refer unfavorable adjudications to the ITCIP, because most unfavorable adjudications stem from financial issues, which SEPS personnel believed were not pertinent to the ITCIP program. However, the ITCIP Directive and protocols state that all unfavorable adjudications should be reported and that financial matters are key indicators of motivation to become an insider threat. A contractor's poor financial situation or desire for luxury items may lead to a need for additional income that could be obtained through the sale of sensitive information.

The ITCIP Program Manager was not provided the opportunity to assess any damage that could have been inflicted by these contractors on the FDIC. Further, the ITCIP Manager could not assess whether unfavorable contractors used their positions to influence or recruit FDIC employees or contractors. The ITCIP Program Manager also missed an opportunity to analyze whether there were any patterns contributing to the FDIC's hiring of unfavorable contractors, such as flawed business practices, ineffective communication, policy gaps, and insufficient training, which could lead to recommendations to change FDIC processes.

Following our notification to SEPS about the failure to remove contractors with unfavorable adjudications, DIT personnel stated that they conducted DLP assessments for potential data breaches for the five DIT contractors with unfavorable

[65] Insider Threat and Counterintelligence Program Management Office, Trigger Submission Cover Sheet.
[66] The FDIC's *Personnel Security Guide for FDIC Employee Background Investigations*.

adjudications, including the two Systems Administrators. According to DIT, the DLP analysis reviewed potential breach activity for a 30-day period beginning on the date the OM requested removal of the contractors' IT access. DIT officials stated that no breach issues were found for the five DIT contractors during that 30-day period. However, the five DIT contractors worked at the FDIC for periods from 256 days (over 8 months) and up to 2,061 days (more than 5-1/2 years) — significantly longer than the 30-day DLP review period. DIT officials told us that they could review DLP events as far back as 2 years, but were not required to do so per FDIC policies.

An insider threat review and an extended DLP breach review period would provide greater assurance that the risks posed by the 11 contractors with unfavorable adjudications were identified and mitigated. Further, these contractors had standard and privileged Systems Administrator access to FDIC systems, data, and sensitive information as well as access to FDIC facilities. Consequently, the contractors had the potential to inappropriately remove sensitive information or PII, harm FDIC personnel, contractors, and visitors, and otherwise seriously impact the mission, integrity, or efficiency of the FDIC. For example, unfavorable contractors included armed security guards and individuals with privileged systems access who built and configured FDIC servers and wireless operations for bank closings.

In two prior reports, we recommended the FDIC's expanded use and refinement of the DLP tool. In our OIG report, The FDIC's Process for Identifying and Reporting Major Security Incidents (July 2016),[67] 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, and resources committed to reviewing the events. In our OIG report, Controls over Separating Personnel's Access to Sensitive Information (September 2017),[68] we recommended that the FDIC's Chief Information Officer establish appropriate policy for using DLP to support the FDIC's Pre-Exit Clearance Process. The FDIC amended its Pre-Exit Clearance policy to require use of the DLP tool for separations, including referral of potential incidents or data breaches. The amendment, however, did not address the period of the DLP review.

In our *OIG Special Inquiry Report* (April 2018),[69] we described eight insider incidents experienced by the FDIC as departing employees improperly took sensitive information shortly before leaving the FDIC. Seven incidents involved PII, including Social Security Numbers, and thus constituted data breaches.

[67] OIG Report, *The FDIC's Process for Indentifying and Reporting Major Information Security Incidents* (AUD-16-004) (July 2016).
[68] OIG Report, *Controls over Separating Personnel's Access to Sensitive Information* (EVAL-17-007) (September 2017).
[69] OIG Special Inquiry Report, *The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches* (OIG-18-001) (April 2018).

Recommendations

We recommend that the Deputy to the Chairman and Chief Operating Officer:

7. Update policies and procedures to ensure all individuals with unfavorable adjudications are referred to the ITCIP Program Manager to ensure full consideration of insider threat risks.

We recommend that the Deputy to the Chairman and Chief Operating Officer and Chief Information Officer:

8. Establish procedures that require the scope and duration of the DLP review process to correspond with the risk associated with the individual being removed due to an unfavorable adjudication.

The FDIC Did Not Initiate and Order Required Periodic Reinvestigations

FDIC employees and contractor personnel in Public Trust and National Security Positions are subject to Periodic Reinvestigation (PR) requirements. Table 6 captures the PR requirements for these positions.

Table 6: Reinvestigation Requirements for Public Trust and National Security Positions

Tier	Type of Position	PR Requirement for Continued Employment*
Tier 1	Non-Sensitive Positions	No PR
Tier 2	Public Trust Positions	Once every 5 years
Tier 4		Once every 5 years
Tier 3	National Security Positions	Once every 5 years
Tier 5		Once every 5 years

Source: 5 C.F.R. § 731.106 (Public Trust) and 5 C.F.R. § 732.203 (National Security).
Note: Government PR Requirements have changed over time. OPM and ODNI established the 5-year time requirement for all positions of Public Trust and National Security in 2015 and provided a temporary deferment period in 2018 as explained below.

In June 2018, as part of the Government-wide reform efforts to address a backlog of investigations, ODNI and OPM issued a memorandum that instituted temporary measures to extend PR timeframes if agencies took certain mitigating steps.[70] The memorandum explained that agencies would be permitted to extend the timeframes for PRs in order for investigative resources to focus on the inventory of pending initial

[70] Memorandum from the ODNI and OPM entitled: *Transforming Workforce Vetting: Measures to Reduce the Federal Government's Background Investigation Inventory in Fiscal Year 2018* (June 2018). The guidance temporarily extended new Public Trust reinvestigation submissions from 5 years to 7 years.

investigations. Specifically, agencies could defer new reinvestigation submissions for individuals at Tier 2 and Tier 4 positions if their review of a newly completed Standard Form 85P[71] did not identify relevant information impacting adjudication and a check of the FBI criminal history records (FBI fingerprint check) was conducted with favorable results. In addition, agencies could defer reinvestigations for Tier 3 and Tier 5 positions contingent upon a review of the Standard Form 86[72] and whether the subject would be enrolled in continuous vetting.[73]

SEPS's procedures state that it will run a report in eWorks each month to identify anyone with a BI that is 4-1/2 years old. However, we found many instances where the FDIC did not conduct PRs and instances where the FDIC did not initiate and order PRs within required timeframes. Specifically, we identified 38 individuals (31 employees and 7 contractor personnel) in our population where the last BI was completed more than 7 years ago according to the data in CHRIS.[74] In 4 cases, SEPS did not initiate and order the PR at all, and in 28 cases, it did not initiate and order PRs within the required timeframes. The average lapse between background investigations in these 28 instances was 8.6 years – well beyond the required timeframe of 5 years. We determined that PRs had been conducted timely in the remaining 6 cases. Table 7 summarizes results of our analysis, including the position risk level and the average time between investigations.

Table 7: OIG Analysis of Selected PRs Cases

Outcome of OIG Follow-up	Result	Moderate Risk (T2)	High Risk (T4)	Average Length Between Investigations (Years)
Not Conducted	4	3	1	N/A
Initiated Late	28	24	4	8.6
Conducted Timely	6	5	1	4.9
Totals	38	32	6	

Source: OIG review of CHRIS data and BI case files in eWorks and Documentum.

We determined that SEPS did not initiate and order PRs for the four individuals for the following reasons:

- SEPS misinterpreted information related to an employee's transfer, which resulted in the cancellation of the scheduled reinvestigation;
- A name change for one person caused a problem when data were migrated from Documentum to eWorks; and

[71] Questionnaire for Public Trust Positions.
[72] Questionnaire for National Security Positions.
[73] Continuous vetting means reviewing the background of a covered individual at any time to determine whether that individual continues to meet applicable requirements.
[74] Using 7 years to test the FDIC's application of PR requirements allowed us to apply a risk-based approach and accounted for the temporary extension granted by OPM and ODNI.

- Records were missing from the files as discussed further below.

This finding is similar to the OIG's Evaluation Report findings in 2014 on records management controls and data reliability. Specifically, we again found that some investigative case files were missing key documentation and system data were not reliable. For example, we found no related investigatory records for one of the four individuals who did not receive a PR. Additionally, in 10 of the 38 cases that we reviewed, the individual's adjudication date was missing from the FDIC systems.

SEPS officials noted that they could not effectively identify certain out-of-scope investigations, because the information contained within their existing systems was not kept up-to-date or accurately recorded due to prior manual processes. SEPS officials stated that this occurred because eWorks was not fully functional and the issues associated with incomplete and inaccurate data had migrated from the previous legacy systems to eWorks. Therefore, it will remain a challenge for the FDIC to ensure that required PRs are initiated when required by Federal regulation.

In addition, we learned that SEPS officials initiated their own review and identified another 99 individuals with out-of-scope BIs. These out-of-scope BIs consisted of 37 FDIC employees and contractor personnel occupying High-Risk positions and 62 occupying Moderate-Risk positions. According to SEPS officials, some of these cases were purposefully delayed so that their reinvestigations could be processed through eWorks, which was contrary to the required timeframes.

In August 2020, OPM advised agencies that the previous 2-year reinvestigation deferral period had expired, and that the agencies should return to applying the current 5-year timeframe for reinvestigations. OPM emphasized that any Public Trust reinvestigation previously deferred should be initiated. According to reports from SEPS officials, this change resulted in the need for the FDIC to initiate PRs for another 607 cases (152 High-Risk and 455 Moderate-Risk positions) that had previously been deferred. In addition, we discovered that the FDIC had never conducted the previously-described minimum checks required by ODNI and OPM to defer these cases. Therefore, all 607 cases were considered to be overdue.[75]

Also, in order to meet the reinstated 5-year requirement referenced above, SEPS officials advised that they would need to initiate another 410 PRs (57 High-Risk and 353 Moderate-Risk positions) by the end of 2020. To address the significant increase in pending cases due to this cycle adjustment, SEPS planned to initiate 200 to 300 reinvestigations per month starting in September 2020. SEPS officials,

[75] During our evaluation, SEPS officials noted that the June 2018 joint guidance provided agencies with an expectation for additional clarifying guidance on the changes to public trust reinvestigations, but that such guidance was never issued.

however, acknowledged that their ability to complete all reinvestigation cases by the end of 2020 may be affected by any surge staffing, which will take priority.

The FDIC may increase hiring to ensure readiness for any potential increase in supervisory workload, bank failure activity, and administrative support. As previously discussed, in December 2020, the FDIC Board approved an increase in the Agency's Operating Budget of $261 million (12.9 percent), largely to address "a potential increase during 2021 in supervision or resolution workload resulting from the ongoing pandemic." A significant hiring surge will increase the number of suitability screenings and background investigations processed through the PSSP. Therefore, FDIC leadership must be assured that the PSSP has the resources needed to ensure all new employees and contractors are properly screened and investigated without compromising efforts to complete PRs.

If misused, Public Trust positions can affect the integrity, efficiency, and/or effectiveness of the FDIC's mission, and diminish public confidence. As described previously in this report, individuals operating within Moderate-Risk and High-Risk Public Trust positions at the FDIC have access to its facilities and personnel, highly sensitive business information, PII, confidential information related to bank closures and confidential reports of examination, and often privileged access to FDIC mission critical systems.

Overdue reinvestigations without proper mitigations in place pose potential risks to national security and the public trust.[76] Without completing PRs on employees and contractors within required timeframes, the FDIC cannot ensure that these individuals continue to adhere to the Federal requirements for suitability and that their continued employment or conduct does not jeopardize the accomplishment of the FDIC's mission. Absent the completion of PRs, the FDIC is also not informed of potential insider threats operating within its environment.

As noted earlier in this Report, the FDIC has a very low tolerance for risks that could threaten its ability to protect the safety and security of its personnel and facilities and identify and prevent insider threats.[77] The FDIC also has a very low tolerance for risks that threaten its ability to comply with a required law or regulation. As a result, the potential for prioritizing PSSP efforts to address surge hiring over its periodic reinvestigation requirements appears to introduce an unacceptable risk to the FDIC.

[76] Memorandum from ODNI and OPM entitled: *Transforming Workforce Vetting: Measures to Reduce the Federal Government's Background Investigation Inventory in Fiscal Year 2018* (June 2018).
[77] See FDIC Risk Appetite Statement. Very Low – Areas in which the FDIC seeks to avoid, minimize, or eliminate risks because the potential downside costs are intolerable.

Recommendations

We recommend that the Deputy to the Chairman and Chief Operating Officer:

9. Develop and implement a project plan to ensure that outstanding PRs are prioritized, ordered, and completed in a timely fashion, and that upcoming PRs are initiated in a timely fashion as required by Federal regulations.

10. Resolve inaccuracies in SEPS's investigative case data.

11. Ensure sufficient resources to meet all program requirements, including reinvestigations, within required timeframes.

Contractor Risk Level Recorded in CHRIS Not Accurate

According FDIC procedures, all FDIC positions, including those of contractor personnel, must be evaluated and assigned a risk and sensitivity designation commensurate with the duties and responsibilities related to the efficiency of service and/or to national security. The purpose of designating a position risk and sensitivity level is to ensure that the incumbent undergoes the appropriate type of investigation consistent with Federal requirements.

FDIC Circular 1610.2, as amended January 15, 2020, states that "each contract[78] contains separately designated risk levels for each FDIC established labor category, or in the absence of labor categories, separately designated risk levels for each defined area of functional responsibility." Risk Level is an evaluative classification designation assigned to contract labor categories or contract functional areas based on duties performed that have the potential for affecting the integrity, efficiency, and/or effectiveness of the FDIC's mission, and when misused, may diminish public confidence. SEPS and OMs share responsibility for making Risk Level determinations in consultation with Information Security Managers. The PSG makes the final risk determination.

We found that risk level designation for contractor personnel was not accurate in CHRIS.[79] Accuracy refers to the extent that recorded data reflects the actual underlying information and is a component of data reliability. To determine whether data in CHRIS accurately reflected underlying support, we traced CHRIS data to the various source documents. Specifically, we traced contractor personnel risk level

[78] Contracts are described as including BOAs, RBOAs, and BPAs.
[79] Steps associated with evaluating whether we could rely on data in CHRIS and the scope limitation associated with this issue is more fully explained in Appendix 1.

designations for a sample of 13 contractors from CHRIS to the applicable FDIC forms and the contract.[80] We found:

- In 6 of the 13 cases, the Risk Level in CHRIS was not the same as the Risk Level in the contract. For 5 of these 6 cases, the Risk Level in CHRIS was lower than the Risk Level in the contract. In one case, the contract did not include a statement regarding the risk designation.
- In 2 of the 13 cases, the Risk Level in CHRIS was lower than the risk level on Form FDIC 1600/17, *Contractor Risk Level Record*.
- In 5 of the 13 cases, we could not find the form FDIC 1600/17.[81]
- In 4 of the 13 cases, the Risk Level in CHRIS was lower than the Risk Level on Form FDIC 1600/13.

Significantly, without accurate risk level data in CHRIS, we could not compare risk designations to the BIs completed for our population of contractors. Because we could not complete planned procedures, we considered this to be a scope limitation. We shared our results with SEPS, so that they could evaluate these results further as part of broader efforts being done to verify data.

As of June 2020, all relevant data in CHRIS had been migrated to eWorks, but not all case files had been migrated from Documentum. SEPS officials stated that they had started working to validate the data in eWorks but had not completed this review. SEPS officials were not able to provide a target date for completion and stated they were validating the data as they were conducting reinvestigations.

Recommendations

We recommend that the Deputy to the Chairman and Chief Operating Officer:

12. Conduct a comprehensive review to validate risk designation information for all contractors, and update risk designations based on the results of the review.

13. Initiate background investigations for contractors where their risk levels are higher than their previously completed background investigations.

[80] The 13 contractors were judgmentally selected to represent each of the Risk Levels 1 through 5 from the OIG population of 1,510 contractors.
[81] SEPS officials are not responsible for maintaining Form FDIC 1600/17, *Contractor Risk Level Record*, for individual contractors.

Employee Background Investigations Not Commensurate with Position Risk Designations

As described in the Background Section of this report, in accordance with Federal regulations, the FDIC requires that all positions be evaluated and assigned a risk and sensitivity designation commensurate with the duties and responsibilities for the position and related risk posed to the FDIC or to national security.[82] The purpose of designating a position risk and sensitivity level is to ensure that the incumbent undergoes the appropriate type of background investigation. If an employee or appointee's position is changed to a higher risk level or if an employee or appointee receives a promotion, demotion, or reassignment that increases their risk level, the employee or appointee is allowed to remain in or encumber the position.[83]

The FDIC's PSSP Employee Directive requires Division Supervisors/Managers to update position descriptions and approve position designation records that establish position risk and sensitivity levels. AOs within each FDIC Division/Office are responsible for informing SEPS of any changes that could affect risk level designations and must submit the associated personnel security documents and forms to SEPS. SEPS is required to initiate and update appropriate background investigations corresponding to position designation levels.

We analyzed CHRIS data for 5,744 FDIC employees and identified 804 instances where the risk and sensitivity levels recorded in CHRIS were not commensurate with the type of BI ordered. This figure represents nearly 14 percent of our FDIC employee population. In 281 cases of these 804 instances, or nearly 35 percent, the information contained within CHRIS for the employees indicated that the risk level for the position exceeded that of the associated BI. These 281 cases represent nearly 5 percent of our FDIC employee population.

We reviewed information in FDIC investigative case file systems for seven employee cases where our analysis of CHRIS data indicated the BI performed was not sufficient for the position risk and sensitivity level. For example, CHRIS data indicated a Tier 5 investigation was required, but a Tier 2 investigation was completed.

For the seven cases, we determined that three individuals did not receive the appropriate background investigation for their respective positions. In addition, SEPS officials determined that a fourth individual also did not receive the appropriate background investigation. In this particular case, the individual was operating in a

[82] FDIC Directive 2120.1 *Personnel Suitability Program* and Directive 1600.3 *National Security Program*. The responsibility for position risk designations and security designations lies with each Division/Office Director, or designee.
[83] 5 C.F.R. § 731.106(e) defines the requirements related to position risk level changes.

Special Sensitive[84] (Tier 5) national security position without the commensurate background investigation.[85]

We also identified numerous inaccuracies in the system data for each of the seven cases, including missing adjudication dates or inaccurate position sensitivity codes in CHRIS. These data issues in CHRIS made it appear that the other three individuals did not have the appropriate BI level, even though they actually did have it. In each of the four cases where the individual's BI was not commensurate with their position risk designation, SEPS had not been advised of the change in position sensitivity levels.

Notably, during our work on the FDIC's Personnel Security and Suitability Program in 2014, we similarly found a number of cases where the BI was not commensurate with the Risk Level Designation. Specifically, of the 108 files reviewed in that evaluation, 23 files (21 percent) supported that the level of background investigation conducted was lower than the required investigation type based on the risk level designated on the FDIC's *Personnel Security Action* form. During that evaluation, SEPS officials initiated work with DOA's Human Resources Branch to correct discrepancies. Nevertheless, these steps were not effective in preventing this problem from happening again.

SEPS officials stated that they were in the process of conducting a broad review of position sensitivity levels that should correct system anomalies and ensure that individuals have the appropriate background investigation.[86] According to SEPS officials, they lacked the capability to effectively monitor this area prior to the implementation and transfer of investigative case information to eWorks in June 2020 because they depended on DOA IT Specialists to create ad hoc queries from CHRIS.

Performing the appropriate level of background investigations on employees (and contractor personnel) is critical to ensure that the FDIC is both in compliance with its own policies and government-wide requirements and that these individuals possess the character, behaviors, and in certain cases, the "unquestioned allegiance to the United States"[87] necessary for their current position.

[84] According to FDIC Directive 1600.3, Special-Sensitive positions have the potential for inestimable impact and/or damage to national security.
[85] We did not initially determine that this individual was an exception because the individual's position risk description form indicated the position as Moderate Risk and the individual had received a Tier 2 background investigation. The individual's position sensitivity level was subsequently changed without SEPS's knowledge.
[86] For example, five of the seven cases we examined had already been flagged by SEPS as a result of this review.
[87] FDIC Directive 1600.3 *National Security Program*.

Recommendations

We recommend that the Deputy to the Chairman and Chief Operating Officer:

14. Review and validate position risk and sensitivity designations and initiate corrected BIs commensurate with position risk and sensitivity levels.

15. Review and update FDIC systems of record to reflect correct position risk information.

16. Provide training to program office officials of their responsibilities to notify SEPS of any changes to employee position risk designations.

17. Ensure that SEPS is aware of all changes to position risk designations and sensitivity levels at the FDIC, and that SEPS will monitor such modifications.

CHRIS Missing Data on PBI Completion Dates

To comply with PBI requirements, SEPS requires Security Specialists to gather certain key documents to conduct a preliminary clearance for determining FDIC employee and contractor personnel suitability. The FDIC uses Form 1600/19, entitled *Preliminary Background Investigation Checklist,* as a tool to record the collection of key documents and the preliminary clearance determination and approval. Specific documents collected include: FBI fingerprint and criminal records check; credit reports from major credit reporting agencies; Lexis/Nexis checks; and OIG/DRR investigation checks.

Our analysis found that CHRIS was missing PBI completion dates for 787 employees and contractors within the population we examined (employees and contractors with active IT accounts as of December 2, 2019). Missing data were predominantly related to FDIC employees (94 percent of the 787 cases) and occurred most frequently between 2008 and 2010 (48 percent of the cases). Missing data primarily related to two periods: (1) individuals within our population subject to PBIs in 2004 and prior years and (2) individuals subject to PBIs between 2008 and 2010, when the FDIC's staffing and contractor staffing increased in response to the 2008-2013 financial crisis. Table 8 identifies the number of PBI dates missing during various time periods relative to the number of PBIs required during that period for individuals in our population.

Table 8: OIG Analysis of Missing PBI Completion Dates in CHRIS

Time period	PBI Cleared Dates Missing in CHRIS	Total PBIs Required During the Period	Percentage
1994-2004	308	555	55%
2005-2007	72	455	16%
2008-2010	369	1,260	29%
2011-2014	16	1,029	2%
2015-2019	22	2,171	1%
Total	787	5,470	14%

Source: OIG analysis of PBI records in CHRIS for OIG population.

We reviewed case files for the 22 individuals with missing PBI dates during the 2015-2019 timeframe. In 16 of these 22 cases, the *Preliminary Background Investigation Checklist* was not always completed consistent with the requirements outlined in the FDIC's procedures. Such inconsistencies occurred due to poor recordkeeping and poor execution of policies and procedures and the lack of proper oversight by SEPS of the contractor personnel responsible for inputting PBI completion dates into CHRIS.

We found similar issues in the evaluation completed by the OIG in 2014. In that review, we found PBI data issues were caused because the PSSP team updated PBI data manually, and there was neither review of data entered nor approval functionality in the system used at that time.

SEPS officials have indicated that they do not plan to undertake a review of documentation for the remaining 765 cases in order to determine whether PBIs were in fact done because of the age of the case files and, in their view, the risks are mitigated by the fact that these individuals have been subject to BIs and applicable PRs.

Recommendations

We recommend that the Deputy to the Chairman and Chief Operating Officer:

18. Evaluate the risks associated with aged cases where the FDIC cannot demonstrate compliance with the statutory requirements for completed PBIs, record such risk evaluations, and assess in writing whether or not these risks are acceptable under the FDIC's Enterprise Risk Management framework.

19. Update employee and contractor data for the 787 cases identified in this report, in order to reflect PBI completion dates or annotate in the system that the PBI data are missing.

20. Establish metrics, develop reports, and monitor PBI performance to ensure consistent execution of this statutory requirement.

The FDIC Not Meeting Goal Established to Complete PBIs

The FDIC's contract establishes a timeliness objective for PBIs to be completed within 3 to 5 days. This goal was established to help monitor the contractor's performance.

We found that SEPS, and its supporting contractor, did not regularly achieve the PBI timeliness objective of 3 to 5 days. As shown in Table 9, SEPS achieved its timeliness objective in only 200 cases or 9 percent of the time, and PBIs exceeded more than 12 days in approximately 59 percent of the cases.

Table 9: OIG Analysis of PBI Timeliness

OIG Analysis of PBI Processing Time	Number of Cases
PBI Processed in 5 days or Less	200
PBI Processed in 6 to 12 days	687
PBI Processed in 13 days or More	1,262
Total	2,149

Source: OIG analysis of PBI data in CHRIS.

SEPS officials believe that this timeliness goal was unrealistic, because it did not allow sufficient time to obtain information necessary to complete the PBIs for employees and contractor personnel. SEPS officials said they intended to revise this metric to a goal of 7 to 12 days.

Nevertheless, as supported by the Table above, SEPS will remain challenged to process PBIs within the revised timeframe. These challenges may be exacerbated by any surge hiring.

Timely completion of PBIs is critical to ensure that the FDIC is able to acquire the resources it needs to execute its mission and objectives. Furthermore, setting reasonable expectations for FDIC managers regarding the timeframes for PBI processing would allow them to better allocate and assign resources to meet their needs.

Recommendation

We recommend that the Deputy to the Chairman and Chief Operating Officer:

21. Update the PBI processing goal, and monitor performance against established metrics to ensure the timely acquisition of FDIC resources.

The FDIC Is Adhering to Reciprocity Requirements

As previously described, reciprocity is the acceptance of previous Federal background investigations for newly-hired employees and contractors who are transferring from other Federal agencies.

Using CHRIS data, we identified 128 employees who had transferred to the FDIC from other Federal agencies during the 3-year period from 2017 through 2019.[88] Of these, we identified 21 employees who had a BI around the time that they transferred to the FDIC. We judgmentally selected 12 of these 21 employees for review and determined that the FDIC initiated new background investigations for appropriate causes, such as changes in position risk levels requiring a higher level clearance or expiration of the employee's previous background investigation. Based on results of our analysis, the FDIC effectively complied with reciprocity rules.

FDIC COMMENTS AND OIG EVALUATION

On January 6, 2021, the FDIC's Deputy to the Chairman and Chief Operating Officer provided a written response to a draft of this report (FDIC Response), which is presented in its entirety in Appendix 4. In its response, the FDIC stated it concurred with the report's findings and was strongly committed to promptly and effectively addressing each of the OIG's recommendations, including those related to the OIG's 2014 report on the PSSP. The FDIC Response recognized that program controls, processes, and data needed to be consistently better and more effectively executed. The FDIC Response further stated that resolving these shortfalls, establishing and sustaining an effective PSSP across the FDIC, and restoring confidence in the Agency's security program is receiving management's full attention and the full attention of senior FDIC leadership.

To that end, in addition to the corrective actions proposed to address our recommendations, the FDIC Response outlined a number of initiatives it has already begun to implement that will help prevent a recurrence of the program failures

[88] Our evaluation procedures for reciprocity did not address contractors because neither SEPS nor CHRIS data could identify contractors who had transferred to the FDIC from other Federal agencies.

identified in our findings. These initiatives included issuing new SEPS-related Directives and procedures; increasing SEPS staff; and enhancing eWorks.

The FDIC stated that all corrective actions would be completed by June 30, 2021.

Objective

Our evaluation objective was to determine whether the FDIC has an effective program to: (1) complete PBIs in a timely manner before hiring individuals; (2) order and adjudicate BIs commensurate with position risk designations and reciprocity rules; and (3) order reinvestigations within required timeframes.

We performed our work from June 2019 to September 2020 at the FDIC's offices in Arlington, Virginia.[89] We performed our work 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 our review included the following *processes*:

1. The FDIC's PBI process (a.k.a., *Minimum Standards for Employment with the FDIC*);
2. BI process for (1) Public Trust and (2) National Security Positions, including the process for evaluating reciprocity; and
3. PR process for (1) Public Trust and (2) National Security Positions.

By design, we limited our analysis of reciprocity to employees within our population that had transferred from other agencies. While the FDIC applies reciprocity requirements to FDIC contractors, we had no way to identify contract personnel who previously worked for Federal agencies before working for the FDIC.

Our approach centered on applying data analytics to PSSP-related data in CHRIS[90] for all employees and contractor personnel with access to FDIC systems as of December 2, 2019. This population included 7,254 individuals consisting of 5,744 FDIC employees and 1,510 contractor personnel. To implement our approach, we first gained an understanding of Federal suitability and security requirements by reviewing applicable laws and regulations and the FDIC's PBI requirements, including the following:

- 12 C.F.R. Part 336 – Minimum Standards of Fitness for Employment with the FDIC;

[89] Due to mandatory telework requirements instituted by the FDIC, we conducted a portion of our work remotely.
[90] In addition to serving as the authoritative source for employee data, CHRIS maintains background investigation submission/clearance dates for FDIC employees. CHRIS was also used to record the background investigation results of FDIC contractors and non-FDIC government employees until June 2020.

- 12 C.F.R. Part 366 - Minimum Standards of Integrity and Fitness for an FDIC Contractor;
- 5 C.F.R. Part 731 Suitability;
- 5 C.F.R Part 732 National Security Positions; and
- Executive Orders listed in Appendix 2.

We furthered our understanding of Federal suitability and security requirements by reviewing information and guidance found on (1) the Office of Personnel Management's website; (2) the Office of the Director of National Intelligence website, and (3) the Defense Counterintelligence Security Agency website. To learn more about government-wide program reforms in this area we reviewed information on the Federal Government's Performance Website (Performance.gov).

To understand the FDIC policies and procedures for the PSSP, we reviewed the following:

- FDIC Directive 2120.1, *Personnel Suitability Program for Applicants and Employees*, dated January 15, 2020;[91]
- FDIC Directive 2120.5, *Minimum Standards for Employment with the Federal Deposit Insurance Corporation ("Corporation") as Mandated by the Resolution Trust Corporation Completion Act ("RTCCA"),* dated February 22, 2013;
- FDIC Directive 1610.2, *Personnel Security and Suitability Program for Contractors and Contractor Personnel*, dated January 15, 2020;[92]
- FDIC Directive 1600.3, *National Security Program*, dated September 24, 2001 and last revised December 11, 2017;
- FDIC Directive 3700.16, *FDIC Acquisition Policy Manual (APM)*, dated August 22, 2008 and last updated January 24, 2020;
- FDIC Directive 1600.7, *FDIC Insider Threat and Counterintelligence Program*, dated September 20, 2016;
- FDIC *Acquisition Procedures, Guidance and Information*, September 2020;
- *SEPS Security Guide for Employee Background Investigations* (undated); and
- *SEPS Personnel Security Procedures Guide for Contracting Officers and Oversight Managers* (undated).

We also reviewed *Standard Operating Procedures Handbook for Operations at the FDIC* developed by Global Resources Solutions, eWorks Resources available on the FDIC's internal and external websites, and assessed prior reviews of the PSSP.

We interviewed officials in the following FDIC Divisions and Offices:

[91] This Directive supersedes 2120.1, *Personnel Suitability Program*, dated December 7, 2007.
[92] This Directive supersedes 1610.2, *Security Policy and Procedures for FDIC Contractors*, dated January 28, 2010.

- DOA, including the Assistant Director, SEPS; the Security Operations Chief; and Personnel Security Specialists in the PSG;
- The FDIC's Insider Threat Program Manager;
- Officials in DIT to understand how the data loss prevent tool is applied; and
- The FDIC's Chief Risk Officer and members of the Chief Risk Officer's staff.

Before requesting and obtaining data from the FDIC, we interviewed both DIT and DOA officials. We interviewed DIT officials to understand and obtain data from the FDIC's Microsoft Windows Active Directory®.[93] We worked with DOA Human Resource Information Specialists and SEPS officials to understand and obtain PSSP-related data from CHRIS. We specifically discussed data fields and cross-walked how we planned to use the data to answer our objective. DOA officials also provided definitions of data to help us confirm our understanding of the data.

We relied on an OIG Senior IT Specialist to review the standard query code used by a DOA HR IT Specialist to extract data from CHRIS to ensure DOA appropriately interpreted our request and to conduct data completeness and validation procedures. We also relied on the OIG Senior IT Specialist to review records in the FDIC's Active Directory to identify unique users with enabled accounts and merge source files from DIT and DOA.

To ensure we could rely on data in CHRIS before applying analytic techniques, we traced a judgmental sample of key data fields to FDIC source documents. Except in one area, we determined we could rely on the accuracy of the data, meaning the data in CHRIS represented what we found on the source documents. We determined we could not rely on the data in CHRIS for contractor personnel risk levels. For a judgmentally selected sample of 13 contractors,[94] we compared Risk Levels in CHRIS to various source documents and judged the discrepancies to render the data not reliable for our purposes. We viewed this as a scope limitation and included a finding on the accuracy of contractor risk level designations in the Results Section of this report detailing the discrepancies found.

Once our two data sets were combined, the Senior IT Specialist used automated techniques to filter and sort the data to identify potential anomalies to answer our objective. Specifically, we analyzed the data to identify the following anomalies:

- Individuals with an unfavorable BI adjudication determination;
- Individuals with out-of-scope BIs, meaning a PR had not been initiated within applicable timeframes;

[93] The Microsoft Windows Active Directory is an IT service within the Windows Server® operating system platform that is used to centrally manage user accounts and security settings (including access).
[94] The 13 contractors were judgmentally selected to represent each of the Risk Levels 1 through 5 from the population of 1,510 contractors.

- Individuals without a PBI cleared date and BI completed date, meaning the individual had not been subject to any review;
- Individuals without a PBI cleared date;
- Individuals with PBI cleared dates before their entered on duty date; and
- Individuals whose BI level was not commensurate with the position risk and sensitivity level recorded in CHRIS.

We also relied on the CHRIS data to evaluate the timeliness of PBIs.

To further evaluate the anomalies identified through analyzing the data, we reviewed case file documentation, information in eWorks, and discussed exceptions with FDIC officials before concluding on our test results.

The EOs, among other things, provide definitions, processes, responsibilities, and authorities related to eligibility for access to classified information, suitability and fitness for government employment, and security clearance reform.

EO 10450 | April 1953 | *Security Requirements for Government Employment, as amend*ed. Contains factors about personal character and conduct that are used to establish whether the employment or continued employment of an individual in the Federal civilian service is "clearly consistent with the interests of national security." The order forms the basis of OPM's civilian personnel suitability program, which includes procedures for determining security clearance eligibility.

EO 12968 | August 1995 | *Access to Classified Information and Background Investigation Standards*. Establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

EO 13381 | June 2005 | Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information. Establishes to the extent consistent with safeguarding the security of the United States and protecting classified national security information from unauthorized disclosure, agency functions relating to determining eligibility for access to classified national security information shall be appropriately uniform, centralized, efficient, effective, timely, and reciprocal.

EO 13467 | June 2008 | Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information. Calls for investigations of suitability and security to be aligned using consistent standards, to the extent practicable. The EO established the PAC to be the government-wide governance structure responsible for driving implementation and overseeing security and suitability reform efforts. Further, the order appointed the Deputy Director for Management at the Office of Management and Budget as the Chair of the Council and designated the Director of National Intelligence as the Security Executive Agent and the Director of OPM as the Suitability Executive Agent.

EO 13488 | January 2009 | Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust. Establishes the following policy when (a) agencies determine the fitness of individuals to perform work as employees in the excepted service or as contractor employees, prior favorable fitness or suitability determinations should be granted reciprocal recognition, to the extent practicable

and (b) it is necessary to reinvestigate individuals in positions of public trust in order to ensure that they remain suitable for continued employment.

EO 13526 | December 2009 | Classified National Security Information. Prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.

EO 13869 | April 2019 | Transferring Responsibility for Background Investigations to the Department of Defense. Shifts primary responsibility for conducting background investigations for the Federal government from the Office of Personnel Management to the Department of Defense. The Defense Counterintelligence and Security Agency serves as the primary entity for conducting background investigations for the Federal government.

AO	Administrative Officer
ASB	Acquisition Services Branch
BI	Background Investigation
BOA	Basic Ordering Agreement
BPA	Blanket Purchase Order
CE	Continuous Evaluation
CHRIS	Corporate Human Resource Information System
CNSI	Classified National Security Information
CVS	Central Verification System
DIT	Division of Information Technology
DLP	Data Loss Prevention
DOA	Division of Administration
EO	Executive Order
eQip	Electronic Questionnaire for Security Processing
ERM	Enterprise Risk Management
eWorks	Enterprise Workforce Solution
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FIS	Federal Investigative Standards
FTE	Full-time Equivalent
GAO	Government Accountability Office
ISM	Information Security Manager
IT	Information Technology
ITCIP	Insider Threat and Counterintelligence Program
LOI	Letter of Issues
ODNI	Office of the Director of National Intelligence
OF	Optional Form
OM	Oversight Manager
OPM	Office of Personnel Management
ORMIC	Office of Risk Management and Internal Controls
PAC	Security, Suitability, and Credentialing Performance Accountability Council
PBI	Preliminary Background Investigation
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PSG	Personnel Security Group
PSO	Personnel Security Officer
PSSP	Personnel Security and Suitability Program
RBOA	Receivership Basic Ordering Agreement
SEPS	Security and Emergency Preparedness Section
SF	Standard Form
SOP	Standard Operating Procedure

FDIC Division of Administration
FEDERAL DEPOSIT INSURANCE CORPORATION

Memorandum January 6, 2021

To: Terry L. Gibson, Assistant Inspector General for Program Audits and Evaluations, Office of Inspector General

From: Arleas Upton Kea, Deputy to the Chairman and Chief Operating Officer ARLEAS KEA Digitally signed by ARLEAS KEA Date: 2021.01.07 16:09:30 -05'00'

Subject: Management Response to the OIG Draft Report, FDIC's Personnel Security and Suitability Program (2019-004)

The FDIC has completed its review of the Office of Inspector General's (OIG) draft evaluation report titled FDIC's Personnel Security and Suitability Program (PSSP), issued on December 19, 2020. In its report, the OIG identified a number of significant findings and recommendations. FDIC management concurs with the report's findings and is strongly committed to promptly and effectively addressing each of the OIG's recommendations, including those related to the OIG's 2014 report on the PSSP program.[1]

Ensuring the safety and protection of FDIC's employees, contractors, visitors, and facilities is the Division of Administration's (DOA) highest priority. DOA takes full responsibility for the breakdown in processes and controls described in the OIG's report, many of which are related to similar findings the OIG made in its 2014 review of the PSSP program. DOA's performance fell significantly short in addressing the recommendations from 2014 and in those areas further identified in this report. We recognize program controls, processes, and data need to be consistently better and more effectively executed. Resolving these shortfalls, establishing and sustaining an effective PSSP across the FDIC, and restoring confidence in the Agency's security program are receiving our full attention and the full attention of senior FDIC leadership.

To that end, in addition to the corrective actions we describe later, DOA has already begun implementation of a number of initiatives that will help prevent a recurrence of the program failures identified in the OIG's findings. These initiatives include:

- Issued new personnel security directives for contractors, applicants, and employees and related implementation guidance on January 15, 2020. These directives updated personnel security authorities and responsibilities, incorporated processes from previously published Interim Policy Memoranda, and addressed how the Enterprise Workforce Solution (eWorks) would be used in the on-boarding process.

[1] OIG Report, The FDIC's Personnel Security and Suitability Program, (EVAL-14-003) (August 2014).

FDIC Division of Administration

- Implemented new operational procedures on January 15, 2020 that provide for enhanced collaboration between DOA's Security and Emergency Preparedness Section (SEPS), Human Resources Branch, and the Insider Threat and Counterintelligence Program (ITCIP).
- Increased professional federal staff and contractor resources in SEPS between August and September 2020.
- Enhanced eWorks to address case management workflow, data analytic capability, data reliability, reporting, and integration of HR system data between April 2019 and September 2020. Additional enhancements are in progress.
- Completed a review of our systems and records on March 8, 2020 to verify that there are no employees or contractors on board or with access to our networks that have unfavorable adjudications. Also verified that all known completion dates for background investigations (BI) have been appropriately documented.

We are also developing an enterprise-wide strategy to review and update all employee and contractor position risk designation levels and data contained in the Agency's official systems of record. DOA will complete this initiative by March 31, 2021.

In its report, the OIG observed that there were a substantial number of days between hiring, on-boarding (which includes a preliminary background investigation), and final adjudication of a complete BI. During the timeframes covered by the OIG report, it is noteworthy that the Office of Personnel Management (OPM) experienced a significant backlog in processing times for BIs. This backlog was compounded by the OPM data breach in 2013-14, which resulted in investigation times exceeding an average of three years. At that time, OPM was the suitability executive agent (SUITEA) and investigative authority for conducting BIs. As such, the OPM backlog and processing times had a significant impact on the completion of BIs for FDIC employees and contractors. On October 1, 2019, responsibility to conduct BIs was transferred to the Defense Counterintelligence and Security Agency (DCSA). Since then, DCSA has significantly reduced the average BI processing timeline.

Recommendations

DOA acknowledges that an effective PSSP requires accountability, continuous improvement, effective deployment of existing and emerging technologies, improved communication between staff and management officials, and appropriate education and training of all employees. The OIG's report includes recommendations that are reasonable and helpful in all of these areas.

In addition to the corrective actions described below, SEPS is currently working with the Chief Information Officer (CIO) and the Chief Financial Officer (CFO) to secure resources and funding for additional eWorks enhancements. These identified improvements, such as a dashboard and other reporting tools, will enhance case monitoring and follow-up efforts and

FDIC Division of Administration
FEDERAL DEPOSIT INSURANCE CORPORATION

enable SEPS to more effectively measure performance. SEPS is also working with the CIOO to enhance eWorks capabilities to address additional compliance requirements, particularly related to processing timelines.

FDIC management responses to the OIG's recommendations follow.

Recommendation 1: Coordinate with the Chief Risk Officer and review the Risk Assessment associated with the "Security - Personnel and Physical" risk to ensure it fully reflects all risks, known weaknesses within the program, and the findings communicated in this report.

Management Decision: Concur

Corrective Actions:

Based on the results of the OIG's audit, DOA has coordinated with the Chief Risk Officer to update the risk assessment and assigned risk rating for this area in the FDIC's Risk Inventory and Risk Profile.

Estimated Completion Date: Completed (pending OIG review of corrective actions)

Recommendation 2: Communicate the results of the updated Risk Assessment to the Operating Committee and update the FDIC's Risk Profile as necessary.

Management Decision: Concur

Corrective Actions:

DOA and the Chief Risk Officer will communicate the updated risk assessment and risk profile for the PSSP to the Operating Committee, along with additional information on corrective actions associated with this report and other improvements, at the first Operating Committee meeting in 2021.

Estimated Completion Date: January 29, 2021

Recommendation 3: Formally define key process steps for removing contractors SEPS adjudicated to be unfavorable and establish timeframes for executing those process steps.

Management Decision: Concur

Corrective Actions:

On March 8, 2020, SEPS completed a review of our systems and records to verify that there

FDIC Division of Administration
FEDERAL DEPOSIT INSURANCE CORPORATION

are no employees or contractors on board or with access to our networks that have unfavorable adjudications.

On August 1, 2020, SEPS implemented case monitoring capabilities in eWorks to allow for improved tracking of all aspects of the BI process, including removal of unfavorably adjudicated contractors.

SEPS also began updating its Standard Operating Procedures (SOPs) upon receipt of the OIG's discussion draft report. SEPS will work with DOA's Management Services Branch (MSB) and the Office of Risk Management and Internal Controls (ORMIC) to ensure the SOPs contain controls, process steps, and timeframes for removing contractors SEPS adjudicates to be unfavorable. These SOPs will articulate clear roles and responsibilities related to the removal of contractors and employees with unfavorable adjudications – within SEPS, for the ITCIP and the Legal Division, and for administrative officers (AOs) and oversight managers (OMs) across the FDIC. These SOPs will help ensure that the BI process is implemented timely and effectively, such that all contractors and employees meet minimum standards of integrity and fitness prior to on-boarding and for the duration of their relationship with the FDIC.

Estimated Completion Date: February 26, 2021

Recommendation 4: Provide training to program office officials with responsibilities under PSSP on process steps and timeframes for removal action of contractors SEPS adjudicates to be unfavorable.

Management Decision: Concur

Corrective Actions:

Upon completion of the SOPs from recommendation 3, SEPS will conduct training sessions for all appropriate FDIC employees on the updated BI process. The training content will emphasize PSSP enhancements, including-specific process steps and corresponding timeframes for removing contractors SEPS adjudicates to be unfavorable.

Estimated Completion Date: March 31, 2021

Recommendation 5: Monitor and confirm that contractors adjudicated unfavorably are removed within established timeframes.

Management Decision: Concur

FDIC Division of Administration
FEDERAL DEPOSIT INSURANCE CORPORATION

Corrective Actions:

As noted in the response to recommendation 3, SEPS has established roles and responsibilities for monitoring and confirming that contractors adjudicated unfavorably are removed within established timeframes. In addition, the SOPs from recommendation 3 will include redundant controls to ensure there is no single point of failure in overseeing the removal process.

Estimated Completion Date: February 26, 2021

Recommendation 6: Evaluate and document the Risk Assessment of completing Background Investigations for contractor personnel in high-risk positions before they begin work at the FDIC.

Management Decision: Concur

Corrective Actions:

SEPS will work with MSB, the Acquisition Services Branch (ASB), ORMIC, and the Legal Division to perform and document a risk assessment of those provisions in Directive 1610.2, Personnel Security and Suitability Program for Contractors and Contractor Personnel, related to when contractor personnel in high-risk positions can begin work for the FDIC.

Estimated Completion Date: March 31, 2021

Recommendation 7: Update policies and procedures to ensure all individuals with unfavorable adjudications are referred to the ITCIP Program Manager to ensure full consideration of insider threat risks.

Management Decision: Concur

Corrective Actions:

SEPS began updating its SOPs upon receipt of the OIG's discussion draft report. The FDIC ITCIP Directive 1600.7 currently provides for suitability-related referrals. SEPS will review associated content in Directive 1610.2 and update it as necessary.

Estimated Completion Date: February 26, 2021

Recommendation 8: Establish procedures that require the scope and duration of the Data Loss Prevention (DLP) review process to correspond with the risk associated with the individual being removed due to an unfavorable adjudication.

FDIC Division of Administration
FEDERAL DEPOSIT INSURANCE CORPORATION

Management Decision: Concur

Corrective Actions:

DOA will coordinate with the CIO organization and Office of Chief Information Security Officer (OCISO) to review timelines and procedures in the current DLP process. The FDIC will adopt a risk-based approach to conducting DLPs, to include considering the risk level associated with the position held by the individual being removed, the conduct that contributed to the unfavorable adjudication, any relevant timeframes associated with the risk, and any other appropriate factors.

Estimated Completion Date: March 31, 2021

Recommendation 9: Develop and implement a project plan to ensure that outstanding Periodic Reinvestigation(s) (PR)s are prioritized, ordered, and completed in a timely fashion, and that upcoming PRs are initiated in a timely fashion as required by Federal regulations.

Management Decision: Concur

Corrective Actions:

SEPS established a strategic plan to address the new PR case workload shortly after OPM's decision in August 2020 to change the PR to a five-year cycle. The plan utilizes the new eWorks capabilities to initiate, process, and monitor PRs through a case workflow process. The plan has been implemented, and SEPS will monitor progress in prioritizing, ordering and completing PRs throughout the first quarter of 2021, to ensure that its project plan is resulting in PRs being initiated in a timely manner as required by Federal Regulations. SEPS will provide a progress report to the Chief Operating Officer that summarizes the PRs ordered and completed each quarter.

Estimated Completion Date: April 30, 2021

Recommendation 10: Resolve inaccuracies in SEPS's investigative case data.

Management Decision: Concur

Corrective Actions:

SEPS is developing quality assurance/quality control procedures for staff and contractors to ensure investigative data is accurate and complete prior to initiating the required BIs. SEPS will complete a review of investigative data in conjunction with its planned corrective actions

FDIC Division of Administration
FEDERAL DEPOSIT INSURANCE CORPORATION

for recommendations 12 through 17. SEPS will provide a progress report to the Chief Operating Officer that describes the status of corrected investigative case data.

Estimated Completion Date: February 26, 2021

Recommendation 11: Ensure sufficient resources to meet all program requirements, including reinvestigations, within required timeframes.

Management Decision: Concur

Corrective Actions:

DOA was authorized two additional full-time employees (FTEs) earlier in 2020, and hired two personnel security specialists in September 2020. At the same time, SEPS hired a third personnel security specialist to fill an existing vacancy, resulting in doubling the PSSP's federal staff. The additional FTEs will help meet program requirements, and prepare the program for potential surge hiring. DOA was recently authorized an additional FTE management program analyst / security specialist to support PSSP requirements. SEPS will work with HRB to post the position and complete the hiring action.

In addition, DOA recently submitted a reorganization proposal that will improve oversight, create more manageable spans-of-control, and enhance the efficiency of the BI process within SEPS. The reorganization proposal is awaiting input from DOA's Human Resources Branch (HRB) and is expected to be approved and implemented in January 2021.

Estimated Completion Date: January 29, 2021

Recommendation 12: Conduct a comprehensive review to validate risk designation information for all contractors, and update risk designations based on the results of the review.

Management Decision: Concur

Corrective Actions:

SEPS will coordinate with ASB and program OMs to validate risk designations for all active contractors. Risk designation updates will be documented in accordance with ASB and SEPS policies and procedures.

Estimated Completion Date:

OMs will complete an initial review and update of risk designations by February 28, 2021.

FDIC Division of Administration
FEDERAL DEPOSIT INSURANCE CORPORATION

OMs will complete a comprehensive review to validate risk designation information by May 31, 2021.

Recommendation 13: Initiate background investigations for contractors where their risk levels are higher than their previously completed BI.

Management Decision: Concur

Corrective Actions:

Upon completion of the review outlined in recommendation 12, SEPS will work with OMs to initiate appropriate BIs for contractors requiring a BI upgrade. This effort will be initiated as Divisions validate the risk designations for all active contractors. The eWorks case management system will be utilized to initiate and manage the case workload.

Estimated Completion Date: March 31, 2021

Recommendation 14: Review and validate position risk and sensitivity designations and initiate corrected BIs commensurate with position risk and sensitivity levels.

Management Decision: Concur

Corrective Actions:

SEPS will coordinate with HRB, Classification, AOs, and other Human Resources and program staff at headquarters and regional offices to validate position risk and sensitivity designations for all active employees. Updates will be documented in accordance with HRB and SEPS policies and procedures by February 26, 2021. Upon completion of the review, SEPS will work with respective parties to initiate BIs for those employees requiring a BI upgrade. This effort will be initiated as Divisions complete their review(s). The eWorks case management system will be utilized to initiate and manage the case workload.

Estimated Completion Date:

Review and validate position risk and sensitivity designations by February 26, 2021.

Initiate corrected BIs commensurate with position risk and sensitivity levels by March 31, 2021.

FDIC Division of Administration
FEDERAL DEPOSIT INSURANCE CORPORATION

Recommendation 15: Review and update FDIC systems of record to reflect correct position risk information.

Management Decision: Concur

Corrective Actions:

Concurrent with recommendation 14, HRB and AOs will update CHRIS HR to reflect position risk level changes. The risk level information will be updated in CHRIS HR and eWorks once the planned CHRIS HR system upgrades associated with position risk level/position description are completed.

Estimated Completion Date: March 1, 2021

Recommendation 16: Provide training to program office officials of their responsibilities to notify SEPS of any changes to employee position risk designations.

Management Decision: Concur

Corrective Actions:

As part of the review of risk designations associated with recommendations 12 through 15, DOA will conduct an extensive outreach and communications campaign with AOs and OMs to ensure they understand their responsibilities, the requirements of the associated review, and associated timelines for both employees and contractors. These communications will continue through the completion of these associated recommendations.

Following the completion of this process, SEPS will review existing training materials on eWorks position risk level designation processes and update as required. SEPS will hold refresher training sessions for AOs, OMs, human resources specialists, and HRB classification specialists to ensure understanding and compliance with position risk designation update procedures. Training will also be provided to new eWorks users as part of the eWorks access request process. Update procedures will also be published on the SEPS website as a resource for program offices.

Estimated Completion Date: June 30, 2021

Recommendation 17: Ensure that SEPS is aware of all changes to position risk designations and sensitivity levels at the FDIC, and that SEPS will monitor such modifications.

Management Decision: Concur

FDIC Division of Administration
FEDERAL DEPOSIT INSURANCE CORPORATION

Corrective Actions:

On August 31, 2020, SEPS implemented a monthly review of position risk level changes utilizing a CHRIS HR report to verify the change(s) against existing case information within eWorks. SEPS will coordinate with respective AOs and HR Specialists, as referenced in recommendations 15 and 16 to ensure appropriate updates are initiated.

Estimated Completion Date: January 29, 2021

Recommendation 18: Evaluate the risks associated with aged cases where the FDIC cannot demonstrate compliance with the statutory requirements for completed PBIs, record such risk evaluations, and assess in writing whether or not these risks are acceptable under the FDIC's Enterprise Risk Management framework.

Management Decision: Concur

Corrective Actions:

SEPS will establish a risk framework to evaluate aged cases based on the Enterprise Risk Management framework, position risk level, and mitigating factors such as BIs or PRs completed since initial hire date. Assessment results will be documented and presented to the Operating Committee.

Estimated Completion Date: February 15, 2021

Recommendation 19: Update employee and contractor data for the 787 cases identified in this report, in order to reflect PBI completion dates or annotate in the system that the PBI data is missing.

Management Decision: Concur

Corrective Actions:

On May 8, 2020, SEPS began review of all PBI completion dates, and updated respective records accordingly. Following the outcome of recommendation 18, SEPS will document standardized language of the risk decision within the respective 787 cases in which PBI completion dates were not available.

Estimated Completion Date: March 31, 2021

Recommendation 20: Establish metrics, develop reports, and monitor PBI performance to ensure consistent execution of this statutory requirement.

FDIC Division of Administration
FEDERAL DEPOSIT INSURANCE CORPORATION

Management Decision: Concur

Corrective Actions:

On March 31, 2020, SEPS developed a weekly report to monitor performance metrics, which include PBI processing data points. SEPS also developed a dashboard report to measure case processing compliance with established timelines. SEPS will develop and administer a quality assurance process to review and monitor compliance of completed PBIs with DCSA quality and timeliness guidelines. This process will complement, and be based on, DCSA's Quality Assessment Reporting Tool, which we use for case quality reviews when BIs are submitted to DCSA.

Estimated Completion Date: March 31, 2021

Recommendation 21: Update the PBI processing goal, and monitor performance against established metrics to ensure the timely acquisition of FDIC resources.

Management Decision: Concur

Corrective Actions:

SEPS will coordinate with ASB to update the processing timeline requirements within the contract's deliverables. Realistic PBI processing goals will be established, and reporting will be used to monitor success.

Estimated Completion Date: January 29, 2021

This table presents management's 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	DOA has coordinated with the Chief Risk Officer to update the risk assessment and assigned risk rating for this area in the FDIC's Risk Inventory and Risk Profile.	January 7, 2021		Yes	Open
2	DOA and the Chief Risk Officer will communicate the updated risk assessment and risk profile for the PSSP to the Operating Committee, along with additional information on corrective actions associated with this report and other improvements, at the first Operating Committee meeting in 2021.	January 29, 2021		Yes	Open
3	SEPS began updating its SOPs to ensure the SOPs contain controls, process steps, and timeframes for removing contractors SEPS adjudicates to be unfavorable.	February 26, 2021		Yes	Open
4	SEPS will conduct training sessions for all appropriate FDIC employees on the updated BI process. The training content will emphasize PSSP enhancements, including specific process steps and corresponding timeframes for removing contractors SEPS adjudicates to be unfavorable.	March 31, 2021		Yes	Open
5	On August 1, 2020, SEPS implemented case monitoring capabilities in eWorks to allow improved tracking of all aspects of the BI process, including removal of unfavorably adjudicated contractors. In addition, updated SOPs will include redundant controls to ensure there is no single point of failure in overseeing the removal process.	February 26, 2021		Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
6	SEPS will work with the Management Services Branch, the Acquisition Services Branch (), the Office of Risk Management and Internal Controls, and the Legal Division to perform and document a risk assessment of those provisions in Directive 1610.2, *Personnel Security and Suitability Program for Contractors and Contractor Personnel*, related to when contractor personnel in high-risk positions can begin work for the FDIC.	March 31, 2021		Yes	Open
7	SEPS will begin review of Directive 1610.2, *Personnel Security and Suitability Program for Contractors and Contractor Personne*l and update it as necessary to align with existing guidance in Directive 1600.7, *FDIC Insider Threat and Counterintelligence Program.*	February 26, 2021		Yes	Open
8	DOA will coordinate with the Chief Information Officer organization and Office of the Chief Information Security Officer to review timelines and procedures in the current DLP process and adopt a risk-based approach to conducting DLP analysis.	March 31, 2021		Yes	Open
9	SEPS established a strategic plan to address the PR case workload in August 2020. The plan has been implemented and utilizes the new eWorks to ensure PRs are being initiated in a timely manner as required by Federal Regulations. SEPS will provide a progress report to the Chief Operating Officer that summarizes the PRs ordered and completed each quarter.	April 30, 2021		Yes	Open
10	SEPS is developing quality assurance and quality control procedures for staff and contractors to ensure investigative data are accurate and complete prior to initiating the required BIs. SEPS will provide a progress report to the Chief Operating Officer that describes the status of corrected investigative case data.	February 26, 2021		Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
11	DOA hired two additional FTEs in September 2020 and hired a third personnel security specialist to fill an existing vacancy to double the PSSP's Federal staff. DOA was recently authorized an additional FTE Management Program Analyst Security Specialist to support PSSP requirements. In addition, DOA recently submitted a reorganization proposal that will improve oversight, create more manageable spans-of-control, and enhance the efficiency of the BI process within SEPS.	January 29, 2021		Yes	Open
12	SEPS will coordinate with ASB and program OMs to validate risk designations for all active contractors.	February 28, 2021		Yes	Open
13	SEPS will work with OMs to initiate appropriate BIs for contractors requiring a BI upgrade based on results of its validation review.	March 31, 2021		Yes	Open
14	SEPS will coordinate with Human Resources Branch (HRB), Classification, AOs, and other Human Resources and program staff at headquarters and regional offices to validate position risk and sensitivity designations for all active employees.	March 31, 2021		Yes	Open
15	HRB and AOs will update CHRIS to reflect position risk level changes.	March 1, 2021		Yes	Open
16	SEPS will conduct an extensive outreach and communications campaign with AOs and OMs to ensure they understand their responsibilities, requirements, and timelines. SEPS will review existing training materials on eWorks position risk level designation processes and update them as required. SEPS will also hold refresher training sessions for AOs, OMs, and human resources staff. Training will also be provided to new eWorks users as part of the eWorks access request process. Updated procedures will also be published on the SEPS website as a resource for program offices.	June 30, 2021		Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
17	On August 31, 2020, SEPS implemented a monthly review of position risk level changes utilizing a CHRIS HR report to verify the change(s) against existing case information within eWorks. SEPS will coordinate with respective AOs and HR Specialists to ensure appropriate updates are initiated.	January 29, 2021		Yes	Open
18	SEPS will establish a risk framework to evaluate aged cases based on the Enterprise Risk Management framework, position risk level, and mitigating factors such as BIs or PRs completed since initial hire date. Assessment results will be documented and presented to the Operating Committee.	February 15, 2021		Yes	Open
19	SEPS will document standardized language of the risk decision within the respective 787 cases in which PBI completion dates were not available.	March 31, 2021		Yes	Open
20	On March 31, 2020, SEPS developed a weekly report to monitor performance metrics, which include PBI processing data points. SEPS also developed a dashboard report to measure case processing compliance with established timelines.	March 31, 2021		Yes	Open
21	SEPS will establish realistic PBI processing goals and reporting will be used to monitor success. SEPS will coordinate with ASB to update the processing timeline requirements within the contract's deliverables.	January 29, 2021		Yes	Open

[a] Recommendations are resolved when —

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.

Federal Deposit Insurance Corporation
Office of Inspector General

3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226

(703) 562-2035

★★★★★★

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our Hotline or call 1-800-964-FDIC.

FDIC OIG website	Twitter	OVERSIGHT.GOV ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE
www.fdicoig.gov	@FDIC_OIG	www.oversight.gov/