The FDIC's Physical Security Risk Management Process

April 2019 **EVAL-19-001**

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 Physical Security Risk Management Process

Given the potential threats against Federal facilities, their employees, contractors, and visitors, the Federal Deposit Insurance Corporation (FDIC) must maintain a robust risk management process for its physical security program. In 1995, President Clinton by Executive Order created the Interagency Security Committee (ISC) in order to issue standards, policies, and best practices to enhance the quality and effectiveness of security in non-military Federal facilities in the United States.[1] The ISC was subsequently placed under the Department of Homeland Security.[2] As the Executive Order required, the ISC was comprised of 60 members, including 21 Federal agencies serving as the primary members and 39 Federal departments servicing as associate members who were selected by the ISC steering committee and Chair. The FDIC, along with other regulatory agencies, including the Federal Reserve Board and the Office of Comptroller of the Currency within the Department of Treasury, are members of the ISC.

The ISC standards represent best practices that were developed by interagency experts and, pursuant to Executive Orders, are applicable to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities. The ISC standards provide a structured methodology for helping to ensure the safety of employees, contractors, and facilities by assessing facility risk, assigning facility security levels, and determining whether implemented countermeasures effectively mitigate risk. The FDIC, in its Circular 1610.1, *FDIC Physical Security Program*, adopted these recommended minimum security standards issued by the ISC for all FDIC facilities where practical.

According to Circular 1610.1, FDIC personnel are responsible for completing critical components of the ISC standards, which include conducting physical security vulnerability assessments in accordance with the ISC standard for facility security levels. Although the Circular did not specifically define which recommended minimum standards were practical to the FDIC, it required that any deviations from the ISC guidelines in Regional, Area, and Field Offices be documented and coordinated with security-related personnel.

[1] Executive Order 12977 (October 19, 1995).
[2] Executive Order 13286 (February 28, 2003).

The FDIC employs approximately 6,000 individuals and has about 3,000 contractor personnel who conduct their work at 94 FDIC-owned or leased facilities throughout the country. Given the FDIC's mission of insuring deposits, examining and supervising financial institutions, making large and complex financial institutions resolvable, and managing receiverships, its facilities house highly sensitive banking and personally identifiable information, mission-critical systems, and valuable equipment. The FDIC must ensure that its employees, contractors, resources, and assets are safe and secure, and following the ISC standards is important to fulfilling this responsibility.

Our evaluation objective was to determine the extent to which the FDIC's physical security risk management process met Federal standards and guidelines.

Results

We concluded that the FDIC had not established an effective physical security risk management process to ensure that it met ISC standards and guidelines. While FDIC management has indicated that there have been no major incidents or threats to any FDIC facility over the past 10 years, we found that the FDIC's physical security risk management process needed improvement. Specifically, the FDIC had not developed adequate policies and procedures, quality control standards, training requirements, or record keeping standards. FDIC officials responsible for the Physical Security Program had not emphasized compliance with the ISC standards, and instead placed priority attention on other security initiatives.

The FDIC frequently did not document its decisions regarding facility security risks and countermeasures, and such decisions were not guided by defined policy or procedure. Instead, FDIC officials relied on a few experienced employees to make important decisions regarding physical security risks and countermeasures at facilities. Without documentation of these decisions, FDIC executives and oversight bodies were unable to fully consider and review the decisions. We found the FDIC did not conduct key activities in a timely or thorough manner for determining facility risk level, assessing security protections in the form of countermeasures, mitigating and accepting risk, and measuring program effectiveness. Collectively, these weaknesses limited the FDIC's assurance that it met Federal standards for physical security over its facilities.

During our evaluation work, we found that the FDIC did not conduct facility security assessments (FSAs) in a timely manner for 58 percent of the FDIC facilities we sampled. In three instances involving high-risk facilities at the FDIC Headquarters locations, the FSAs were delayed almost 2 years. For one of its medium-risk facilities, the FDIC had begun, but had not completed, an assessment more than 2½ years after the FDIC had occupied the leased space. Further, the FDIC's assessments did not adequately address certain risks or countermeasures identified

in the standards, such as those related to information technology, training, child care centers, and facility security plans.

We also found that the FDIC did not adequately address countermeasures or track recommendations for additional minimum security protections. At some facilities, these countermeasures remained outstanding for more than 4 years, and in some cases, the FDIC could not provide the resolution status of recommendations, including those relating to the routine screening of visitors.

In other instances, the FDIC was not able to provide justification for significant expenditures for countermeasures beyond recommended security protections. For example, Division of Administration (DOA) management presented incorrect information to the FDIC's Board of Directors (Board) regarding facility security levels and the justification for additional expenses pertaining to armed security guards. The FDIC's Board relied upon this information in its decision-making to approve the contract for security guards. As of the completion of our fieldwork (March 2018), DOA management had not corrected the errors in the information presented to the FDIC Board. Similarly, the FDIC could not provide documentation to support its decision to install security cameras at certain facilities. The FDIC estimated that by the end of 2018 it would spend $7.1 million on these security guards and cameras. [3]

We further determined that the FDIC did not develop goals and performance measures to help ensure the physical security program was effective. The FDIC also did not have sufficient personnel to perform security risk management activities in a timely manner. Further, the FDIC did not maintain adequate documentation to support decisions to implement countermeasures, or alternatively to accept the risk.

The FDIC needs to develop a consistent documented process for timely establishing and assessing facility security countermeasures and addressing risk mitigation activities at its facilities. Our evaluation did not assess the safety of FDIC personnel and facilities. Nevertheless, without a more robust physical security risk management process, the FDIC cannot be certain that it has taken appropriate and cost-effective measures commensurate with risk and aligned with ISC standards, which are designed to help ensure the safety of its employees, contractors, and facilities.

Recommendations

We made nine recommendations to address the weaknesses in the FDIC's physical security risk management process, including: enhancing policies and procedures;

[3] The costs shown cover the 6-year period 2013 through 2018. DOA management stated that this amount was within delegations of authority to DOA and justification of the procurement decisions did not need to be documented.

implementing quality control practices; training employees; reviewing security level determinations; conducting thorough assessments; tracking recommendations for appropriate countermeasures; documenting risk mitigation alternatives and approvals to accept risk; and establishing performance goals and measures. In a written response to the report dated April 2, 2019 the Chief Operating Officer and Deputy to the Chairman concurred with all nine recommendations. The FDIC plans to complete actions to address the nine recommendations by December 31, 2019.

Contents

Contents

Tables

Figure

April 9, 2019

Arleas Upton Kea, Deputy to the Chairman and Chief Operating Officer

Subject | The FDIC's Physical Security Risk Management Process

The Federal Deposit Insurance Corporation (FDIC) employs approximately 6,000 individuals and has about 3,000 contractor personnel who conduct their work at 94 FDIC-owned or leased facilities[4] throughout the country. Given the FDIC's mission of insuring deposits, examining and supervising financial institutions, and managing receiverships, its facilities house highly sensitive banking and personally identifiable information, mission-critical systems, and valuable equipment. The FDIC must ensure that its employees, contractors, resources, and assets are safe and secure.

Attacks on Federal facilities and their occupants attest to the importance of an effective physical security program.[5] In October 1995, President Clinton established the Interagency Security Committee (ISC) in response to the Oklahoma City Federal building bombing.[6] The ISC issues standards, policies, and best practices to enhance the quality and effectiveness of security in non-military Federal facilities. The ISC developed risk-based standards for identifying, assessing, and prioritizing risks to Federal facilities. The standards provide a means for making informed decisions to identify and implement cost-effective countermeasures for mitigating vulnerabilities and thus reducing risks. The ISC standards and best practices were developed by interagency experts and are followed throughout the Federal government. By serving as a member of the ISC, the FDIC demonstrated a commitment to developing these standards as best practices. In February 2012, the FDIC adopted the ISC standards for all of its facilities where practical.

We conducted an evaluation to determine the extent to which the FDIC's physical security risk management process (RMP) met Federal standards and guidelines. According to *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (November 2016 2nd Edition) (ISC RMP Standard), an

[4] Certain terms that are underlined when first used in this report are defined in Appendix 4, *Glossary*.
[5] The Federal Protective Service reported 737 workplace violence incidents from 2012 to 2016 at the Federal facilities that they protect. The Federal Bureau of Investigation reported 7 active shooter incidents from 2014 to 2017 at non-military government properties, resulting in 12 killed and 19 wounded. Division of Administration (DOA) management indicated that during this same period, the FDIC did not experience any active shooter or serious workplace violence incidents.
[6] Executive Order 12977 (October 19, 1995), as amended by Executive Order 13286 (February 28, 2003), which placed the ISC under the United States Department of Homeland Security.

agency's physical security RMP is intended to uncover threats, identify related vulnerabilities, and recommend protective countermeasures to mitigate risk. Of note, the ISC's primary members concurred in their approval of the standard. To address our objective, we reviewed the results of the FDIC physical security RMP activities performed during the period 2011 through September 2017[7] for a judgmental sample of 26 of 94 FDIC facilities across the United States.

We conducted this evaluation in accordance with the *Quality Standards for Inspection and Evaluation* of the Council of the Inspectors General on Integrity and Efficiency.

BACKGROUND

The ISC's mission is to safeguard nonmilitary Federal facilities from all hazards by developing state-of-the-art security standards in collaboration with public and private homeland security partners. The ISC is comprised of more than 100 senior level executives from 60 Federal agencies and departments. ISC members, including the FDIC, serve on subcommittees and working groups[8] to develop physical security policies and standards, promote key management practices, and facilitate mitigation of threats to employees and the visiting public. The ISC also engages with industry and other government stakeholders to advance best practices.

According to the ISC's *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide* (December 2015) (ISC Best Practices), implementing effective physical security helps protect an agency from adverse actions by aggressors who mean to do harm. The ISC has identified five main objectives of aggressors:

- Instilling fear in victims;
- Inflicting injury or death;
- Destroying or damaging facilities, property, equipment, or resources;
- Stealing equipment, material, or information; and
- Creating adverse publicity.

According to the ISC Best Practices, an agency should determine aggressor types (e.g., criminals, protesters, terrorists, etc.) and associated tactics (e.g., explosives/incendiary devices, unauthorized entry, surveillance, etc.) for its mission or assets and analyze the threats these assets face from those aggressors and their

[7] As new information became available, we expanded our evaluation to include a review of certain documents. We did not perform any independent physical security testing as part of our evaluation work.
[8] The FDIC participated in the ISC's Facility Security Level Determination Working Group and the Facility Security Committee Working Group.

tactics. Security assessments enable the agency to reduce security threats by deploying the most appropriate security measures, countermeasures, and policies designed to protect facilities, people, and information systems from undesirable events.

The ISC RMP Standard identifies 33 undesirable events that may impact Federal facilities, such as assault, arson, or an active shooter, and organizes them into nine categories: Criminal Activity; Explosive Events/ Incendiary Device; Ballistic Attack; Unauthorized Entry; Chemical/ Biological/ Radiological Release; Vehicle Ramming; Hostile Surveillance; Cyber Attack; and Adversarial Use of Unmanned Aircraft Systems (see Appendix 6).

The ISC RMP Standard defines the criteria and processes that those responsible for a facility's security should use in determining its security level. It provides an integrated, single source of physical security countermeasures and guidance on countermeasure customization for all nonmilitary Federal facilities. Pursuant to the authority of the ISC contained in Executive Order (E.O.) 12977, *Interagency Security Committee* (October 19, 1995), and as amended by E.O. 13286 (February 28, 2003), the ISC RMP Standard is applicable to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities. Therefore, it makes good business sense for all Federal agencies, including the FDIC, to follow these standards.

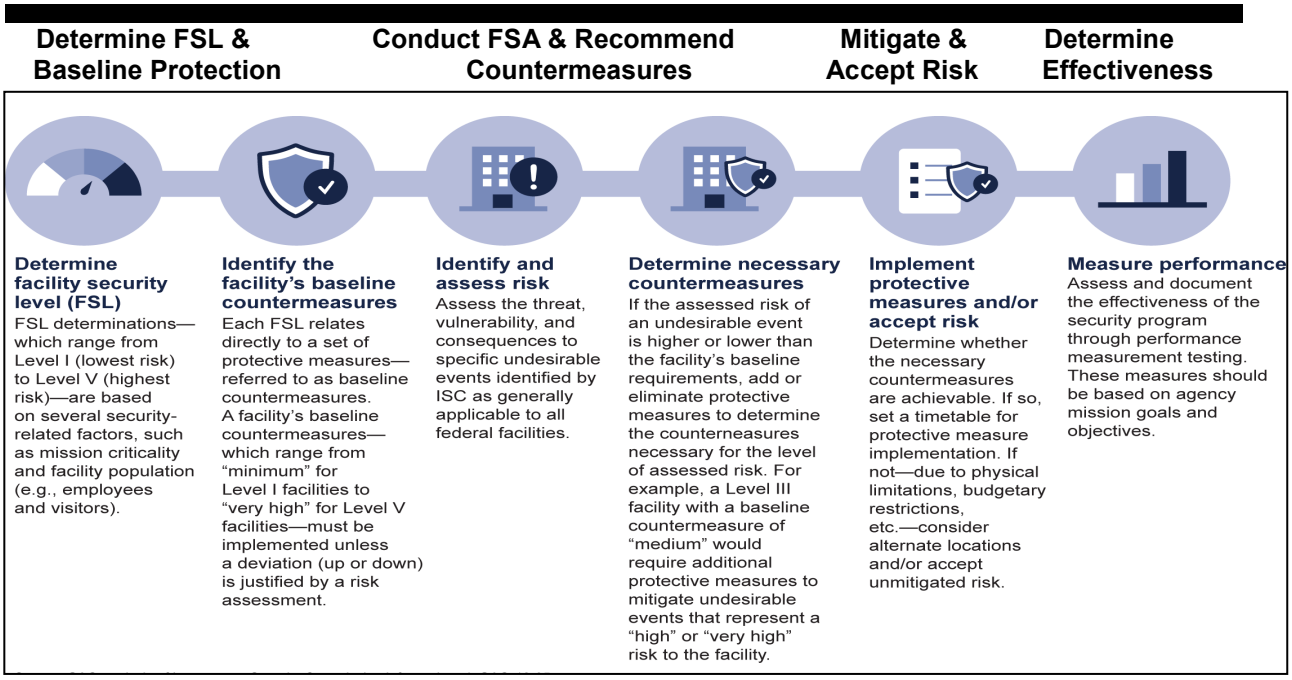
The Physical Security Risk Management Process

As depicted in the Figure below, the ISC RMP Standard involves the following key steps:

(1) Determining the facility security level (FSL) and identifying the corresponding baseline level of protection;
(2) Conducting a facility security assessment (FSA) that identifies and assesses the risk of undesirable events and recommends needed countermeasures;
(3) Deciding whether to implement countermeasures to mitigate risk or to accept the risk of delaying or foregoing implementation; and
(4) Determining the overall effectiveness of the security program.

We used this standard as the primary basis for evaluating the FDIC's physical security RMP.

Figure: Summary of the ISC Risk Management Process



Source: Office of Inspector General (OIG) adaptation of the Government Accountability Office (GAO) analysis of ISC information from GAO Report 18-72, *Federal Facility Security: Selected Agencies Should Improve Methods for Assessing and Monitoring Risk* (October 2017).

The FDIC's Physical Security Program

On February 9, 2012, the FDIC issued its Circular 1610.1, *FDIC Physical Security Program*. The FDIC adopted the "recommended minimum security standards adopted by the Interagency Security Committee (ISC) (a group created pursuant to Executive Order 12977, dated October 19, 1995) . . . for all FDIC facilities where practical."[9] The Circular directed FDIC personnel to complete critical components of the ISC standards, which included conducting physical security vulnerability assessments in accordance with the ISC standard for facility security levels.

The Circular further stated "the provisions outlined in this directive apply to all FDIC employees, contractors, visitors, and others who have access to FDIC facilities and encompass a variety of physical security areas including employee and manager responsibilities, access control, reporting of security related incidents or suspicious activity, and security alert procedures."

The Circular also stated "the application of standards and measures referred to in this directive may not be necessary or feasible for implementation at all FDIC facilities. The DOA Facilities Specialist/Security Manager having responsibility for the local security program at each FDIC facility shall, in consultation with the DOA Regional Manager and DOA, Corporate Services Branch (CSB), Security and

[9] These standards are now included in the ISC RMP Standard.

Emergency Preparedness Section (SEPS) determine and document when adjustments to physical security safeguards and procedures are necessary."

The Circular did not define which recommended minimum standards were considered to be practical and which were not. It did not identify criteria or standards by which to evaluate and make such determinations.

Consistent with the ISC standards, the Circular outlined physical security program activities and assigned overall responsibility for these to the Division of Administration. DOA personnel carried out these responsibilities in Headquarters, regional, and remote worksites, by:

- Overseeing physical security-related contracts;
- Coordinating the maintenance and operation of security equipment and systems;
- Determining FSLs;
- Conducting FSAs; and
- Serving as the primary physical security liaison for the FDIC.

SEPS, based at the FDIC Headquarters, is responsible for ensuring the security of all 94 FDIC-owned and leased facilities[10] housing approximately 9,000 employees and contractors. The Assistant Director of SEPS is responsible for physical security risk management. At the time of our evaluation, SEPS had four physical security specialists who carried out physical security risk management activities, with assistance from DOA facilities operations specialists in the FDIC Regional and Area Offices. SEPS staff, supported by contractor personnel, performed the FSAs of the Headquarters, Regional, and Area Offices. One or more DOA facilities operations specialists from each FDIC Regional Office performed the FSAs of the Field Offices.

FDIC Facilities & Occupants

The FDIC's 94 facilities include:

- 6 Headquarters Offices in the Washington, DC area,
- 6 Regional Offices,
- 2 Area Offices,
- 80 independently located Field Offices across the nation.

The FDIC owns 4 of these offices and leases the remaining 90 offices.

As of June 30, 2018, these facilities housed almost 9,000 FDIC employees and contractors. At that time 1,947 employees worked in the Headquarters Offices. Regional, Area, and Field Offices primarily support the FDIC's examination function with 4,123 employees. In addition, about 2,947 contractors had access to FDIC facilities.

[10] The FDIC uses a contractor-owned facility to house its disaster recovery data center. Physical security for this facility is the contractual responsibility of the contractor and is assessed periodically by the FDIC Information Security and Privacy Staff (ISPS). ISPS personnel indicated there are no FDIC employees regularly onsite at this facility.

In addition, the FDIC hired four primary contract companies to provide personnel and technology services in support of its physical security program:

- Armed security officers at the Headquarters, Regional, and Area Offices,[11] and assistance with FSAs;
- Installing, monitoring, and repairing electronic security systems (ESS) at the Headquarters, Regional, Area, and Field Offices;
- Network services used to transmit ESS data; and
- Personnel and other services to support the FDIC's physical access control program.

In 2018, the physical security program budget for the FDIC was approximately $24.6 million. Approximately $20.9 million was allocated to the annually recurring costs of these contracts, and approximately $3.7 million was for one-time security enhancements, such as upgrades to the ESS, new vehicle barriers, and other physical security equipment. Table 1 summarizes the DOA budget for 2018 physical security program costs.[12]

Table 1: Physical Security Program – DOA Budgeted Costs for 2018

Service	2018 Budgeted Cost
Security Guard Force	$17,000,000
ESS Monitoring and Maintenance	$1,449,381
ESS Network	$793,640
Access Control Program and Other Support Services	$1,687,425
Security Enhancements	$3,655,000
Total	**$24,585,446**

Source: OIG summary of 2018 budgeted cost information provided by DOA SEPS.

THE FDIC DID NOT ESTABLISH AN EFFECTIVE PHYSICAL SECURITY RISK MANAGEMENT PROCESS TO ENSURE IT MET FEDERAL STANDARDS AND GUIDELINES

ISC standards contain best practices for implementing effective physical security, as identified by experts, and are widely followed by government agencies. Fundamental to the FDIC's physical security risk management process was FDIC

[11] The FDIC does not provide security guard services at standalone FDIC Field Offices that have FSL I – Minimum or FSL II – Low risk ratings, which constitute all standalone Field Offices. As determined by the ISC RMP Standard, FSL I and FSL II facilities do not require security officers.

[12] Another FDIC contractor assesses certain physical security countermeasures at the six FDIC Headquarters facilities every 3 years as part of the FDIC's Information Security and Privacy Support Services contract. The FDIC Chief Information Officer Organization manages the contract and therefore we did not show the costs for that contractor in Table 1. The contractor uses guidelines established by the National Institute of Standards and Technology (NIST) to assess physical security countermeasures such as controlling physical access to a building and to restricted areas within a building, with the objective of protecting information systems and applications.

Circular 1610.1, which clearly stated the program goal of protecting its employees, visitors, and facilities from internal and external threats (for example, fire, theft, vandalism, and other security concerns) and preventing, detecting, and investigating security incidents.

We found that the FDIC had not established an effective physical security risk management process to ensure that it met ISC standards and guidelines. Without policies and procedures that clearly define the roles and responsibilities for key physical security risk management activities and identify which ISC standards are practical, the FDIC has less assurance that its physical security program is operating in an efficient and effective manner. In our assessment, the FDIC lacked the necessary policies, procedures, quality controls, training, and records management to ensure that key ISC standards for effective physical security were followed. Instead, FDIC officials relied on a few experienced employees to make important decisions regarding physical security risks and countermeasures at facilities. Without documentation of these decisions, FDIC executives and oversight bodies were unable to fully consider and review the decisions. We identified that the FDIC did not conduct key activities for determining facility risk level, assessing security protections in the form of countermeasures, mitigating and accepting risk, and measuring program effectiveness. Our evaluation did not assess the safety of FDIC personnel and facilities. However, the weaknesses we identified limited the FDIC's assurance that it met Federal standards for physical security over its 94 facilities that protected 9,000 employees and contractors.

Policies and Procedures Did Not Define Roles and Responsibilities and Explain How and When ISC Standards Would Be Followed

FDIC Circular 1610.1 for the FDIC's physical security risk management process did not clearly define specific roles, responsibilities, and levels of authority for key management decisions. For example, the Circular stated that FDIC should adopt the ISC recommended minimum security standards "where practical," yet the Circular did not establish roles and responsibilities for determining, justifying, approving, and documenting FDIC decisions related to where the security standards were or were not practical. Specifically, the Circular did not clearly describe who was authorized to make such decisions, at what level of seniority within the FDIC, nor how such decisions should be recorded. The Circular did not provide direction as to when to involve Legal counsel or senior FDIC management in such decisions. As a result, it was unclear who had the authority to make decisions regarding the applicability and execution of the physical security standards.

Further, the policy did not define the specific roles and responsibilities of each group for conducting FSL determinations and FSAs, and did not include roles and responsibilities for:

- Quality review of FSL determinations and FSA results, including who was responsible for reviewing, accepting, and making decisions based on the results, and how the quality reviews should be documented;

- Risk mitigation and acceptance activities, to ensure risk mitigation or acceptance decision-makers were clearly identified and were at an appropriate management level and independent of the assessment function, and decisions were documented; and

- Performance measurement activities that would lead to program improvement.

The Circular also did not provide guidance for making decisions related to what government-wide ISC standards would be practical, or impractical. Moreover, the FDIC had not developed physical security risk management procedures to implement the Circular's requirements beyond certain FSL and FSA templates and FSA report documents. While these templates and documents provided some general guidance for performing risk management process activities, the FSL and FSA exceptions we identified below indicated that these guidance documents were not adequate.

Security Assessments Were Not Subjected to Proper Quality Control Review

Based on our review of Federal internal control standards,[13] reasonable quality control practices for security assessments should have included:

- Supervisory review prior to acceptance of the FSL determination and of the FSA;

- Acceptance by the designated representative[14] of the FSL determination before the security organization conducted the FSA; and

- Periodic review of the schedules of dates for FSL determinations and FSAs for accuracy.

DOA personnel did not consistently perform and document quality reviews of the accuracy and completeness of FSL determinations, FSA reports, and/or FSA templates. Assessments for 50 percent of our sampled facilities (13 of 26) did not have evidence of a quality review.

[13] GAO Report 14-704G, *Standards for Internal Control in the Federal Government* (September 2014)
[14] According to the ISC RMP Standard, a representative designated by the agency, such as the agency Director of Security, in consultation with the security organization, should make all final FSL determinations to ensure consistency.

In addition, a change in the most recent FSL for two sampled facilities, between FSL II and III, had a significant impact on the extent and nature of the baseline countermeasures that needed to be assessed for each facility. Specifically, the FSL for one Headquarters facility decreased from III to II, indicating fewer countermeasures should be assessed for the facility, while the FSL for one Regional Office increased from II to III, indicating additional countermeasures should be assessed for the facility. However, there was no evidence that a designated FDIC representative reviewed and accepted the revised FSL as accurate and complete before FDIC or contractor personnel conducted the related FSA. Such a review would help ensure that the appropriate countermeasures are assessed in the FSA.

Assessment Personnel Lacked Sufficient Training

FDIC position descriptions for Headquarters physical security specialists required staff to have the knowledge, skill, and ability to perform physical security risk management activities. However, other FDIC and contractor personnel who performed security assessments did not have sufficient training. At a minimum, the FDIC should ensure that these personnel enroll in training courses regarding the risk management process offered by the ISC.

For example, contractor personnel that the FDIC hired to perform FDIC Headquarters FSAs did not have sufficient training on the ISC standards to properly perform these activities. As a result, the FSA documents that the contractor had submitted in 2017 and 2018 were inaccurate and incomplete, thus requiring additional FDIC and contractor resources to correct and complete. Moreover, we found that 7 of 9 FDIC Regional Office personnel who performed FSL determinations and FSAs in the 12 sampled Field Offices had not received recent ISC or FDIC training related to these activities.

If the assessors do not have sufficient training practices, the FSL determinations and FSA products may be inaccurate or incomplete. Thus, the FSLs and FSAs may not properly identify or mitigate risks to FDIC personnel and facilities. Absent training, the assessors may not determine the appropriate FSL and therefore may not properly identify and assess the appropriate set of baseline security countermeasures for a facility.

Recordkeeping Controls Were Ineffective

We found that the FDIC's physical security risk management process records, both hard copy and electronic, were incomplete and disorganized, reflecting poor recordkeeping controls. FDIC Circular 1210.1, *FDIC Records and Information Management (RIM) Policy Manual* (June 2, 2016) stated that "it is fundamental that all business records, created or collected by the FDIC in the course of conducting

business, are properly maintained and protected from damage, misuse, or improper disposition."

Specifically, we found that DOA personnel were unable to locate hard copy assessment files for two Headquarters facilities, two Regional Office facilities, and one Area Office facility. In addition, electronic files did not consistently contain the final signed versions of assessment documents. It was unclear what constituted the official records of the assessment process.

Proper documentation provides FDIC employees and contractors with timely and reliable access to needed records and information, and helps protect the legal and financial rights of the FDIC. In addition, effective recordkeeping controls help retain important historical program knowledge when there is turnover in key program personnel and management, such as SEPS experienced during 2016 and 2017.[15]

FDIC Circular 4010.3 *FDIC Enterprise Risk Management* (April 16, 2012) mandated these basic controls by requiring that FDIC management establish and implement the following fundamental requirements for every operating and policy area in the FDIC:

(1) Procedures that are both current and appropriately documented;
(2) Reasonable controls that have been incorporated into those procedures;
(3) Employees who have been trained in the proper execution of their duties; and
(4) Supervisors and managers who are both empowered and held accountable for performance and results.

Facility Security Levels Were Not Adequately Determined or Supported

The physical security risk management process begins by assigning an FSL that reflects the relative value and risk of a facility (from minimum to very high), and helps determine the best means of protecting that facility. The ISC RMP Standard establishes the FSL using a point system based on five primary factors (mission criticality, symbolism, facility population, facility size, and threats). An agency determines the preliminary FSL from the total of the points assigned to each of these five factors, and may adjust it by a one-level increase or decrease after considering a sixth factor, "intangibles," to determine the final FSL. Intangibles are circumstances unique to the facility or agency needs. As examples, the ISC RMP Standard notes that a short duration of occupancy may reduce the value of the facility in terms of investment or mission, which may justify an intangible adjustment to decrease the FSL one level. Alternatively, proximity to higher risk facilities, such as the White

[15] Three SEPS employees with physical security-related responsibilities and program knowledge resigned or retired in the 10-month period from September 2016 to July 2017. In addition, the Assistant Director of SEPS position was filled in an acting capacity during the majority of 2017.

House, may increase the risk to a facility, which may justify an intangible adjustment to increase the FSL one level.

Table 2 shows the relationship between the FSL and the facility's estimated level of risk and baseline level of protection.

Table 2: Relationship Between FSL, Level of Risk, and Level of Protection

FSL	V	IV	III	II	I
Level of Risk/ Level of Protection	Very High	High	Medium	Low	Minimum

Source: ISC RMP Standard

Complete, supported, and accurate FSL determinations help the FDIC ensure it has appropriate security countermeasures for its facilities.

FSL Determinations Were Not Always Completed, Accurate, or Sufficiently Supported

The FDIC recorded the FSL determination using an FSL template document that included the factors identified in the ISC RMP Standard. Together, these factors help determine a facility's potential as a target for threats, consider the severity of consequences of adversarial acts, and establish a commensurate level of risk and level of protection for the facility. According to the ISC RMP Standard, an agency should document the rationale for each factor and retain this information as part of the official facility security records. However, the FDIC did not consistently complete the FSL template with documented support for each factor, and did not always calculate the FSL accurately.

We found that there were omissions, inaccuracies, or insufficient support for the FSL determinations we reviewed for 11 of 26 (42 percent) sampled facilities:

- For two facilities, the FDIC could not provide a completed FSL template for the most recent security assessment and, therefore, neither FSL for these field office facilities was documented. As a result, the FDIC did not know what level of protection was appropriate for these facilities.

- For four facilities, the FDIC may have set the FSL at a lower level than it should have been because it either did not increase the FSL for intangibles or did not assign the accurate FSL based on the total score. An FSL that is too low can lead the FDIC to establish a baseline level of protection that does not adequately mitigate security risk to employees and contractors working in that facility.

- For five facilities, the FDIC may have set the FSL at a higher level than it should have been based on the available supporting documentation. An FSL that is too high can lead the FDIC to establish a baseline level of protection higher than the facility would otherwise have merited, which could bring into question the cost-effectiveness of security enhancements.

Table 3 provides additional details of the 11 FSL determinations that were incomplete, inaccurate, or insufficiently supported that we identified, and their impact on the FSLs for the affected facilities.

Table 3: Incomplete, Inaccurate, or Insufficiently Supported FSLs

Number of Facilities	Office Type	Discrepancy	Impact on the FSL
		2 Incomplete FSLs	
2	Field Offices	No completed FSL template.	Unknown.
		4 Inaccurate FSLs	
2	Headquarters	FSL was not increased for intangibles.[a]	Lowered 1 FSL from III to II, no impact on the other.
1	Regional Office	FSL was not increased for intangibles.	Lowered FSL from IV to III.
1	Field Office	FSL assigned was inaccurate based on the total FSL score.	Lowered FSL from II to I.
		5 Insufficiently Supported FSLs	
1	Headquarters	Intangible adjustment to increase the FSL was insufficiently supported.	Raised FSL from III to IV.
3	Field Offices	High mission criticality score was insufficiently supported. [b]	Raised 2 of 3 FSLs from I to II, no impact on the third.
1	Field Office	High symbolism score was insufficiently supported. [c]	Raised FSL from I to II.

Source: OIG analysis of the FDIC's FSL templates.
[a] Intangibles are discussed on page 12 of this report.
[b] Most of our sampled Field Offices had a low or medium mission criticality score.
[c] Most of our sampled Field Offices had a low symbolism score.

Facility Security Assessments Were Not Always Completed or Timely

After determining the FSL for a facility, the agency conducts an FSA to identify and assess risks to a facility in order to determine (1) whether the baseline level of protection is sufficient or (2) adjustments or customization of the protective countermeasures are needed. In addition to assessing risk, an FSA reviews the countermeasures established for a facility, and identifies any missing or incomplete countermeasures. The resulting FSA report documents the facility risks and the sufficiency of countermeasures. It highlights recommendations for enhancing the level of protection if it is too low, or reducing the level of protection if it is too high. The FDIC developed a standard FSA template document to use for all FDIC facilities, regardless of the FSL. The FSA template contained a list of questions

designed to identify risks to the facility and to determine whether a specific set of security countermeasures were in place. The FDIC also developed a standard FSA report document for Headquarters, Regional, and Area Offices, to summarize the information captured on the FSA template, and to document any recommendations. However, DOA personnel did not adequately revise the FSA template and report to incorporate all current and relevant risk assessment and countermeasures guidance in the ISC RMP Standard.[16]

FSA Risk Assessments of Undesirable Events Were Incomplete

The ISC RMP Standard recommends that the agency security organization conduct accurate and complete risk assessments, and present credible and documented FSAs to the agency decision-making authority for acceptance. The ISC RMP Standard advises that the methodology to assess risk should adhere to fundamental principles. The methodology should be:

- Credible and assess the threat, consequences, and vulnerability to specific undesirable events;
- Reproducible and produce similar or identical results when applied by various security professionals; and
- Defensible and provide sufficient justification for deviation from the baseline.

The ISC RMP Standard identifies 33 undesirable events that may impact Federal facilities, such as assault, arson, or an active shooter, and that an agency must consider when assessing risks to its facilities. Undesirable events are incidents that have an adverse impact on the facility occupants or visitors, operation of the facility, or mission of the agency. An agency should review its list of undesirable events as updates to the ISC RMP Standard occur and document justifications for not considering any undesirable event during its risk assessments.

We found that the FDIC did not have a documented risk assessment methodology, and the FDIC's FSAs did not consistently document that the FDIC considered all the undesirable events in the ISC RMP Standard. The FDIC also did not fully assess the three components of risk—threat, vulnerability, and consequence—for these undesirable events.

[16] Based on our interviews of physical security personnel at other Federal agencies, we believe the use of a more comprehensive automated template or tool for conducting and documenting FSAs and tracking FSA results is a best practice.

The risk-related questions in the FSAs generally focused on gathering local information related to undesirable events in the criminal activity and unauthorized entry categories, including questions about the area crime rate, neighborhood composition, and recent incidents of theft, vandalism, and other crimes at or near the facility. The risk assessments did not adequately cover the risks of other categories of undesirable events, such as explosive events, cyber attack, and hostile surveillance. In other instances, the FSA was incomplete because it did not recommend countermeasures to address identified risks.

Examples of Incomplete Risk Assessments of Undesirable Events

- Three FSAs assessed the vulnerability of the facility garages to a vehicle-borne explosion but did not assess the likelihood of the threat or the potential consequences to support a resulting recommendation to add garage barriers at the facilities.
- One FSA determined that pedestrian lobbies were vulnerable to ballistic attack but did not include a recommendation to add ballistic protection, a minimum standard.
- Two FSAs identified the risk of a vehicle-borne explosion at the facility's pedestrian entrance or at street level, but did not include a recommendation to add vehicle barriers in these locations, another minimum standard.

FDIC management asserted that it evaluated undesirable events in completing its risk assessments, and the security countermeasures at FDIC facilities reflect decisions made based on its risk assessment process. However, management was not able to provide any evidence to support its contention that it appropriately considered all undesirable events and departures from the ISC standards were sufficiently justified. Absent such support, the FDIC cannot demonstrate the credibility of its assessments and whether appropriate security countermeasures have been effectively and efficiently deployed at its 94 owned or leased office facilities.

FSAs Did Not Address Important Countermeasures

The ISC RMP Standard establishes 93 security criteria and related countermeasures to mitigate the risks posed by the undesirable events. The higher the FSL, the higher the number of applicable security criteria and related countermeasures that should be in place at the facility and assessed during the FSA. For example, all 93 security criteria apply to an FSL V facility while only 30 apply to an FSL I facility. (*see* Appendix 7 for examples of the 93 security criteria, by category.) Similarly, the higher the FSL, the stronger are the countermeasures that should be in place to protect the facility from risks.

We found that important ISC-recommended minimum security countermeasures were either not in place at a facility or had not been adequately assessed. For example:

Security System Testing. According to the ISC RMP Standard, the agency should conduct operational performance tests of security systems, such as closed-circuit television (CCTV), at least annually, including recording testing results, and repairing or replacing malfunctioning equipment as needed. During our review, we found that FDIC physical security staff or contractors only performed security system testing on an ad hoc basis, not annually as recommended by the standards. Further, we identified that one of the three Field Offices that we visited retained video for 18 days rather than the ISC-recommended minimum standard of 30 days.

Security System Maintenance. According to the ISC RMP Standard, the agency should conduct periodic preventive maintenance of its security systems to replace critical components that become inoperable within certain timeframes that vary based on the FSL. During our review, FDIC physical security staff stated that the FDIC had not established such a program, focusing instead on repairing security system equipment as it breaks rather than proactively replacing it. As a result, security controls may not be effective during the repair period, when equipment is not functioning.

Cyber Security of Building Access and Control Systems (BACS).[17] ISC Best Practices guidance emphasizes that integrating physical and information security is a key element to managing and planning physical security resources. The agency should implement controls that, among other things, identify BACS devices and networks, establish and maintain BACS configuration management, manage BACS access points, and establish incident response processes for BACS. During our review, FDIC physical security staff stated that they had not coordinated with FDIC information technology personnel to ensure such cyber security controls were in place and documented during the FSA. As a result, FDIC personnel may not be aware of vulnerabilities which could allow these systems to be compromised and used inappropriately.

Physical Security Awareness Training Program. According to the ISC RMP Standard, the agency should conduct annual physical security awareness training, which may include topics such as security policies and procedures, workplace violence, general crime prevention, security incident reporting, and active shooter response. During our review, FDIC physical security staff stated that the FDIC had not developed and implemented an annual physical security awareness training program.

Child Care Center (CCC) Protection. According to the ISC RMP Standard, the agency should assess all relevant CCC-specific countermeasures designed to

[17] BACS include the electronic security systems plus other systems involved in building control, as described in more detail in Appendix 4, *Glossary*.

protect children on site at Federal facilities. During our review, we noted that the FSA reports for the two FSL IV FDIC Headquarters facilities with a CCC had documented countermeasures for access control and the placement of CCTV cameras. However, we found that these FSAs did not demonstrate that the FDIC had tested other potentially relevant CCC-specific countermeasures that could alert security guards and CCC personnel of, or provide time to respond to, incidents that may cause harm to children. These countermeasures include duress alarm buttons within the CCC to call for help in emergency situations and delayed opening of emergency exit doors to prevent children from leaving without an authorized escort. Subsequent to our fieldwork, DOA personnel provided duress button monitoring logs for 2018 and informed us that the duress buttons are monitored and tested.

Facility Security Plan (FSP). According to the ISC RMP Standard, the agency should develop, and annually review and update, an FSP for each facility that addresses security system testing and maintenance procedures, collaboration with the Chief Information Officer to ensure cyber security of BACS, physical security awareness training, and building-specific security policies, such as those related to on-site child care centers. The ISC indicates that the FSP is a critical component of an effective security program.[18] During our review, we found that the FDIC did not prepare an FSP for any of its facilities. As a result, FDIC personnel responsible for physical security may not know of the security measures at a facility and therefore may not be able to respond as effectively when undesirable events occur.

FSL Determinations and FSAs Were Outdated

Initial FSL Determinations and FSAs Not Conducted in a Timely Manner. The ISC RMP Standard indicates that an agency should conduct the initial FSL and FSA for newly leased or owned space as soon as practical after it identifies space requirements. An agency should act early enough in the acquisition of leased space to allow it to implement baseline protective countermeasures, or reconsider occupying the space if the agency cannot meet recommended minimum physical security standards. The FDIC leasing policy indicated that, during the pre-lease planning process, SEPS personnel would perform vulnerability assessments and advise leasing specialists on security requirements for new leased space as required.[19] However, the FDIC physical security program policy omitted such requirements for the FDIC's 90 leased facilities.

The FDIC moved into 13 leased facilities in our sample within the last 8 years. For 7 of these sampled leased facilities (54 percent), the FDIC could not demonstrate

[18] *Facility Security Plan: An Interagency Security Committee Guide* (February 2015).
[19] *FDIC Leasing Policy Manual*, Circular 3540.1 (July 13, 2004), and *FDIC Space Utilization Policy*, Circular 3010.2 (October 24, 2008).

that it had conducted FSL determinations and FSAs in a timely manner.[20] The delays in the initial FSL determination and FSA ranged from 6 to 35 months after the FDIC had occupied the facility. One of the longest FSA delays related to an FSL III Headquarters facility that housed approximately 400 FDIC employee and contractor personnel as of December 2017. FDIC management could not demonstrate that it had properly conducted nor reported its risk management for this facility.[21]

FSL Determinations and FSAs Not Updated on a Timely Basis. The ISC RMP Standard recommends an agency update FSL determinations and FSAs at least once every 5 years for FSL I and II facilities and at least once every 3 years for FSL III, IV, and V facilities. Untimely updates can delay identification of, or revision to, the appropriate baseline level of protection for a facility.

The FDIC did not consistently update FSL determinations and FSAs within the recommended timeframes for FSL III and IV facilities. Based upon our review of the FDIC's June 2017 tracking schedule of FSL determinations and FSAs for the 14 Headquarters, Regional, and Area Offices, we found that there were delays for five of the six Headquarters facilities and for four of the eight Regional and Area Offices as of July 31, 2017. DOA should have updated most of the delayed FSL determinations and FSAs in 2015 or 2016. DOA had not informed FDIC senior management of the delayed FSL determinations and FSAs. As of September 30, 2017, the FDIC had updated FSL determinations and FSAs timely for 10 of 12 sampled Field Offices.

On August 9, 2017, we issued a Management Memorandum to the DOA Director that noted our significant concerns about the delays in conducting the FSAs[22] at high-risk FDIC facilities,[23] an issue warranting urgent attention. Our concerns included:

- Non-compliance with the ISC RMP Standard, which had the potential to expose the FDIC workforce, visitors, and facilities to security risk.
- Security changes since the prior FSAs that had not yet been assessed.
- Deficiencies previously identified at FDIC facilities that had been outstanding for more than 4 years with no formal risk acceptance by the FDIC.

[20] See Appendix 8 for details by sampled facilities. Of note, 6 of the 7 facilities were FSLs I and II, or lower risk facilities.
[21] DOA personnel initiated an FSA of this facility in June 2015, shortly after the FDIC occupied the facility, but never completed it. DOA personnel began a new FSA of this facility in 2017 and DOA management indicated that it approved the FSA in April 2018.
[22] At the time of the memorandum, we used the term "physical security assessment (PSA)" to refer to an FSA.
[23] OIG memorandum, *Concerns Related to FDIC Physical Security Assessments* is located at Appendix 2 of this report.

- A decision to delay the FSAs that DOA had not discussed with other FDIC senior management.

In a response dated September 27, 2017,[24] the Director stated that the FDIC would complete the delayed FSAs by year end 2017. DOA management indicated that as of April 30, 2018, the FDIC had performed and approved the FSAs on 8 of the 9 facilities with delays. The FSA for one Area Office was planned for 2018.

Of particular significance, the outdated 2012 FSL for one facility indicated that the facility was FSL IV, which would warrant vehicle barriers and ballistic protection at the garage entrance. In late 2017, the FDIC began to implement these additional countermeasures at a cost of approximately $400,000. The FDIC subsequently updated the FSL determination for this facility in February 2018 and concluded that the facility was FSL III, for which vehicle barriers and ballistic protection at the garage entrance are not minimum standards. Had FDIC personnel conducted a timely assessment in 2015 and assigned the facility an FSL III at that time, the FDIC may not have elected to expend the funding to add vehicle barriers and ballistic protection at the garage entrance to the facility.

FDIC management noted that the Headquarters FSAs conducted in 2012 and 2013 identified a number of deficiencies that required significant funds and time to mitigate, and the related physical security enhancements were ultimately targeted for implementation in late 2017. FDIC management did not begin to update the Headquarters FSL determinations and FSAs until the FDIC initiated the enhancements in August 2017. In addition, FDIC management indicated that SEPS had been understaffed, with only two physical security specialists qualified to conduct security assessments. FDIC management postponed FSL determinations and FSAs in favor of assigning these limited resources to other physical security activities, including implementing the personal identity verification (PIV) card program,[25] upgrading the ESS, and developing insider threat and active shooter programs.

Risk Mitigation and Acceptance Lacked Complete, Documented Analysis

Following the completion of the FSA, an agency must determine whether and how the agency will address the unmitigated risk that is present. The ISC RMP Standard cites two key decisions for the agency to consider:

[24] DOA Memorandum, *Management Response to the Office of Inspector General Concerns Related to FDIC Physical Security Assessments* is located at Appendix 3 of this report.
[25] The FDIC designed the PIV card program to address the goals and objectives of Homeland Security Presidential Directive -12, *Policies for a Common Identification Standard for Federal Employees and Contractors* (August 2004).

- Risk Mitigation - Can the necessary level of protection be achieved by implementing recommended countermeasures and is the investment in the countermeasures cost-effective?

- Risk Acceptance - Should the agency accept the risk of not implementing recommended countermeasures?

The ISC RMP Standard recommends an agency clearly document the reason for its decisions, in particular, any decision to accept risk by rejecting or deferring implementation of countermeasures due to cost or other factors. The risk acceptance documentation should outline alternative mitigation strategies considered or implemented, and opportunities in the future to implement needed countermeasures. The ISC RMP Standard notes that risks accepted at a facility may have a bearing on agency-wide risk management efforts and therefore the agency shall provide risk acceptance documentation to the Headquarters security office.

FDIC SEPS personnel could not provide the status of 37 important recommended countermeasures at 10 of our 14 sampled facilities. As a result, they could not provide evidence that the FDIC had either implemented the recommended countermeasures or had accepted the risk for not doing so and documented the reason for its decisions. As noted earlier in this report, updated FSAs for these facilities, which could have provided the status of certain recommendations, had been performed but not approved at the time of our evaluation.

Examples of Important Recommendations with Unknown Status

- Install ballistic protection at lobby screening stations. (2 facilities)
- Install duress alarm buttons at security guard stations. (3 facilities)
- Routinely screen visitors or visitor vehicles. (4 facilities)
- Move trash containers or install blast mitigation measures. (3 facilities)
- Install CCTV cameras at entrances or critical areas. (2 facilities)
- Install position switches on doors at entrances or critical areas. (2 facilities)

The FDIC had not developed a tool, such as an automated worksheet, to identify and track the resolution of recommendations, thus making it difficult for FDIC personnel to determine what recommendations may have been outstanding and therefore represent ongoing security vulnerabilities.

In addition, for our sampled facilities, the FDIC did not consistently document formal risk acceptance for rejected or deferred countermeasures. Such documentation should have included a description of the rationale, proposed alternative mitigations, and plans for future implementation of recommended countermeasures.

Of note, the 2012 FSA report for one sampled FDIC FSL IV Headquarters facility noted that visitors entering through one entrance were not screened and had almost unrestricted access to the entire facility. As a result, visitors could bring harmful or prohibited items (such as contraband or weapons) into the facility undetected, or enter FDIC office space containing sensitive information. FDIC security guards screen visitors at other entrances to this facility by having individuals pass through a metal detector and they screen visitor possessions by passing them through an x-ray machine.

Foreign Visitors

In March 2018, a group of foreign visitors planned to attend a training course at an FDIC FSL IV Headquarters facility. At that time, FDIC personnel did not intend to provide escorts for these visitors while at the facility as required by Circular 1610.1. Because of the continuing vulnerability that allowed all visitors access to the entire facility, we highlighted significant security concerns to the DOA Director about non-citizens having access to FDIC facilities, offices, equipment, and sensitive information without monitoring. DOA management took action to ensure that the foreign visitors were escorted at all times while at the FDIC facility, and indicated DOA personnel would look into options for addressing the physical security vulnerability.

The FSA report recommended the FDIC erect doors, walls, or other barriers to control visitor access to non-public areas within the facility, as well as to provide the ability to isolate sections of the building in the event of contamination. Both of these security enhancements are ISC-recommended minimum countermeasures for this facility. We determined that the FDIC had not implemented the recommendation, and had not documented the rationale or any alternative mitigating controls that it considered.

Further, the FSA reports for three sampled FSL IV Headquarters facilities identified recommended minimum countermeasures for which the FDIC had deferred implementation for years. Specifically, the 2012 FSA reports[26] for these three facilities included significant recommendations to install:

- Vehicle barriers to protect entrances to the garages in these facilities.
- Ballistic protective barriers for the security guard booths.

During the years 2013 through 2016, DOA personnel made several attempts to evaluate these recommendations, but DOA management indicated that other important and Federally mandated physical security priorities and changes in key personnel interrupted these efforts. Ultimately, in December 2016, DOA management presented a proposal to implement the recommended countermeasures to the FDIC Chairman, and received approval to proceed with the

[26] The 2012 FSAs for two of these facilities indicated that the 2008 FSA reports had also included this recommendation.

security enhancements. The FDIC subsequently modified the contract for ESS in August 2017 to implement the vehicle barriers, replace the guard booths, and make other related enhancements for a total of $3.2 million.[27]

However, despite 4 years having passed since the last FSA reports were completed for these three sampled Headquarters facilities, FDIC management did not document an updated risk assessment prior to implementing the countermeasures to determine whether there was a continued need for the countermeasures or whether more cost-effective alternatives existed to mitigate risk. As noted earlier in this report, the updated risk assessment for one of these three facilities (February 2018) indicated a reduced risk level, for which a vehicle barrier at the garage entrance is not a recommended minimum standard. However, as supported by its 2017 budget documents, DOA management stated it wanted to maintain consistent security with other Federal regulators and recently implemented a vehicle barrier at that facility's garage entrance at a cost of approximately $305,000. In addition, at the time of our evaluation, the FDIC was in the midst of updating the risk assessment for another of the facilities, yet was proceeding to implement four vehicle barriers at an estimated cost exceeding $1.2 million.[28]

Further, the ISC RMP Standard indicates that providing security guards with body armor is an acceptable alternative to a ballistic protective barrier. This approach would have come at no additional cost to the FDIC because the security guard contract requires that the contractor provide body armor as part of the basic uniform and equipment for each guard. Instead, the FDIC planned to spend approximately $340,000 for the ballistic protective barriers.

In two cases, DOA management did not adequately document the support or justification for implementing security countermeasures beyond the recommended minimum security standards in the ISC RMP Standard. Specifically:

- Starting in 2013, the FDIC began installing CCTV camera equipment in FDIC Field Offices, which are mostly FSL I facilities, even though CCTV cameras are not an ISC-recommended minimum countermeasure for an FSL I facility. DOA personnel could not provide support for the decision to install and maintain this equipment, including who had made the decision. DOA personnel indicated that the FDIC had spent at least $80,000 on cameras for FDIC Field Offices. Although requested during our evaluation, DOA did not provide us with the total labor and materials costs to install and maintain the CCTV equipment.

[27] The contract modification estimated completion of the vehicle barrier project by March 2, 2018; however, the contractor did not meet this milestone due to technical challenges.
[28] The FDIC updated the risk assessment for the third Headquarters facility in February 2018, resulting in a risk level at which vehicle barriers at garage entrances remain a recommended minimum standard.

- In May 2014, DOA management presented a case to the FDIC Board of Directors (Board) requesting authority to procure a new contract for security guard services. The FDIC Board approved the case and the FDIC executed the contract, which covers all facilities except Field Offices. The contract is effective from November 2014 through December 2019, with a contract ceiling of $75 million. DOA stated that in order to ensure uniformity of services, meet ISC standards, and provide a consistent level of protection throughout the FDIC, then-current unarmed guard posts would be upgraded to armed guard posts under the new contract. In presenting the case, DOA erroneously stated that all of the FDIC's 14 Headquarters, Regional, and Area Office facilities were FSL III or IV, for which armed security guard services are an ISC-recommended minimum standard. In fact, 6 of the 14 facilities were FSL II at that time, for which security guard services of any kind are not an ISC-recommended minimum standard. As a result, we estimated that from 2015 through 2018, the FDIC will have spent about $7 million on armed guard services for FSL II facilities, which exceed the ISC-recommended minimum standard.[29] DOA management could not explain the FSL-related discrepancies in the case, nor could they provide, as of the completion of our field work (March 2018), documentation to support that this presentation to the FDIC Board was corrected and clarified.

Because of the limited documentation of the risk mitigation and acceptance process, we could not determine whether the FDIC had conducted adequate alternative analysis for countermeasures that were implemented. As described above, the FDIC incurred costs to enhance the protection of FDIC personnel without having presented complete and accurate factual information to the FDIC Board.

Procedures and Goals Were Insufficient for Measuring Program Effectiveness

The ISC RMP Standard calls for an agency to assess and document the effectiveness of its security program through performance measurement and testing—a key management practice the ISC is promoting within the Federal physical security community. The agency should base performance measures on agency mission, goals, and objectives, and link performance results to goals and objectives, resource needs, and program management.

In addition, agency leadership must communicate its priority and commitment to performance measurement and ensure that its physical security performance measures enhance accountability, prioritize security needs, and justify investment decisions to maximize available resources. Such measures could include, for

[29] This figure takes into account the impact of FDIC changes to FSLs for two facilities subsequent to the 2014 FDIC Board case.

example, determining whether the FDIC is performing security assessments on schedule. Such a measure indicates management's commitment to maintaining an organized and efficient physical security program. Another example could be determining whether the FDIC is monitoring the countermeasures in use and is regularly testing[30] them to ensure they are working properly. Testing confirms the reliability, or lack thereof, of maintenance programs; ensures credibility with facility occupants; and provides empirical data to support countermeasure replacement, if necessary, all of which help support the conclusion that a facility complies with the ISC RMP Standard.

At the time of our evaluation, the FDIC had not established goals for the physical security program, or procedures for measuring program effectiveness. Regarding information that could be used to measure security program effectiveness:

- The FDIC tracked information regarding the completion dates for FSLs and FSAs; however, this information was often incomplete and inaccurate. Specifically, on the DOA assessment tracking schedules as of September 30, 2017, DOA personnel either incorrectly recorded or omitted the most recent FSL for 5 of 26 sampled facilities and the most recent FSA date for 4 of 26 sampled facilities. The schedules also omitted the FSL for 19 other Field Office facilities that were not in our sample.

- The FDIC performed testing of ESS countermeasures; however, as noted earlier, DOA personnel indicated that the testing was performed on an ad hoc basis, and the FSAs did not summarize the results of such countermeasure testing. In addition, the FDIC did not maintain a comprehensive and accurate inventory of current and newly installed security devices covering all FDIC facilities, which would support countermeasure testing activities. DOA personnel indicated that they had recently begun working with the ESS contractor to develop the FDIC's short-term and long-term inventory requirements and related cost analysis, so that the contractor could provide the inventory contract deliverable.

ISC standards make clear that performance measurement data is essential to appropriate decision-making on the allocation of resources. Without established goals, procedures, and comprehensive data for measuring program effectiveness, the FDIC's ability to prioritize security resources and ensure accountability for the program's overall effectiveness and efficiency is limited.

[30] Testing procedures assess the performance of security equipment, security guards, and emergency planning and response. Testing encompasses such elements as determining whether or not equipment is calibrated properly, security guards are knowledgeable in post order procedures, and intrusion detection systems are activating properly.

Recommendations

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

(1) Revise and update the FDIC Physical Security Program Circular and develop and implement procedures to define the roles, responsibilities, and requirements for physical security risk management activities and decision-making. These revisions should include:

   a. Ensuring that there is sufficient documentation and support for physical security risk management activities and decisions, including those decisions related to when the ISC standards were determined to be not practical;
   b. Ensuring that each FSL determination is documented, accurate, and adequately supported;
   c. Ensuring that if an FSL is revised, the FDIC reviews the countermeasures and risk mitigation strategies for the facility;
   d. Updating and reviewing facility security plans on an annual basis;
   e. Ensuring that all FSA recommendations are identified, prioritized, and tracked;
   f. Identifying requirements for pre-lease physical security activities and deliverables; and
   g. Requiring that FDIC senior management be routinely advised of the status of the physical security program at FDIC Headquarters, Regional, Area, and Field Offices.

(2) Establish and implement training requirements for personnel conducting FSL determinations and FSAs.

(3) Establish and implement controls to ensure that DOA maintains security assessment-related records in accordance with the *FDIC Records and Information Management Policy Manual*.

(4) Implement an automated FSA template, tool, or other mechanism to ensure that that the FSAs consider all threat, consequence, and vulnerability assessments of undesirable events and assess relevant countermeasures for each FDIC facility. This tool or mechanism should track and record:

   a. Recurring, structured testing and maintenance programs for the FDIC's electronic security systems;
   b. Controls for electronic building and access systems at FDIC facilities;

c. Security countermeasures for child-care centers in FDIC facilities;
d. Facility Security Plans for FDIC facilities; and
e. Accurate FSL and FSA data.

(5) Track and record training programs for physical security awareness that is provided to FDIC employees and contractors annually.

(6) Evaluate the resource needs for the physical security risk management process and modify resources as necessary.

(7) Document the justifications for the physical security activities that the FDIC has taken in response to recommendations, including decisions to accept risk or regarding expenditures for security countermeasures above the recommended standards for an assigned FSL.

(8) Provide the FDIC Board with revised, accurate information supporting the use of security guards at FSL II Offices and identifying the related financial impact.

(9) Identify goals and metrics for measuring the performance of the physical security program to ensure the timeliness, quality, and effectiveness of FDIC risk management process activities.

FDIC COMMENTS AND OIG EVALUATION

On April 2, 2019, the FDIC's Chief Operating Officer and Deputy to the Chairman, on behalf of the Agency, provided a written response to a draft of this report (FDIC Response), which is presented in its entirety in Appendix 9. We carefully considered the comments in this FDIC Response.

The FDIC concurred with the nine recommendations we made in this report and indicated that they would help improve the risk management process for its Physical Security Program. We believe that the planned corrective actions are significant undertakings by the Agency and, once implemented, are likely to achieve important improvements towards the efficiency and effectiveness of its risk management process for physical security.

The FDIC Response acknowledged that "the success of our [its] physical security risk management program hinges on such things as continuous improvement, keen awareness and implementation of emerging technologies, effective communication among staff and management officials, and compliance with policies and procedures." The FDIC therefore agreed to undertake the following actions:

1. Revising and updating the FDIC Physical Security Program Circular and implementing procedures;
2. Establishing and implementing training requirements for personnel conducting FSLs and FSAs;
3. Establishing and implementing controls for maintaining security assessments and related documents;
4. Implementing an automated tool or mechanism to conduct assessments to ensure that all threats, consequences, and vulnerabilities of undesirable events are considered and relevant countermeasures are assessed;
5. Tracking and recording training programs on physical security awareness for FDIC employees and contractors;
6. Evaluating the resource needs for the physical security risk management process;
7. Documenting the justifications for physical security activities that the FDIC has taken in response to recommendations;
8. Providing the FDIC Board of Directors with revised, accurate information supporting the use of security guards at certain offices and identifying the financial impact; and
9. Identifying goals and metrics for measuring the performance of the physical security program to ensure the timeliness, quality, and effectiveness of the Agency's physical security risk management activities.

The planned actions are responsive to the recommendations, and the recommendations are considered to be resolved.

The FDIC also stated in its response that it has hired a Physical Security Specialist to address workload needs, and is awarding a contract to develop an approach for establishing a nationwide, standardized Physical Security Program. In addition, the FDIC will develop operating procedures to define roles, responsibilities, and requirements in the risk management and decision-making processes for its Physical Security Program. Notwithstanding the concurrence with our recommendations, the FDIC Response highlighted several completed, ongoing, and planned security enhancements.

We did not express an opinion as to the Agency's physical security posture, since that was not within the scope of our review. Our report, instead, focused on the risk management process of the FDIC's Physical Security Program during our period of review from March 2017 to March 2018. Our objective was "to determine the extent to which the FDIC's physical security *risk management process* (RMP) met federal standards and guidelines." See pages ii and 29 (emphasis added). The findings and conclusions in our report relate to this objective. Indeed, the report states that we "did not assess the safety of FDIC personnel and facilities." See pages iii and 7 of the report.

The FDIC Response stated that our report implied that the FDIC selected certain security priorities at the expense of complying with ISC standards. We believe that it is important for the FDIC to implement and execute procedures in compliance with applicable standards and requirements – including the Government-wide ISC standards, as adopted by FDIC Directive 1610.1, as well as other security measures, including the implementation of Personal Identity Verification cards. These requirements are not stated in the alternative and are not mutually exclusive of one another. While we acknowledge that the FDIC must set priorities and manage resources within budgetary constraints, we maintain that the FDIC should work towards meeting applicable security standards and requirements. We believe that our recommendations (particularly, Recommendation 6), once implemented, and as concurred to by the FDIC, should aim to accomplish this goal.

With respect to our finding regarding the need for documentation of security decisions, the FDIC Response asserts that FDIC executives were kept apprised of important security decisions and, therefore, were able to perform their oversight responsibilities. The FDIC Response concurred that DOA did not document the justification for all security-related decisions and agreed that documenting the justifications could have provided FDIC executives with an opportunity to evaluate such decisions and provide feedback. Our finding relates to the *documentation* of decisions, as required by FDIC Directive 1610.1 and the transparency provided. Without such documentation, FDIC executives and oversight bodies – such as the FDIC Board (including the Chairman), the OIG, Congressional committees, and others – did not have visibility into the process and could not adequately consider nor review such decisions. We believe that our recommendations (specifically, Recommendation 7), once implemented, and as concurred to by the FDIC, should aim to maintain proper documentation for key security decisions.

With respect to our finding regarding the inaccurate statements provided to the FDIC Board of Directors, the FDIC acknowledged that it had provided inaccurate statements to the Board and that the Board relied, in part, on this information in its decision-making. The FDIC Response, however, asserted that the Board's decision to approve the security guards contract was also influenced by its desire to provide the same level of security services to FDIC employees in Headquarters, Regional, and Area Office facilities. As described in our finding, after DOA provided inaccurate information to the Board regarding facility security levels, the Board made a decision regarding this matter and allocated a significant expenditure of funds. The FDIC has not disputed this finding and could not explain the discrepancies. See pages iii and 22 of the report. We maintain that our recommendations (particularly, Recommendation 8), once implemented, and as concurred to by the FDIC, should accomplish the goal of providing accurate information to the Board.

We acknowledge the efforts of the FDIC to implement security and safety measures, and we appreciate the information provided for this important report. We look forward to the FDIC's implementation of our recommendations in order to improve the risk management process of its Physical Security Program.

Objective, Scope, and Methodology

Objective

Our evaluation objective was to determine the extent to which the FDIC's physical security risk management process met Federal standards and guidelines.

We performed our work from March 2017 to March 2018 at the FDIC's offices in Arlington, Virginia; Dallas, Texas; Atlanta, Georgia; Charlotte, North Carolina; Raleigh, North Carolina; and Austin, Texas. We updated the number of FDIC employees and contractors and the approval status of FSAs as of June 30, 2018. We also reviewed and considered information about security incidents and countermeasures relevant to our scope period that the FDIC personnel provided as part of the draft report process in September 2018 and January 2019. 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 evaluation scope included physical security risk management activities for FDIC Headquarters, Regional, Area, and Field Offices.

To address our evaluation objective, we gained an understanding of the FDIC's policies and practices for mitigating physical security risk. We reviewed FDIC policies and procedures related to physical security, internal controls, and leasing, including:

- *FDIC Physical Security Program,* Circular 1610.1 (February 9, 2012);
- *FDIC Enterprise Risk Management Program,* Circular 4010.3 (April 16, 2012);
- *FDIC Leasing Policy Manual*, Circular 3540.1 (July 13, 2004); and
- *Space Utilization Policy*, Circular 3010.2 (October 24, 2008).

We also reviewed Federal standards and guidelines relevant to physical security, including the following ISC publications:

- *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (2nd Edition, November 2016).[31] We used the

[31] The ISC issued the first edition of the ISC RMP Standard, a compilation of several previously distinct standards, in August 2013.

standards in this document as the primary[32] basis for evaluating the FDIC's physical security risk management process, including the adequacy of its assessment templates, reports, and tracking tools;

- *Security Specialist Competencies: An Interagency Security Committee Guide* (2nd Edition, January 2017). We used this best practices guidance to assess the physical security-related qualifications and training of FDIC personnel performing FSAs; and

- *Facility Security Plan: An Interagency Security Committee Guide* (1st Edition, February 2015). We used this best practices guidance to determine if the FDIC's FSA template incorporated recommended FSP contents.

We interviewed FDIC personnel, including:

- The DOA Corporate Services Branch SEPS staff to obtain an understanding of their process for physical security risk management;

- The DOA Information Security Manager to determine the extent of coordination with ISPS on testing of cyber security controls for BACS;

- The ISPS to obtain an understanding of physical security controls at the FDIC disaster recovery site and the testing of cyber security controls for BACS; and

- The Division of Finance Risk Management and Internal Control Branch staff to understand what risk-related information this group shared with SEPS personnel.

We also interviewed physical security officials from the ISC, the Federal Protective Service, the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency to obtain information about physical security risk management best practices and the application of the ISC RMP Standard.

We considered the following recent reviews while conducting our evaluation:

- GAO Report 18-72, *Federal Facility Security – Selected Agencies Should Improve Methods for Assessing and Monitoring Risk* (October 2017);

[32] Prior to the issuance of the ISC RMP Standard in August 2013, the ISC risk management process was reflected in two ISC standards, *Facility Security Level Determinations for Federal Facilities* (February 21, 2008) and *Physical Security Criteria for Federal Facilities* (April 12, 2010). We considered these standards, whose key provisions in general appeared to be reflected in the August 2013 standard, when reviewing FDIC risk management activities conducted prior to August 2013.

- GAO Report 18-95, *Physical Security – National Institute of Standards and Technology and Commerce Need to Complete Efforts to Address Persistent Challenges* (October 2017); and

- GAO Report 18-201, *VA Facility Security: Policy Review and Improved Oversight Strategy Needed* (January 2018).

Sampling Methodology

We selected a non-statistical sample[33] of 26 FDIC facilities to review aspects of the physical security risk management process, including the timeliness and completeness of FSL determinations and FSAs, as well as risk mitigation or acceptance activities. The FDIC had 94 facilities as of September 30, 2017, including 6 Headquarters Offices, 6 Regional Offices, 2 Area Offices, and 80 independently located Field Offices. We selected for review all 6 Headquarters, 6 Regional, and 2 Area Office facilities, and 12 of the 80 Field Offices, comprising the 2 Field Offices in each region that had the highest number of FDIC employees. For each sampled facility, we reviewed the most recently completed FSL and FSA documents as of September 30, 2017. Table 4 lists the 26 FDIC offices we sampled, the facility type, the FSL, and the date of the FSA that we reviewed.

Table 4: OIG-Sampled FDIC Facilities

Sample Number	Facility Type	Facility Security Level	Most Recent FSA Date (as of September 30, 2017)
1	Headquarters	IV	January 2013
2	Headquarters	II	September 2017
3	Headquarters	II	September 2017
4	Headquarters	IV	April 2012
5	Headquarters	III*	June 2015*
6	Headquarters	IV	December 2012
7	Regional Office	III	April 2014
8	Regional Office	II	October 2012
9	Regional Office	III	December 2015
10	Regional Office	II	November 2011
11	Regional Office	III	November 2014
12	Regional Office	III	June 2017
13	Area Office	II	October 2011
14	Area Office	II	August 2014
15	Field Office	I	April 2016
16	Field Office	I	February 2017
17	Field Office	II	October 2012
18	Field Office	I	March 2013
19	Field Office	II	July 2017
20	Field Office	Unknown**	July 2017
21	Field Office	I	December 2015

[33] The results of a non-statistical sample cannot be projected to the intended population by standard statistical methods.

Sample Number	Facility Type	Facility Security Level	Most Recent FSA Date (as of September 30, 2017)
22	Field Office	I	August 2017
23	Field Office	Unknown**	November 2016
24	Field Office	I	January 2017
25	Field Office	II	November 2011
26	Field Office	I	October 2013

Source: OIG review of FDIC FSL and FSA documents. The most recent FSA date is the "Date of Assessment" from the FSA template.
* The FSL and FSA date are from a draft FSA report that the FDIC did not complete.
** The FDIC did not document the FSL determination.

To evaluate the FDIC's physical security risk management process, for each sampled facility we determined whether:

- The FDIC determined the FSL in accordance with the ISC RMP Standard;
- The FDIC conducted FSAs timely in accordance with the ISC RMP Standard;
- The FDIC reviewed completed FSA templates and reports and concluded as to whether the facility met the recommended minimum standards;
- The completed FSA templates and reports contained any significant omissions or anomalies;
- The FDIC correctly recorded FSL and FSA information in its assessment tracking schedules;
- The FDIC took action on significant physical security recommendations contained in the FSA reports; and
- The FDIC provided justification for significant recommendations that the FDIC did not implement, or did not implement in a timely manner.

We did not perform an independent FSL determination or FSA at any FDIC facilities as part of our evaluation work.

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

Office of Program Audits and Evaluations
Office of Inspector General

DATE: August 9, 2017

MEMORANDUM TO: Arleas Upton Kea, Director
Division of Administration

/signed/

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

SUBJECT: Concerns Related to FDIC Physical Security Assessments

While planning our evaluation of *Physical Security at Non-Headquarters Facilities* (Assignment No. 2017-013), we learned that the FDIC has experienced delays in conducting physical security assessments (PSAs) at its headquarters and regional facilities, and therefore, the FDIC is not in compliance with Federal guidance. We believe that these circumstances present risk to the FDIC and warrant management's urgent attention.

Background

The Interagency Security Committee (ISC) publishes security standards and best practices for nonmilitary Federal facilities in the United States.[1] The ISC's *Risk Management Process: An Interagency Security Committee Standard, 2nd Edition 2016* (ISC Standard) defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level (FSL), and provides an integrated, single source of physical security countermeasures to be applied based on the designated FSL.

The Division of Administration (DOA), Security and Emergency Preparedness Section (SEPS), Physical Security Staff, is responsible for conducting PSAs of FDIC-owned and leased facilities in accordance with the ISC standard, pursuant to FDIC Circular 1610.1, *FDIC Physical Security Program*, dated February 9, 2012.

The PSA process first requires the agency to determine the FSL, ranging from Level I (lowest risk) to Level V (highest risk).[2] The FDIC is responsible for making the FSL determination for each FDIC facility, and has assigned three of the six headquarters facilities as Level IV and the remaining three facilities as Level III.[3] The PSA process then requires the agency to identify

[1] The ISC is a group of Federal agency physical security representatives created pursuant to Executive Order 12977, dated October 19, 1995. According to FDIC Circular 1610.1, the FDIC Chairman adopted the ISC recommended minimum security standards for all FDIC facilities where practical.
[2] According to the ISC Standard, the factors for determining the FSL are mission criticality, symbolism, facility population, facility size, threat to tenant agencies, and other intangible factors. The FSL should be reviewed and adjusted, if necessary, as part of each initial and recurring risk assessment.
[3] Level IV facilities have a high level of risk and require a high baseline level of protection. Level III facilities have a medium level of risk and require a medium baseline level of protection.

risks and to fund and implement countermeasures to mitigate the identified risks based on the FSL designation. The ISC Standard indicates that the agency should conduct PSAs at least once every 3 years for Level III- and Level IV-rated facilities.

Delayed Physical Security Assessments

In June 2017, DOA officials provided us a schedule identifying the most recent PSAs of FDIC headquarters, regional, and area office facilities. The schedule also identified the due date for the next PSA of each location. As noted in Table 1 below, the DOA schedule showed that PSAs for five of the six FDIC headquarters facilities were delayed based on due dates required by the ISC Standard. The sixth headquarters facility had recently been leased by the FDIC and had a current PSA. (a)

Table 1: Schedule of Past Due Headquarters Physical Security Assessments

FDIC Facility	Last Assessment Date	FSL Level	Next Assessment Due Date	Delay as of July 31, 2017
[redacted]	December 2012	IV	December 2015	19 months
[redacted]	February 2013	IV	February 2016	17 months
[redacted]	August 2012	IV	August 2015	23 months
[redacted]	July 2012	III	July 2015	24 months
[redacted]*	October 2012	III	October 2015	21 months

Source: DOA SEPS email dated June 21, 2017.
*This location was incorrectly coded on the DOA PSA schedule as a FSL Level II with a 5-year assessment cycle. The correct FSL Level III requires a 3-year assessment cycle, which is reflected in the above table. (b)

Moreover, the schedule showed that PSAs for 4 of the 8 FDIC regional and area offices (Atlanta, Boston, Kansas City, and San Francisco) were overdue by 4 to 15 months.

We discussed this matter with the Deputy Director, DOA Corporate Services Branch (CSB), who provided two reasons for the delayed PSAs:

- The Deputy Director noted that the PSAs conducted in 2012 and 2013 identified a number of deficiencies that required significant funds and time to remediate. DOA developed a plan to address the deficiencies and presented it to the FDIC Executive Management Committee (EMC) in December 2016.[4] DOA developed a cost estimate for the physical security enhancements in January 2017 and briefed the EMC on an implementation timeline in July 2017. The Deputy Director believed that it did not make business sense to update the PSAs until the physical security enhancements were implemented.

- The Deputy Director also stated that SEPS is understaffed and has only two Physical Security Specialists qualified to conduct the PSAs. These Specialists have been occupied with other physical security projects (such as the Personal Identity Verification (PIV) card implementation and the Electronic Security System upgrade).

[4] Remediation will include, among other items, the installation of additional vehicle barriers and enhanced guard booths at Level IV facilities. DOA estimates the physical security enhancements will cost approximately $3.2 million.

2
Privileged and Sensitive Information

(a): We subsequently learned that the FDIC had initiated, but had not completed a PSA (referred to in the remainder of the report as FSA) for the sixth facility, as of the date of the memorandum.

(b): We subsequently received the FSA for this facility, which indicated FSL II, and therefore the PSA (FSA) was not past due as of the date of the memorandum.

The Deputy Director stated that DOA SEPS staff intended to wait until 2018 to conduct the PSAs for the FDIC headquarters facilities, after the planned physical security enhancements were implemented.

OIG Concerns

These PSA delays and outstanding deficiencies present risks for the Corporation. Our specific concerns include:

- The FDIC is currently not in compliance with the ISC Standard for FSL Level III and IV facilities. Non-compliance with the ISC Standard has the potential to expose the FDIC to risks in protecting its workforce, visitors, and facilities.

- Three of the headquarters facilities are designated as FSL Level IV, two of which are just a few blocks from the White House and the Eisenhower Executive Office Building. These facilities present a high level of risk and thus require a high baseline level of protection.

- The previous PSAs at FDIC headquarters facilities are outdated. For example, certain security changes at FDIC facilities—such as the PIV card implementation, development of a secured compartmentalized information facility, and Electronic Security System upgrades—have not yet been subject to a PSA. In addition, the ISC Standard has been updated since the time of the last PSAs, and the ISC has provided guidance on best practices for physical security of facilities.

- Some of the deficiencies previously identified at FDIC facilities have been outstanding for more than 4 years. The ISC standards state that where countermeasures cannot be implemented immediately, the agency must institute a plan to phase in countermeasures to bring itself into compliance or formally accept the risk of not implementing countermeasures.

- The decision to delay the PSA was internal to DOA and not discussed with senior FDIC leadership.

We request that you let our office know how DOA plans to address the risks raised in this memorandum and any time frames for doing so. Please let us know any planned actions by August 31, 2017. We will continue to evaluate the PSA process as part of our ongoing assignment and address any actions taken by FDIC management in our written report.

If you would like to discuss these concerns further, please contact me at (703) 562-6378, or Lisa Conner at (972) 761-2297.

cc: Barbara A. Ryan, Chief of Staff, COO
Steven O. App, CFO
Michael Spencer, Deputy to the Vice Chairman
Ronald T. Bell, DOA
Charles Yi, General Counsel
Daniel H. Bendler, DOA
James E. Anderson, DOF

FDIC

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

DATE: September 27, 2017

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

FROM: /signed/
Arleas Upton Kea, Director
Division of Administration

SUBJECT: Management Response to the Office of Inspector General Concerns Related to FDIC Physical Security Assessments

This response addresses the observations and concerns reported in your August 9, 2017 memorandum entitled "*Concerns Related to FDIC Physical Security Assessments*". In that memorandum, you noted a number of observations related to delays in conducting physical security assessments (PSA) at FDIC headquarters and regional facilities. You further noted that, as a result, FDIC was not in compliance with Federal guidance.

The Division of Administration (DOA) has taken corrective actions to address the risks raised in your memorandum. On August 25, 2017, we awarded a contract to [redacted] to conduct physical security assessments at the following six locations:

- 3501 N. Fairfax Drive, Arlington, VA
- 3701 N. Fairfax Drive, Arlington, VA (FDIC occupied spaces only)
- Courthouse Square (FDIC occupied spaces only)
- 550 17th Street, Washington, DC
- 1750 F Street, Washington, DC
- NY Avenue, Washington, DC (FDIC occupied spaces only)

As part of this arrangement, [redacted] will conduct assessments using Interagency Security Committee (ISC) guidelines to identify potential risks and vulnerabilities, evaluate threats and vulnerabilities and develop security countermeasures to mitigate risk. FDIC security staff will provide [redacted] with a list of ISC guidelines to be used for each risk assessment. In turn, [redacted] will provide FDIC with a final report for each assessment that will include fact-based findings and recommendations. All assessments will be completed by December 31, 2017.

Once received, DOA will share the assessment reports with the OIG for your information and as evidence that the assessments were completed. In addition, we will brief senior FDIC leadership once the assessments, findings, and report are complete. DOA is committed to taking timely corrective actions to address any recommendations that might result from [redacted] assessments.

We appreciate the OIG's observations and recommendations and believe that our planned corrective action adequately addresses the risks raised in your memorandum. If you would like to discuss this response, please contact me at 703-562-2100 or Dan Bendler at 703-562-2123.

cc: Barbara A. Ryan, Deputy to the Chairman and Chief Operating Officer
Steven O. App, Deputy to the Chairman and Chief Financial Officer
James E. Anderson, Acting Deputy Director, DOF Corporate Management Control Branch
Ronald T. Bell, Deputy Director, DOA, Corporate Services Branch
Daniel H. Bendler, Assistant Director, DOA, Management Services Branch

2

Appendix 4 Glossary

Term	Definition
Ballistic Attack	An attack using a handgun, rifle, multiple handguns, a combination of firearms, or explosive laden projectiles such as mortars, guided or unguided missiles, rocket propelled grenades, etc. [ISC RMP Standard]
Baseline Level of Protection	The baseline level of protection is the degree of security provided by the set of countermeasures for each FSL that an agency must implement unless a risk assessment justifies a deviation. [ISC RMP Standard]
Building Access and Control Systems	All information systems in a Federal facility that support the security and safety functions, such as systems for physical access control, video surveillance, building power and energy control, and automated heating and cooling, among others. [ISC RMP Standard]
Consequence	The level, duration, and nature of the loss resulting from an undesirable event. Consequence is commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment. [ISC RMP Standard]
Countermeasure	A specific control or action designed to mitigate the security risks related to the threat from one or more undesirable event. [*Facility Security Plan: An Interagency Security Committee Guide* (1st Edition, February 2015)] Examples of security countermeasures include the placement of security guards, physical barriers, access control devices, and closed-circuit television devices at one or more locations around and within a facility. [ISC RMP Standard]
Critical Areas	Areas that, if damaged or compromised, could have significant adverse consequences for the mission of the agency or the health and safety of individuals within the building or the surrounding community. [ISC RMP Standard]
Cyber Security	Measures and controls that ensure the confidentiality, integrity, and availability of information system assets, including information being processed, stored, and communicated. [ISC RMP Standard]
Electronic Security Systems	Electronic systems designed to prevent theft or intrusion and protect property and life. Physical access control systems, burglar alarm systems, CCTV video surveillance systems, and fire alarm systems are all a type of security system. [ISC RMP Standard]
Facility	A space built or established to serve a particular purpose. It is inclusive of a building or suite and the associated support infrastructure and land. [ISC RMP Standard]
Facility Security Assessment	The process and final product documenting an evaluation of security-related risks to a facility. The process analyzes potential threats, vulnerabilities, and estimated consequences. It culminates in the risk affecting a facility using a variety of sources and information, and in recommendations for specific security countermeasures commensurate with the level of risk. [ISC RMP Standard]

Term	Definition
Facility Security Level	A categorization based on the analysis of several security-related facility factors, which serves as the basis for implementation of countermeasures specified in the ISC standards. [ISC RMP Standard]
Intangibles	Circumstances unique to the agency needs or to the facility. As examples, a short duration of occupancy may reduce the value of the facility in terms of investment or mission. Alternatively, proximity to higher risk facilities, such as the White House, may increase the risk to a facility. [ISC RMP Standard]
Intangible Adjustment	A one-level increase or a one-level decrease to the FSL based on the intangibles identified for the facility. [ISC RMP Standard]
Interagency Security Committee	The ISC, chaired by the Department of Homeland Security, consists of 60 Federal departments and agencies, with the mission to develop security standards and best practices for nonmilitary Federal facilities in the United States. The FDIC is a member of the ISC. [ISC RMP Standard]
Level of Protection	The degree of security provided by a particular countermeasure or set of countermeasures. [ISC RMP Standard]
Occupant	Any person who is assigned permanently or regularly to the government facility and displays the required identification badge for access, with the exception of those individuals providing a service at the facility. [ISC RMP Standard]
Position Switch	A device used to detect the open or closed status of an opening and then send this status to a control panel. They come in a variety of shapes and sizes and are designed for monitoring door positions, roof hatches, gates, etc. [Allegion]
Preventive Maintenance	A program to reduce electronic security component down time through regular periodic inspection and service of such components and by replacement of components that are nearing the end of their useful life expectancy. [FDIC ESS contract]
Risk	A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence. It is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. [ISC RMP Standard]
Risk Acceptance	The explicit or implicit decision not to take an action that would affect all or part of a particular risk. [ISC RMP Standard]
Risk Assessment	The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences. Risk assessment methodologies involve assigning ratings to each of those three factors and combining these ratings to produce an overall measurement of risk for each identified undesirable event. [GAO Report 18-72, *Federal Facility Security: Selected Agencies Should Improve Methods for Assessing and Monitoring Risk* (October 2017)]

Term	Definition
Risk Management	A comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and—when necessary—risk acceptance. [ISC RMP Standard]
Risk Mitigation	The application of strategies and countermeasures to reduce the threat of, vulnerability to, and consequences from, an undesirable event. [ISC RMP Standard]
Security Organization	The internal agency component responsible for physical security for a specific facility. [ISC RMP Standard]
Threat	The intention and capability of an adversary to initiate an undesirable event. [ISC RMP Standard]
Undesirable Event	An incident that has an adverse impact on the facility occupants or visitors, operation of the facility, or mission of the agency. Undesirable events represent the "reasonable worst case scenario" for each threat. [GAO Report 18-72, *Federal Facility Security: Selected Agencies Should Improve Methods for Assessing and Monitoring Risk* (October 2017)]
Visitors	Any persons entering the government facility that do not possess the required identification badge or pass for access or who otherwise do not qualify as occupants. [ISC RMP Standard]
Vulnerability	A weakness in the design or operation of a facility that an adversary can exploit. [ISC RMP Standard]

Appendix 5 Acronyms and Abbreviations

BACS	Building Access and Control Systems
CCC	Child Care Center
CCTV	Closed-Circuit Television
CSB	Corporate Services Branch
DOA	Division of Administration
ESS	Electronic Security Systems
FDIC	Federal Deposit Insurance Corporation
FSA	Facility Security Assessment
FSL	Facility Security Level
FSP	Facility Security Plan
GAO	Government Accountability Office
ISC	Interagency Security Committee
ISPS	Information Security and Privacy Staff
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
PIV	Personal Identity Verification
PSA	Physical Security Assessment
RIM	Records and Information Management
RMP	Risk Management Process
SEPS	Security and Emergency Preparedness Section

Appendix 6 Undesirable Events by Category

This table identifies the 33 undesirable events that the ISC RMP Standard indicates an agency should consider when performing a physical security-related risk assessment. The table also identifies the nine categories into which the ISC groups undesirable events, and the number of undesirable events within each category.

Category	Undesirable Events	Number
Criminal Activity	Assault Kidnapping Robbery Theft Vandalism Civil Disturbance Workplace Violence Insider Threat	8
Explosive Events/ Incendiary Device	Parcel Bomb or Parcel Improvised Explosive Device - Mail or Delivery Person-Borne Improvised Explosive Device External Person-Borne Improvised Explosive Device Internal Suicide/Homicide Bomber Vehicle Borne Improvised Explosive Device Arson	6
Ballistic Attack	Ballistic Attack - Active Shooter Ballistic Attack - Small Arms Ballistic Attack - Standoff Weapons	3
Unauthorized Entry	Unauthorized Entry - Forced Unauthorized Entry - Surreptitious Breach of Access Control Point – Covert Breach of Access Control Point – Overt	4
Chemical/ Biological/ Radiological Release	Chemical/ Biological/ Radiological Release - External Chemical/ Biological/ Radiological Release - Internal Chemical/ Biological/ Radiological Release - Mail or Delivery Chemical/ Biological/ Radiological Release - Water Supply Release of Onsite Hazardous Materials	5
Vehicle Ramming	Aircraft as a Weapon Vehicle (Automobile) Ramming	2
Hostile Surveillance	Hostile Surveillance	1
Cyber Attack	Unauthorized Access Interruption of Services Modification of Services	3
Adversarial Use of Unmanned Aircraft ystems	Adversarial Use of Unmanned Aircraft Systems	1
	Total	**33**

Source: OIG summary of ISC RMP Standard Appendix A: *The Design-Basis Threat Report* (11th Edition, June 2017).

Appendix 7 Security Criteria by Category

This table lists examples of the 93 security criteria that the ISC RMP Standard identifies to analyze and mitigate risks related to specific undesirable events. We judgmentally selected these examples to include, among others, criteria discussed in the body of the report. The example security criteria are divided into the same seven categories into which the ISC groups the 93 criteria.

Category	Example Security Criteria
Site Security	Identification as a Federal Facility Vehicle Barriers Vehicle Screening Receptacle and Container Placement
Structure Security	Protection of Air Intakes Blast Resistance – Windows & Under-Building Parking Biological Filtration – Lobbies and Mailrooms
Facility Entrance Security	Visitor Screening Ballistic Protection at Screening Locations After Hours Access Control
Interior Security	Building Systems and Roof Access Control Blast Resistance – Mail Screening and Receiving Location
Security Systems	CCTV Monitoring and Recording Duress Alarms or Assistance Stations Security System Testing Security System Maintenance
Security Operations and Administration	Security Force Patrols Facility Security Plan Mail/Package Handling and Other Deliveries Security Awareness Training
Cyber Security	Identify & Define Building Access and Control Systems Devices and Networks Establish Processes for Incident Response for BACS

Source: OIG summary of ISC RMP Standard Appendix B: *Countermeasures* (3rd Edition, May 2017).

Appendix 8 Summary of Delayed Initial FSLs and FSAs

This table identifies the 7 sampled leased facilities that the FDIC newly occupied within the last 8 years for which the FDIC could not provide evidence that it had completed initial FSL determinations and FSAs in a timely manner.

Facility Type - Sample Number	Lease Occupancy Date	First FSL/FSA Date	FSL Rating	Time After Occupied Before Completing First FSL/FSA
Headquarters Office				
5	April 2015	---*	III	2 years, 6 months*
Area Office				
14	December 2012	August 2014	II	1 year, 9 months
Field Office				
16	November 2015	February 2017	I	1 year, 3 months
17	April 2017	October 2017	II	6 months
18	April 2010	March 2013	I	2 years, 11 months
19	June 2015	July 2017	II	2 years, 1 months
21	November 2013	December 2015	I	2 years, 1 month

Source: OIG analysis of FDIC facility lease, FSL, and FSA documents.
* As of September 30, 2017, the FDIC had not completed an FSA for this facility.

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

DATE: April 2, 2019

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

FROM: **/signed Julia N. Goodall for/**
Arleas Upton Kea
Chief Operating Officer and Deputy to the Chairman

SUBJECT: Management Response to the OIG Draft Report, *FDIC's Physical Security Risk Management Process* (Assignment No. 2017-013)

Introduction

The FDIC has completed its review of the Office of Inspector General's (OIG) draft evaluation report titled *FDIC's Physical Security Risk Management Process*, issued on March 13, 2019. We appreciate the opportunity to comment on the report's findings and recommendations. DOA acknowledges that the success of our physical security risk management program hinges on such things as continuous improvement, keen awareness and implementation of emerging technologies, effective communication among staff and management officials, and compliance with policies and procedures. While FDIC has a robust Physical Security Program in place, we welcome and continually pursue opportunities to make improvements. To that end, we accept the OIG's recommendations and find them to be reasonable and helpful. We intend to implement corrective actions in a timely manner.

Management Response

While we accept the OIG's recommendations, we believe that the OIG's report could have been more balanced and provided greater coverage of our many successful and critical security-related initiatives that contribute to FDIC's safe work environment. These security-related initiatives help meet the Interagency Security Committee's (ISC) mandate to enhance the quality and effectiveness of security in, and the protection of, buildings and federal facilities. Accordingly, we offer a description of those initiatives in our response to provide readers of the report with a more complete representation of FDIC's Physical Security Program.

In its report, the OIG concluded that the FDIC has not established an effective physical security risk management process to ensure that it meets ISC standards and guidelines; cannot be certain that it has taken appropriate measures commensurate with risk and aligned with ISC standards to ensure the safety of its employees, contractors, and facilities; and has less assurance that its Physical Security Program is operating in an efficient and effective manner. The OIG also concluded that the weaknesses it identified limited the FDIC's assurance that it met Federal standards for physical security in its 94 facilities that protected 9,000 employees and contractors.

In addition to making these conclusions, the OIG stated in its report that "*The Federal Protective Service reported 737 workplace violence incidents from 2012 to 2016 at the Federal facilities that they protect*." The OIG also noted that "*The Federal Bureau of Investigation reported 7 active shooter incidents from 2014 to 2017 at non-military government properties, resulting in 12 killed and 19 wounded*." The OIG's conclusions combined with its use of facts about workplace violence incidents may create an undue level of concern and fear regarding the safety and protection of FDIC employees, contractors, and facilities.

DOA believes that FDIC employees, contractors, and facilities are safe. In fact, DOA evaluated over ten years of incident reporting data and confirmed that there have been no major incidents or threats to any FDIC facility during this timeframe. Further, DOA officials could not identify a single major incident or serious threat to any of its facilities, employees, or guests at any time. FDIC has made extraordinary efforts to successfully implement a number of substantive, effective, and cutting edge security and safety measures. These measures are consistent with industry best practices and expert consultation. We are particularly pleased that nearly 90 percent of 2018 Federal Employee Viewpoint Survey (FEVS) respondents acknowledged feeling well-protected and safe in FDIC facilities. This information was not included in the OIG's report and, in our view, provides important context for readers to fully understand the significance of the OIG's findings.

In the Executive Summary of its report, the OIG states that *"FDIC officials responsible for the Physical Security Program had not emphasized compliance with ISC standards, and instead placed priority attention on other security initiatives."* As written, this sentence implies that the FDIC selected certain security priorities at the expense of complying with ISC standards. The "other security initiatives" that the OIG referenced in its report included a major effort to implement Personal Identity Verification (PIV) cards at the FDIC. The OIG itself urged FDIC to adopt this initiative as part of its September 2015 audit of FDIC's Identity, Credential, and Access Management Program. In March 2016, the OIG accepted the Agency's management response that outlined our decision to deploy PIV cards as part of a strategic vision for managing physical and logical access. The PIV card initiative and so many other security-related projects mentioned below increased FDIC's security posture in support of ISC standards.

The OIG also noted in its Executive Summary that "*FDIC officials relied on a few experienced employees to make important decisions regarding physical security risks and countermeasures at facilities. Without documentation of these decisions, FDIC executives and oversight bodies were unable to fully consider and review the decisions.*" While we agree that key security-related decisions should be better documented, the few employees mentioned in the OIG's report were subject matter experts, professional, well-trained, and qualified to make such decisions. Further, FDIC executives were routinely apprised of important decisions that impacted FDIC's security initiatives and risks. All key decisions to implement security-related initiatives were fully vetted, discussed, and briefed to management prior to implementation. As such, we believe that FDIC executives were able to adequately perform their oversight responsibilities. We agree that DOA did not document the justification for all security-related decisions including instances where security measures were not implemented. Documenting the justification for accepting or

not accepting security measures could have provided FDIC executives with an additional opportunity to evaluate such decisions and provide feedback.

The OIG reported that FDIC's Board of Directors (Board) relied upon incorrect information in its decision-making to approve the contract for security guards. Specifically, the OIG noted that in May 2014, DOA erroneously told the Board that all Headquarters, Regional, and Area Office facilities were facility security level III or IV, for which armed security guard services are an ISC-recommended minimum standard. Furthermore, in its Executive Summary, the OIG concluded that the Board relied upon this information when approving the contract for security guards. DOA acknowledges that it mistakenly provided inaccurate information during the May 2014 Board meeting and that Board members relied, in part, on this information in its decision-making when approving the contract for security guards. The Board's decision to approve the security guards contract was also influenced by its desire to provide the same consistent high-level of security services to all FDIC employees in these locations. Specifically, during the May 2014 Board meeting, the Board requested assurance that the new contract would effectively ensure that the Corporation had a consistent level of security services across the regional offices. In response, DOA officials emphasized that the new contract would indeed provide a consistent level of protection.

Ensuring the safety and protection of FDIC's employees, contractors, visitors, and facilities is among DOA's highest priorities. Without exception, this critical responsibility receives our full attention and commitment on a regular basis. Likewise, this strong commitment is widely shared and supported by officials at the highest level of the Agency and among every Division and Office. DOA has implemented and continues to oversee many successful initiatives that have contributed to FDIC's safe work environment and ability to accomplish the Agency's vital mission. Many of these initiatives met federal requirements and mandates such as HSPD-12 and others[1].

The following section explains a number of relevant security related actions that DOA has successfully implemented along with our partners in other Divisions and Offices. The OIG did not adequately acknowledge these items or consider how these items aligned with ISC's security mandate.

Actions Taken to Help Ensure that FDIC Employees, Visitors, and Facilities are Safe and Protected

- **Vehicle Access Control Point (VACP) Security Upgrades** – This project, started in early 2017 and completed in 2018, involved the installation of seven [redacted] crash rated [redacted] active vehicle barriers (AVBs), ballistic rated guard booths, high-speed garage doors and complementary electronic security system (ESS) equipment (ACS, IDS, CCTV, etc.) at seven parking garage entrances at owned FDIC

[1] Other Federal requirements and mandates include OMB 05-24 and M-11-11, FIPS 201, NIST SP800-116, FICAM, and FISMA.

Headquarters facilities. These upgrades substantially increased VACP security and access control measures, addressed lifecycle replacement and technology refresh needs, and met Federal requirements and industry standards.

- **Physical Barriers 550 Building** – To prevent a vehicular attack and injuries due to explosive blasts, DOA installed physical granite block barriers and other physical security measures around the FDIC's Main Building (550 17th Street) in early 2018.

- **Blast-Resistant Windows** – DOA installed blast resistant windows at the 550 Main Building in 2016. Windows on floors two through six are blast resistant. The frames and supporting steel were designed and installed slab to slab to achieve this safety performance goal. These windows provide a medium level of protection as defined by industry standards. In addition, all windows at the Virginia Square (VASQ) campus are coated with a blast-resistant coating and other measures intended to protect building occupants. Blast-resistant windows can save lives by keeping windows intact during an explosion.

- **Security Services Contract** – DOA's Security and Emergency Preparedness Section (SEPS) provides security services for the protection of FDIC personnel, property, and facilities. To support SEPS, DOA relies on Security Services contract that provides a professionally trained, fully qualified and industry certified protective guard force that strictly adheres to FDIC regulations, policies and procedures. The Security Services contract took effect in 2015.

  All contractor personnel who are assigned to this contract are required to successfully complete 119 hours of basic training within four months of hiring. This training curriculum includes Weapons and Defensive Tactics, Inspections, Law Enforcement Support, Patrol, Communications, and Emergency Response tactics. DOA's current Security Services contractor handles armed guard services; investigative services; mail screening; security operation centers; fire protection watch; badging; fingerprinting, and escorting.

  The Security Services contract helps ensure the correct level of protection is being executed every day. FDIC security guards provide reassurance to the workforce that their workplace is safe and that on-site emergency response is always available. The guards are positioned at all FDIC entrances. Their presence greatly reduces the risk of any wrong doing on FDIC property. The current contract also employs a full time investigator who thoroughly investigates all incidents using various investigative techniques. Incident reports are prepared for FDIC management to review and to act on as appropriate. Security officers are required to physically walk through all FDIC floors multiple times a day and report any suspicious activity they encounter.

  Each Regional and Area Office has been categorized as either FSL-II (Low-Risk) or FSL-III (Medium-Risk). Under the current contract, FDIC chooses to protect all Regional and Area Offices at the higher FSL-III Level of Protection using armed guards at these sites.

- **FDIC Physical Security Program Circular 1610.1** - The FDIC has an established policy in place to govern the Agency's Physical Security Program. Circular 1610.1 dated February 9, 2012, contains the Circular's purpose, scope, background, policy, functional responsibilities, and physical security access guidelines. The Circular also contains detailed building access procedures, badge identification guidelines, guidelines for handling security-related incidents, and valuable threat alert procedures.

- **Active Shooter Awareness** -- On its website, DOA's SEPS maintains an "Active Shooter Occupant Awareness Plan" for FDIC's Headquarters buildings and Regional and Area Offices. Each plan describes essential information on how to recognize potential workplace violence and indicators of potential violence. The plans, issued from 2016 to 2018, also contain information on how to respond to an active shooter, key emergency contacts, and shelter-in-place procedures.

- **Personal Identity Verification (PIV) Cards** – In 2016 and 2017, DOA partnered with the CIO Organization and other Divisions and Offices to implement the agency's roll-out of PIV cards to over 6,000 employees and more than 2,000 contractors. Fully developing and implementing the PIV card program was a successful Corporate-wide priority that consumed tremendous time and resources throughout 2016 and 2017. The PIV card program also addressed an earlier OIG finding and recommendation[2] that urged the FDIC to complete the FDIC's Identity, Credential, and Access Management (ICAM) program.

- **Electronic Security Systems (ESS) Program –** DOA's SEPS has a mature and evolving electronic security systems (ESS) program. This program was created in 2015 and consists of physical access control systems (PACS), intrusion detection systems (IDS) and video surveillance systems (VSS) all of which are designed to enhance FDIC's security posture. To help implement and operate FDIC's ESS, the Agency relies on a six year, multi-million dollar nationwide contract that provides sustainment, maintenance, and new installation services.

  When integrated or combined with other types of security mechanisms (i.e. active vehicle barriers (AVB), perimeter detection, armed security guards, etc.) these systems provide security in depth (SID) and increased situational awareness. The fundamental goals of physical security are to reduce or mitigate risk and to deter, detect, delay and defeat adversaries. Well-established ESS and security guard programs provide FDIC the ability to meet these goals and continue to provide a safe and secure work environment for agency employees, visitors and assets. Additional value is realized by meeting federal requirements and mandates such as HSPD-12, OMB 05-24 and M-11-11, FIPS 201, NIST SP800-116, FICAM, FISMA, and others.

  ESS Examples: Security upgrades executed under the current contract consist of, but are not limited to, the following:

[2] Office of Inspector General, Office of Audits and Evaluations Report No. AUD-15-011, *The FDIC's Identity, Credential, and Access Management Program*, dated September 2015.

1) Replacement of the legacy PACS and IDS, [redacted], with the personal identity verification (PIV) compliant [redacted] system.
2) Replacement of analog CCTV cameras with digital IP cameras at all field offices and some Regional and Headquarter offices.
3) Implementation and upgrade of agency SOCs at Virginia Square (VASQ) and 1776 F Street owned Headquarters buildings.
4) Installation and upgrade of owned Headquarters (VASQ, 1776 F Street and Main Building) vehicle access control points (VACP). This consists of crash-rated AVB's, ballistic guard booths, high-speed garage doors, automated controls, enhanced ESS and video intercoms.
5) Installation of card readers in the 3701 Fairfax Drive Building elevators to prevent unauthorized access to FDIC leased space by separating public common space from FDIC space.
6) Reset Headquarters lobby doors to lockdown Monday through Friday at 5:30 p.m. to limit access by the general public.
7) Changed access hours from 24-hour access to limit contractor access and set normal working hours Monday through Friday 5:00 a.m. to 7:00 p.m.

Planned upgrades and initiatives to be executed under the ESS contract consist of, but are not limited to, the following:

1. Upgrade of [redacted] hardware and software and network migration. This will upgrade the software to a modern platform, replace unsupported hardware, increase system performance, enhance functionality, and position FDIC for migrating ESS from the current standalone Verizon network to the agency AT&T production network. This network migration is currently being planned, tested and coordinated in conjunction with the FDIC CIO organization. The result of this migration is phasing out the Verizon network and contract, increasing failover, redundancy and resiliency capabilities of the systems, ensures appropriate cyber security controls are implemented, integration with agency priority initiatives (i.e., eWORKS) and creation of an integrated physical access converged enterprise solution (PACES).
2. Upgrade of the legacy video surveillance systems (VSS) with a VSS that is more cost effective, capable of enterprise management, integrates with 40+ camera manufacturers, integrates with C-Cure, has built-in analytics, ability to view live and recorded video simultaneously and other capabilities.
3. Upgrade of remaining analog CCTV cameras to an IP based VSS at FDIC offices nationwide. This will standardize VSS assets for live and recorded video nationwide, provide additional capabilities (analytics, video IDS, etc.), network bandwidth reduction technology and other capabilities.
4. Upgrade of legacy intercoms nationwide with IP addressable and networkable video intercoms.
5. Lifecycle replacement (LCR) of lobby turnstiles within owned headquarters (VASQ, 1776 F Street, and Main Building) facilities to provide greater security and accountability for employees and visitors.

6. Implementation of a new visitor management system to provide visitor vetting capabilities, automate manual processes, enforce escort policies, implement more secure visitor credentials, and create accountability for visitor population.
7. Implementation of a new parking management/enforcement system and license plate reader (LPR) technology to assist in parking management and enforcement efforts, automate manual processes (e.g. visitor management tie-in) and provide enhancements to investigative efforts.
8. Implementation of the Physical Access Converged Enterprise Solution (PACES) to provide a holistic approach to identity management, automating and integrating physical security systems and processes, enterprise management and communication with authoritative data sources (e.g. CHRIS, USAccess), as well as positioning FDIC to converge logical and physical access.

The OIG made nine recommendations to the FDIC to strengthen the Agency's Physical Security Program. Our responses below contain actions already planned or in process for each recommendation along with an alternative action for recommendation # 3.

Recommendation 1: Revise and update the FDIC Physical Security Program Circular and develop and implement procedures to define the roles, responsibilities, and requirements for physical security risk management activities and decision-making. These revisions should include:

a. Ensuring that there is sufficient documentation and support for physical security risk management activities and decisions, including those decisions related to when the ISC standards were determined to be not practical.
b. Ensuring that each FSL determination is documented, accurate, and adequately supported.
c. Ensuring that if an FSL is revised, the FDIC reviews the countermeasures and risk mitigation strategies for the facility.
d. Updating and reviewing facility security plans on an annual basis;
e. Ensuring that all FSA recommendations are identified, prioritized, and tracked;
f. Identifying requirements for pre-lease physical security activities and deliverables;
g. Requiring that FDIC senior management be routinely advised of the status of the Physical Security Program at FDIC Headquarters, Regional, Area, and Field Offices.

Management Decision: Concur

Corrective Actions:

DOA will revise the FDIC Physical Security Program Circular 1610.1 and develop Standard Operating Procedures (SOP) to more completely define the specific roles, responsibilities, and requirements for physical security risk management activities and decision making. Updates to Circular 1610.1 and SOP will ensure that:

a. There is sufficient documentation and support for physical security risk management activities. Any deviation from ISC standards will be justified and documented.
b. Each FSL determination is documented, accurate, and adequately supported.
c. If an FSL is revised, the FDIC reviews the countermeasures and risk mitigation strategies for the facility.
d. Facility security plans are updated and reviewed on an annual basis.
e. All FSA recommendations are identified, prioritized, and tracked.
f. Requirements for pre-lease physical security activities and deliverables are identified.
g. FDIC senior management is advised of the Physical Security Program on a periodic and as needed basis.

Estimated Completion Date: December 31, 2019

Recommendation 2: Establish and implement training requirements for personnel conducting FSL determinations and FSAs.

Management Decision: Concur

Corrective Actions:

DOA will incorporate training requirements into the FDIC Physical Security Program Circular 1610.1 for SEPS personnel engaged in the conduct of FSL determinations and FSAs. At a minimum, required training will include completion of both the ISC 1170 Series courses and Federal Risk Management Process (FED-RMP) Certification course. A requirement for periodic refresher training will also be incorporated into the Circular.

Estimated Completion Date: December 31, 2019

Recommendation 3: Establish and implement controls to ensure that DOA maintains security assessment-related records in accordance with the FDIC Records and Information Management Policy Manual.

Management Decision: Concur

Corrective Actions:

DOA will incorporate into revised Circular 1610.1 requirements to maintain security assessment-related records in accordance with the FDIC Records and Information Management Policy Manual. With regards to the records retention schedule, DOA will adhere to requirements outlined in the ISC guidelines which call for a longer retention period of the security assessment related-records than what the current FDIC retention period dictates. DOA SEPS has already discussed the ISC records retention requirements with the DOA Records and Information Management Section (RIM) and RIM agrees that the retention period should align to the ISC

guidelines. Specific reference to ISC security records retention requirements will be incorporated into Circular 1610.10 and the planned new Security SOP.

Estimated Completion Date: December 31, 2019

Recommendation 4: Implement an automated FSA template, tool, or other mechanism to ensure that the FSAs consider all threat, consequence, and vulnerability assessments of undesirable events and assess relevant countermeasures for each FDIC facility. This tool or mechanism should track and record:

a. Recurring, structured testing and maintenance programs for the FDIC's electronic security systems;
b. Controls for electronic building and access systems (BACS) at FDIC facilities;
c. Security countermeasures for child-care centers in FDIC facilities; and
d. Facility Security Plans for FDIC facilities.
e. Accurate FSL and FSA data.

Management Decision: Concur

Corrective Actions:

DOA has signed a Memorandum of Agreement (MOA) with the Department of Homeland Security Federal Protective Service (DHS-FPS) for the use of the DHS-FPS Modified Infrastructure Survey Tool (MIST). MIST is an automated vulnerability assessment tool used to conduct FSAs. The tool will be used by DOA-SEPS to review and document the security posture, current level of protection, and recommended countermeasures for each FDIC facility. The application of MIST will ensure that all threats, consequences, and vulnerabilities of undesirable events are considered and will assess relevant countermeasures for FDIC facilities. In addition, MIST will enable FDIC to track and record bulleted items "a" through "e" as recommended by the OIG. The MOA includes DHS-FPS training that will be completed by 1st Quarter 2019. MIST will be fully in place by 2nd Quarter 2019.

Estimated Completion Date: August 30, 2019

Recommendation 5: Track and record training programs for physical security awareness that is provided to FDIC employees and contractors annually.

Management Decision: Concur

Corrective Actions:

DOA SEPS is currently developing a web-based physical security awareness training program that it will provide annually to FDIC employees and contractors. DOA will rely on Corporate

University's Learning Management System to track and record participation in training programs. The web-based training module(s) will be completed and implemented by September 30, 2019.

Estimated Completion Date: October 31, 2019

Recommendation 6: Evaluate the resource needs for the physical security risk management process and modify resources as necessary.

Management Decision: Concur

Corrective Actions:

Consistent with Corporate guidance, DOA routinely identifies opportunities to streamline staff, reduce costs, and leverage resources where possible. As part of the 2019 budget and staffing formulation process, DOA assessed the reasonableness of its resources in SEPS as it relates to our ability to effectively implement the FDIC physical security risk management program. As a result of this assessment, DOA-SEPS recently hired a Physical Security Specialist CG-14 to help address emerging workload needs. In addition, DOA is awarding a new Physical Security Support (PSS) contract to develop a multifunctional approach for establishing a nationwide standardized Physical Security Program. The PSS contract will be awarded by May 31, 2019.

Estimated Completion Date: May 31, 2019

Recommendation 7: Document the justifications for the physical security activities that the FDIC has taken in response to recommendations, including decisions to accept risk or regarding expenditures for security countermeasures above the recommended standards for an assigned FSL.

Management Decision: Concur

Corrective Actions:

DOA will revise the FDIC Physical Security Program Circular 1610.1 and develop Standard Operating Procedures (SOP) to define the specific roles, responsibilities, and requirements for physical security risk management activities and decision making. Updates to Circular 1610.1 and SOP will provide requirements for documenting the justifications for physical security activities taken to address future FSA recommendations including decisions to accept risk or regarding expenditures for security countermeasures above the recommended standards for an assigned FSL. In addition, DOA will document the justification for installing CCTV camera equipment in FDIC Field Offices.

Estimated Completion Date: December 31, 2019

Recommendation 8: Provide the FDIC Board with revised, accurate information supporting the use of security guards at FSL II Offices and identifying the related financial impact.

Management Decision: Concur

Corrective Actions: DOA will prepare a memorandum to the FDIC Board of Directors to further explain the use of armed security guards at all Regional and Area Offices and the financial cost of doing so.

Estimated Completion Date: April 30, 2019

Recommendation 9: Identify goals and metrics for measuring the performance of the Physical Security Program to ensure the timeliness, quality, and effectiveness of FDIC risk management process activities.

Management Decision: Concur

Corrective Actions:

DOA SEPS is currently developing a series of internal performance metrics, objectives, and strategic goals based on Federal / industry best practices. This performance related information should be completed by July 31, 2019.

Estimated Completion Date: July 31, 2019

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 will revise the FDIC Physical Security Program Circular 1610.1 and develop Standard Operating Procedures to more completely define the specific roles, responsibilities, and requirements for physical security risk management activities and decision-making.	December 31, 2019	$0	Yes	Open
2	DOA will incorporate into Circular 1610.1 training requirements for DOA-SEPS personnel engaged in the conduct of FSL determinations and FSAs. At a minimum, required training will include completion of both the ISC 1170 Series courses and the Federal Risk Management Process Certification course.	December 31, 2019	$0	Yes	Open
3	DOA will incorporate into Circular 1610.1 requirements to maintain security assessment- related records in accordance with the FDIC Records and Information Management Policy Manual. DOA will adhere to record retention requirements outlined in the ISC guidelines, which call for a longer retention period of the security assessment related-records than what the current FDIC retention period dictates.	December 31, 2019	$0	Yes	Open
4	DOA signed a Memorandum of Agreement with the Department of Homeland Security Federal Protective Service for the use of their Modified Infrastructure Survey Tool (MIST). MIST is an automated vulnerability assessment tool for conducting FSAs. DOA-SEPS will use the tool to review and document the security posture, current level of protection, and recommended countermeasures for each FDIC facility. The application of MIST	August 30, 2019	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
	will enable DOA-SEPS to consider all threats, consequences, and vulnerabilities of undesirable events and will assess relevant countermeasures for FDIC facilities.				
5	DOA SEPS is currently developing a web-based physical security awareness training program that it will provide annually to FDIC employees and contractors. DOA will rely on Corporate University's Learning Management System to track and record participation in training programs.	October 31, 2019	$0	Yes	Open
6	As part of the 2019 budget and staffing formulation process, DOA assessed the reasonableness of its resources in SEPS. As a result, DOA-SEPS recently hired a Physical Security Specialist CG-14 to help address emerging workload needs. In addition, DOA is awarding a new Physical Security Support contract to develop a multifunctional approach for establishing a nationwide standardized Physical Security Program.	May 31, 2019	$0	Yes	Open
7	DOA will revise Circular 1610.1 and develop Standard Operating Procedures to define the specific roles, responsibilities, and requirements for documenting the justifications for decisions to accept risk or regarding expenditures for security countermeasures above the recommended standards for an assigned FSL. In addition, DOA will document the justification for installing CCTV camera equipment in FDIC Field Offices.	December 31, 2019	$0	Yes	Open
8	DOA will prepare a memorandum to the FDIC Board of Directors to further explain the use of armed security guards at all Regional and Area Offices and the financial cost of doing so.	April 30, 2019	$0	Yes	Open
9	DOA SEPS is currently developing a series of internal performance	July 31, 2019	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
	metrics, objectives, and strategic goals based on Federal / industry best practices.				

[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.