PRIVACY IMPACT ASSESSMENT (PIA) FOR VISITOR MANAGEMENT AND SECURITY INCIDENT SOLUTIONS (VMSIS)

April 16, 2026

FDIC

FEDERAL DEPOSIT INSURANCE CORPORATION

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

An FDIC Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) the FDIC collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. The FDIC publishes its PIAs, as well as its System of Records Notices (SORNs), on the FDIC's public-facing website,[1] which describes FDIC's activities that impact privacy, the authority for collecting PII, and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

Abstract

This Privacy Impact Assessment (PIA) covers the systems that the Federal Deposit Insurance Corporation (FDIC) uses to collect, process and manage personally identifiable information (PII) about members of the public who visit FDIC facilities and/or are involved in FDIC physical security incidents, such as an injury at an FDIC building or property theft or loss. The FDIC is conducting this PIA to provide transparency to the public and to assess and mitigate any risks associated with FDIC's collection, use, and maintenance of this PII.

Background

The FDIC is an independent agency of the U.S. government charged with maintaining stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions, making large and complex financial institutions resolvable, and managing receiverships.

As part of operating, FDIC provides a variety of mission-support services, including without limitation (a) hospitality-related services such as lodging, catering, conference planning, and parking; (b) facilities operations services; and (c) security enterprise services designed to protect FDIC personnel, visitors, and facilities from internal and external threats (e.g., fire, theft, vandalism, and other security concerns) and to prevent, detect, and investigate physical security incidents.

[1] www.fdic.gov/privacy

In providing these services, FDIC may collect and maintain a significant amount of data, including PII, about individuals who visit FDIC facilities for a variety of reasons, such as attending FDIC training and events, accessing the cafeteria or daycare centers within FDIC facilities, inquiring about deposit insurance, resolving examination and enforcement matters, or for interagency collaboration. Additionally, FDIC may collect and maintain PII about visitors who experience or are otherwise involved in a security incident at FDIC facilities, such as a slip and fall accident or property theft or loss. Such PII could relate to FDIC employees, contractors, interagency partners, and members of the public who access or attempt to access FDIC facilities. In some cases, PII could relate to foreign nationals who visit FDIC facilities. The type of PII varies depending on the nature of a particular visit or security incident being tracked by FDIC. This PIA focuses on the systems and associated processes that collect PII about members of the public. The section below provides additional information about the specific systems and platforms used by FDIC and the types of PII maintained within each.

Overview of VMSIS

Visitor Management and Security Incident Solutions (VMSIS) supports a range of functions related to managing physical access by visitors to FDIC facilities. VMSIS helps ensure the protection of FDIC employees, visitors, and facilities from internal and external threats (e.g., fire, theft, vandalism, and other security concerns) and the prevention, detection, and investigation of physical security incidents, such as unauthorized access, vandalism or property damage; theft or loss of property; suspicious persons/packages; workplace violence; illness or injury; or criminal incidents. VMSIS also supports the administration and management of facilities operations and the hospitality services, including lodging, cafeteria, and parking services available to FDIC employees, contractors and their visitors.

The VMSIS PIA provides coverage for the systems, programs and records listed in the table below.

System/ Project	Purpose	Data Description
Enterprise Physical Access Control Systems (ePACS)	ePACS consists of a physical access control system (PACS) and intrusion detection system (IDS) used by the FDIC to meet the personal identity verification (PIV) requirements of Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*,[2] and other federal directives. FDIC uses ePACS to produce employee and contractor photo identification access badges and to manage controlled access to FDIC facilities and suites. ePACS provides the capability to configure and manage badge readers, alarm monitoring, and output control devices. Additionally, ePACS sets up and maintains badge holder-related access parameters and monitors alarm queues.	ePACS receives data from the U.S. General Services Administration (GSA) USAccess Program,[3] with which the FDIC collaborates to facilitate the issuance of PIV cards to FDIC employee and contractor personnel nationwide. ePACS maintains data about FDIC employees, contractors, and employees from other government agencies who visit FDIC facilities, including their full name, digital photograph, access clearances, personal identification number (PIN), employment status, title, division, home office, region (if applicable), company name and FDIC Oversight Manager (OM) information (if contractors). The record also includes card information for PIV and non-PIV badges, as detailed in Question 1.1.
Enterprise Visitor Management System (EVMS)	EVMS is a visitor management system used to validate visitor identities and grant access to FDIC facilities. The system generates temporary visitor badges and allows for integration with ePACS (described above) to validate certificates and provision temporary access to visitors from other government agencies. The system is also used to issue temporary credentials to PIV card holders who forget their PIV cards. While the system can be configured to facilitate background checks on all visitors, FDIC has not deployed this functionality. FDIC visitors receive a link to EVMS to complete the visitor registration form prior to arrival. For visitors who do not pre-register, the FDIC security guard/officer will validate and manually enter their information into EVMS. In certain FDIC locations, terminals will be available for visitors to complete the pre-registration process. When FDIC visitors arrive onsite for their appointment/event, they are processed through designated FDIC security checkpoints in the lobbies of FDIC buildings. The visitor provides the FDIC security officer with an approved form of government-issued photo identification (e.g., state driver's license, passport) that will be swiped through	EVMS maintains PII about visitors to FDIC facilities, including their name; date of birth; digital photograph; contact information; physical attributes from PIV card (height, weight, eye color, etc.); organization or agency name and affiliation; date, time and purpose of visit; the name of the FDIC employee/contractor who sponsored their visit (FDIC sponsor); whether they are a foreign visitor; copies of documents used to verify identification; and other information described in Question 1.1. As applicable, the system accesses the PIV/Public Key Infrastructure (PKI) certificate (via an integration with ePACS) for the individual's PIV credentials in order to grant/provision access to FDIC facilities, but it does not store or maintain the certificate. The system also includes a notation when an individual is barred from entering FDIC facilities. Refer to the Do Not Admit subsection for more information.

[2] Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 24, 2004), https://www.dhs.gov/homeland-security-presidential-directive-12.

[3] GSA Privacy Impact Assessment (PIA) for USAccess Program (January 1, 2023), https://www.gsa.gov/system/files/GSA-USAccess-%28PIA-391%29.pdf.

System/ Project	Purpose	Data Description
	a scanner equipped with an optical character recognition (OCR) device. The security officer matches the identification with the appointment information in EVMS before credentials are provisioned or a badge is issued, as applicable.	
Property Management System	Located at FDIC's Virginia Square campus, the Student Residence Center (SRC) consists of a training and meeting facility with an accompanying hotel that offers lodging for traveling FDIC employees and their guests/visitors. FDIC leverages a cloud-based property management system to manage SRC hotel reservations, rates, inventory, guest profiles, billing, and reporting. All SRC reservations must be made through designated FDIC Division/Office Lodging Coordinators, in accordance with FDIC Directive 1800.06, *Special Events and Hospitality Services*.[4] When checking-in at the SRC, individuals must complete a registration card/form and sign the SRC Code of Conduct, which establishes the principles and expectations for professional conduct and ethical behavior for all employees and guests of the SRC.[5] They also provide a form of identification (e.g., driver's license) and may swipe their credit/debit card if they are a paying guest. The SRC Front Desk personnel match the identification with the reservation information in the property management system.	The property management system contains SRC reservation details and guest profiles, which include PII such as visitors' and guests' full names, contact information, and vehicle information (if applicable) provided on the guest registration card/form. The property management system is not connected to any external reservation portals, and guests do not access or enter their information into the system directly. No persons other than authorized SRC Front Desk personnel input guest information into the system.
FDIC Hospitality - Student Residence Center and Cafeterias (HSC)	The FDIC has contracted with a third-party vendor to operate and manage HSC. The HSC system boundary covers the hardware and software components hosted within FDIC facilities. These are owned, operated and managed by the vendor. Certain components within the HSC system boundary process PII about FDIC visitors, including: • Hospitality/event tool – The FDIC events team use this tool to manage meeting space reservations and associated room blocks. • Cash registers and Point-of-Sale terminals – Vendor staff use the cash registers and Point-of-Sale terminals located in the SRC and cafeterias to capture and process payments.	The hospitality/event tool within HSC interfaces with the property management system (described above), transmitting information about group details and associated rooms, including individual reservation numbers within a block. The Point-of-Sale component within HSC maintains information associated with food and beverage items purchased, type of credit card used, and the last four numbers of the customer's account number. The full debit and credit card number and details are stored by the third-party terminal vendor, not HSC.

[4] FDIC Directive 1800.06, *Special Events and Hospitality Services* (December 12, 2024).
[5] *Ibid.*

System/ Project	Purpose	Data Description
Visitor Parking Records	FDIC oversees and manages an enterprise Parking Program, which includes providing temporary parking in the FDIC's Virginia Square Building for visitors. FDIC event coordinators or sponsors may request temporary parking for visitors via email. Visitors must be registered in EVMS (discussed above).	Visitor parking requests include the visitor name, date(s) for which parking is requested, and vehicle information (e.g., vehicle make/model, vehicle color, year, vehicle state registration, and tag number). Visitor parking information is collected via email and logged by FDIC.
Foreign National Visitor Vetting Records	Pursuant to FDIC Directive 1600.09, *Intelligence and Counterintelligence Programs*,[6] the Corporation's defensive Counterintelligence Program protects the FDIC from external risks by (among other things) vetting and screening foreign visitors to FDIC facilities. Accordingly, all foreign national visitors must be vetted by the FDIC prior to entry into FDIC facilities. The FDIC Foreign National Visitor Notification form is utilized when registering foreign national visitors. The foreign national visitor completes relevant sections of the form and sends it via email or webform to FDIC. FDIC uses information provided on the form to conduct record checks to determine whether adverse information exists on a foreign national visitor and to recommend whether FDIC should deny a foreign visitor access to FDIC facilities as a result.	The FDIC Foreign National Visitor Notification form collects PII about foreign nationals who will be visiting FDIC facilities, such as full name, date and place of birth, passport information, and employment information.
Physical Security Incident Management Software	All physical security incidents must be reported in accordance with FDIC Directive 1610.01, *FDIC Physical Security Program*.[7] Examples of reportable incidents include unauthorized access; vandalism or property damage; theft or loss of property; suspicious persons or packages; workplace violence or threats; health incidents (e.g., a fall, fainting, or symptoms of illness); and criminal incidents. FDIC's security incident management system captures and maintains details about physical security incidents that occur on FDIC property. The system	Security incident case files contain information relating to FDIC physical security incidents, including the incident dates/times, a narrative/details about the incident, and other relevant incident information, such as names of individuals involved, property descriptions, vehicle information, and chain of custody information, as applicable. Depending on the nature of the incident, the case file may also include additional PII about individuals involved in the incidents, such as their contact information and other PII specified in Question 1.1. Case files may also include records obtained from

[6] FDIC Directive 1600.09, *Intelligence and Counterintelligence Programs* (June 30, 2021).
[7] FDIC Directive 1610.01, *FDIC Physical Security Program* (August 19, 2021).

System/ Project	Purpose	Data Description
	automatically tracks FDIC security officer's availability and time stamps the dispatch, arrival, and time spent on each incident. The system generates an incident file and auto populates all reports into the file for the FDIC investigator. Relevant FDIC managers and investigators are notified in real-time, allowing management oversight and response as the incident unfolds rather than after incidents have occurred. FDIC uses several investigatory methods to gather and document information on physical security incidents, including taking statements from witnesses, conducting research and interviews, and composing investigative reports. During the course of an investigation, FDIC adheres to its Security Procedural Guide and coordinates closely with the Legal Division. FDIC may share information with the Office of Professional Conduct (OPC), and other FDIC Divisions and Offices with a need to know when necessary to resolve particular matters. FDIC refers criminal matters to FDIC Office of Inspector General (OIG) and other appropriate law enforcement agencies for investigation and action, as applicable. Any external sharing, such as with local law enforcement, requires the approval of the FDIC Legal Division and other appropriate management officials specified in FDIC's security policies and procedures.	FDIC research, such as social media posts, criminal records, and police reports. Note that FDIC collects the minimum amount of PII necessary to respond to and document the incident, in accordance with FDIC policy and procedures. For example, for health incidents, the incident report typically captures the fact that an incident occurred, the dates/times and nature of the incident (e.g., fall, fainting, or symptoms of illness), the FDIC security officer(s) who responded, and the actions taken in their security capacity.
Do Not Admit Records	In limited cases, FDIC receives requests to bar entry to individuals who potentially pose a safety or security risk to FDIC personnel or property. FDIC Physical Security coordinates with the Legal Division on all such requests and completes an internal "Do Not Admit" form that documents the justification for barring entry, the FDIC POCs to contact if the individual attempts to gain entry, and details about the individual.	Do Not Admit records include the following PII about individuals prohibited from entry to FDIC facilities: full name and nicknames, contact information (email and address), physical description, date of birth and photograph (if available), vehicle description (if applicable/known), dates and details of why the individual has been barred from FDIC facilities, and the names of FDIC POCs to contact if the individual attempts to access FDIC facilities. FDIC adds a "Do Not Admit" notation in relevant visitor files in EVMS to alert FDIC security guards when an individual is barred from entry, but does not store the "Do Not Admit" form or associated records in EVMS. "Do Not Admit" records are maintained securely in locked filing cabinets and in the security incident management system (described above). Additionally, hardcopies of active "Do Not

System/ Project	Purpose	Data Description
		Admit" forms are maintained in binders accessible only to security guards in garage posts and other entry points of FDIC facilities.

The FDIC is conducting this PIA to evaluate and provide transparency to the public about FDIC's collection, use, and maintenance of PII about visitors to FDIC facilities. Note that FDIC has conducted a separate PIA that covers the Video Surveillance System Monitoring Program (VSSMP), which captures real-time and recorded visual information in and around FDIC facilities to aid in crime prevention and forensic analysis, enhance personnel safety, and secure critical assets.[8]

Additionally, FDIC has documented in multiple FDIC System of Records Notices (SORNs) the records about individuals that are processed or maintained within VMSIS. Such SORNs include: FDIC-009, *Safety and Security Incident Records*;[9] FDIC-012, *Financial Information Management Records*;[10] FDIC-015, *Personnel Records*;[11] FDIC-027, *Parking Program Records*;[12] FDIC-035, *Credentialing, Facility Access, and Visitor Management Records*;[13] FDIC-040, *Mailing, Event, and Other Contact Lists*;[14] and FDIC-041, *Personal Information Allowing Network Operations*.[15] The context of the data being processed by the VMSIS tools determines the applicable SORN, with examples provided in Question 2.2.

It should be noted that the Privacy Act of 1974 generally protects the privacy of U.S. citizens and lawful permanent residents. Accordingly, FDIC has determined that its collection of information about foreign national visitors described in this PIA does not require a Privacy Act SORN or Privacy Act Statement. In instances where FDIC has determined that notice is not required or feasible, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one. Additionally, FDIC provides direct notice to foreign national visitors on the FDIC Foreign National Visitor Notification form, which they are required to complete prior to being granted access to FDIC facilities.

---

[8] FDIC PIA for VSSMP PIA (July 20, 2022), https://www.fdic.gov/about/privacy-impact-assessments-pias.

[9] FDIC SORN-009, *Safety and Security Incident Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.

[10] FDIC SORN-012, *Financial Information Management Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.

[11] FDIC SORN-015, *Personnel Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.

[12] FDIC SORN-027, *Parking Program Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.

[13] FDIC SORN-035, *Credentialing, Facility Access, and Visitor Management Records*, 91 FR 8239 (February 20, 2026), https://www.fdic.gov/about/system-records-notices.

[14] FDIC-040, *Mailing, Event, and Other Contact Lists*, 87 FR 66696 (November 4, 2022), https://www.fdic.gov/about/system-records-notices.

[15] FDIC SORN-041, *Personal Information Allowing Network Operations*, 88 FR 27509 (May 2, 2023), https://www.fdic.gov/about/system-records-notices.

PRIVACY RISK SUMMARY

In conducting this PIA, FDIC identified potential privacy risks, which are summarized below and detailed in the subsequent sections of this PIA. As indicated, recommendations to mitigate those risks were addressed with stakeholders during the assessment. The privacy risks for this system are categorized within the following privacy functional areas:

- Data Minimization;
- Data Quality and Integrity; and
- Purpose & Use Limitation

Data Minimization Risk:

Privacy Risk: There is a risk that the PII collected within the various VMSIS components, particularly those supporting physical security investigations, may be unnecessary or excessive, or may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: FDIC collects the minimum amount of information necessary to confirm the identities of visitors to FDIC facilities, credential or issue badges, and provide support services, such as hospitality and lodging at the SRC. All FDIC users are required to complete annual Information Security and Privacy Awareness Training, which addresses the creation, maintenance and retention of FDIC records. Additionally, FDIC Directive 1360.09, *Protecting Information*,[16] requires that information only be collected and retained when it is necessary to satisfy an FDIC business requirement. Further, FDIC users are responsible for complying with FDIC Directive 1210.01*, Records and Information Management Program*,[17] which is informed by the Federal Records Act and National Archives and Records Administration (NARA) regulations.

In terms of PII collected in the context of physical security investigations, this risk is mitigated by FDIC users being appropriately trained, and by FDIC policies for data minimization, coupled with FDIC's policies, procedures and responsibilities for conducting physical security investigations. FDIC investigators are not law enforcement officers; they are FDIC contractors with defined requirements and training. FDIC investigations are internal, administrative fact-finding and documentation activities to determine the nature of an incident. FDIC investigations may result in a referral to a law enforcement agency for investigation of a potential violation of law or to internal FDIC offices like the Office of Professional Conduct for appropriate follow-up, such as a full administrative investigation into the conduct of an FDIC employee. FDIC investigators are trained to collect only the information necessary to support

[16] FDIC Directive 1360.09, *Protecting Information* (March 2, 2024), https://www.fdic.gov/formsdocuments/d1360-09.pdf

[17] FDIC Directive 1210.01*, Records and Information Management Program* (November 8, 2024).

the investigation and OIG and other law enforcement, if applicable. Accordingly, FDIC investigators restrict the collection of social media and criminal information to rare and limited circumstances where the information is necessary for a physical security purpose (e.g., a photograph for a Do Not Admit request). Similarly, in the case of a health incident or an incident involving workplace violence, FDIC collects the minimum amount of PII necessary to document and respond to the incident. The incident report captures basic facts about the incident, such as the type, location and date/time of the incident; the name of the individual(s) involved if known; and any actions taken by FDIC security officers to respond to the incident. For health incidents, medical details beyond what is operationally necessary for the security record are expressly excluded from collection. Further, physical security incident reports undergo several levels of review to ensure accuracy and the inclusion of only relevant and necessary information. FDIC Physical Security personnel have oversight over the work of the investigators and make all decisions regarding case closures or other next steps.

Data Quality & Integrity Risk:

Privacy Risk: There is a risk that information about individuals in certain VMSIS components could be inaccurate. As an example, there is a risk associated with the accuracy of foreign national names in VMSIS, as well as a risk that FDIC could obtain inaccurate source data about foreign nationals. Specifically, translation errors may occur when a foreign national name is adapted from its native alphabet. Name translation errors could result in misidentification of the foreign national requesting access to FDIC facilities. Additionally, information obtained by FDIC during the vetting process for foreign nationals could be inaccurate.

Mitigation: To mitigate this risk, FDIC collects information directly from the foreign nationals or their representative via an FDIC form (FDIC Foreign National Visitor Notification Form) and verifies the information for accuracy by checking it against information collected and maintained by U.S. government agencies. To minimize risks associated with translation errors, the FDIC Foreign National Visitor Notification Form requests additional information, such as date of birth and country of citizenship, to validate a foreign national's identity.

Further, FDIC trains its personnel on intelligence and information evaluation techniques and clearly identifies its sources and judgements when providing a final risk recommendation for a foreign national visitor. Identities are checked against multiple databases to ensure vetting results are attributed correctly.

Purpose and Use Limitation Risk:

Privacy Risk: There is a risk that information in VMSIS could be used or disclosed for a purpose not compatible with the original purposes for which the information was collected.

Mitigation: Through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Directive 1360.09, *Protecting Information*.[18] VMSIS restricts access to data to users with a "need-to-know" who require the information to perform their job responsibilities. Any disclosures outside of VMSIS are initiated by authorized FDIC personnel who have a responsibility to share the information for purposes that are compatible with the purpose for which the PII was originally collected and/or that are otherwise legally authorized or required by statute, federal court rules, or responsive document requests. Any information disclosures or withholdings are made based on the nature of the records and, as applicable, pursuant to the routine uses and exemptions in the SORNs that cover those records.

Privacy Risk: There is a risk that PII maintained in VMSIS could be accessed or used inappropriately or for unauthorized purposes.

Mitigation: To help prevent unauthorized access and use of information, VMSIS employs role-based permissions to restrict access to VMSIS and the data contained therein to only authorized FDIC employees and contractors who have a "need-to-know" in order to fulfill their job responsibilities. VMSIS administrators grant access to users, and each individual user must be properly credentialed. In addition, all FDIC users are subject and must adhere to agency policies and procedures for using, sharing and safeguarding PII. All users receive annual Information Security and Privacy Awareness training, as well as specialized training, as applicable, which helps ensure PII is handled and safeguarded appropriately. Certain VMSIS systems and platforms are capable of generating and maintaining detailed audit logs that capture a user's unauthorized use of information contained within the respective platform.

[18] FDIC Directive 1360.09, *Protecting Information* (March 2, 2024), available at: https://www.fdic.gov/formsdocuments/d1360-09.pdf

Section 1.0: Information System

1.1 What information about individuals, including PII (e.g., name, Social Security number, date of birth, address) and non-PII, will be collected, used or maintained in the information system or project?

VMSIS processes the following PII about FDIC visitors to confirm their identity and determine their access eligibility: full name, PIV/PKI certificates/credentials (if applicable), date of birth, physical/mailing address, phone numbers, email address, physical attributes (height, weight, hair color, eye color) derived from PIV, and driver's license or passport information (if applicable). The system also maintains the name of the visitor's company, their position title, length of visit, whether the visitor is a foreign guest (if applicable), and the name of the FDIC employee/contractor who sponsored their visit (FDIC sponsor).

For foreign national visitors, the FDIC collects the following types of PII: full name, date and place of birth, passport information, and employment information. Within VMSIS, EVMS maintains the name of foreign national visitors, the dates of their visits, and their FDIC sponsor in order to permit and facilitate their access to FDIC facilities. EVMS does not ingest or maintain copies of records reviewed as part of the vetting process. The Visitor Notification form and final recommendations/notations from the vetting process are stored in a secure document management repository.

In cases where visitors/guests of FDIC employees lodge at the FDIC Student Residence Center, the property management system within VMSIS maintains their reservation details and guest profiles, which include PII such as their full name, contact information (address, telephone number, and email address), and vehicle information (if applicable for parking purposes).

For visitors who make purchases in the FDIC cafeteria or pay for lodging at the Student Residence Center, the Point-of-Sale components of VMSIS receive a token and last four (4) digits of the debit/credit card number, the card expiration date, and card type. The full card number and details are stored by the third-party terminal vendor, not in VMSIS.

For visitors who park at FDIC facilities, FDIC collects the following information to issue them parking permits: name, vehicle information (make, model, color, year), vehicle license number, state of registration, and contact information.

VMSIS also maintains PII about individuals who experience, commit, or are otherwise involved with physical security incidents at FDIC facilities, which may include their

name, address, date of birth, telephone number, email address, employment status and position information, photographs, vehicle license plate, official government-issued identification source, and SSNs (in cases where it is necessary to fully identify a person related to a legal case). Certain incident records may include social media posts, criminal records, and police reports. In the case of a health incident, FDIC collects the minimum amount of information necessary to respond to and document the incident. The incident record typically captures the fact that a health incident occurred, the dates/times and nature of the incident (e.g., fall, fainting, or symptoms of illness), the security officer(s) who responded, and the actions taken in their security capacity.

PII Element	Yes
Full Name	☒
Date of Birth	☒
Place of Birth	☒
Social Security number (SSN)	☒
Employment Status, History or Information	☒
Mother's Maiden Name	❒
Certificates (e.g., birth, death, naturalization, marriage)	❒
Medical Information	☒
Address	☒
Phone Number(s)	☒
Email Address	☒
Employee Identification Number (EIN)	❒
Financial Information (e.g., checking account #/PINs/passwords, credit report)	☒
Driver's License/State Identification Number	☒
Vehicle Identifiers (e.g., license plates)	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records)	☒
Education Records	☒
Criminal Information	☒
Military Status and/or Records	☒
Investigation Report or Database	☒

PII Element	Yes
Biometric Identifiers (e.g., fingerprint, voiceprint)	☒
Photographic Identifiers (e.g., image, video)	☒
User Information (e.g., User ID, password)	☒
Specify other: Information obtained from commercial databases, publicly available records, security case number, office/room number, and passport information.	☒

1.2 What are the sources of the PII in the information system or project?

Data Source	Description of Information Provided by Source
FDIC Sponsors and Visitors	FDIC visitors and their sponsors provide information to facilitate visitor access to FDIC buildings. Visitors provide more detailed information about themselves (detailed in Section 1.1) via EVMS for pre-screening purposes and/or when they arrive onsite at FDIC facilities. Authorized FDIC employees and contractors have the ability to manually enter and update visitor information in VMSIS. Visitors who lodge at the Student Residence Center will provide their name, contact information, and vehicle information (if applicable) to SRC Front Desk staff. Additionally, visitors who lodge at SRC or make purchases in FDIC cafeterias will swipe their credit or debit cards at the Point-of-Sale terminals. The full card number and details are stored by the third-party terminal vendor, not by VMSIS.
Individuals Involved in Physical Security Incidents, Complaints, or Requests	FDIC collects information from individuals involved in physical security incidents. FDIC gathers this information via in-person interviews, phone, email, or fax and manually enters incident details into the incident management system. FDIC may also receive "Do Not Admit" requests or other requests for investigations. FDIC Physical Security personnel coordinate with the Legal Division prior to initiating such investigations, and pending Legal approval, may conduct research using criminal, commercial or publicly available sources as described below.
FDIC Systems, Programs, and Vendors/Contractors	VMSIS integrates with other FDIC systems for user authentication, to grant permissions to locations throughout FDIC facilities, and to validate and provision certificates of FDIC employees/contractors and visitor credentials. Information may also be obtained from relevant FDIC Divisions/Offices and systems when investigating security incidents or responding to requests or complaints relating to physical security. Within VMSIS, the property management system interfaces with the hospitality/event tool, transmitting information about group details and associated rooms.

Data Source	Description of Information Provided by Source
	Point-of-Sale terminals and cash registers in the FDIC's SRC and cafeteria allow the clerk at the register to ring up customer/visitor purchases, process the payment via the connected Point-of-Sale terminal, and keep records of all financial transactions. The full debit and credit card information is stored with the Point-of-Sale vendor, not in VMSIS.
Government Agencies and Law Enforcement Authorities	Within VMSIS, ePACS receives data from the U.S. General Services Administration (GSA) USAccess Program,[19] with which the FDIC collaborates to facilitate the issuance of PIV cards to FDIC employee and contractor personnel nationwide. The services provided by USAccess include enrollment services, systems infrastructure, PKI certificates and maintenance of identity accounts, card production, and finalization. ePACS allows for integration with the central federal database/repository that maintains PKI certificates[20] for federal government agency employees and contractors. GSA manages the PKI Shared Service Providers Program, which includes PKI-compliant service offerings to support Federally issued PIV and PIV-I, as well as associated certificates and cryptographic key service programs.[21] As applicable, FDIC refers matters to and coordinates with law enforcement authorities to gather and provide information pertinent to FDIC physical security incidents. The sharing of any information with law enforcement by FDIC must be approved by the Legal Division and other appropriate management officials defined in FDIC policies and procedures. Law enforcement authorities provide police reports for FDIC incidents that may result in criminal prosecution. Authorities typically provide the reports to FDIC via secure email after discussing the matter with FDIC via phone or in-person. Additionally, FDIC may share with or receive information from the Federal Bureau of Investigation, Central Intelligence Agency, National Security Agency, or other U.S. Government agencies that collect and retain threat-related information on foreign nationals to identify threats.

[19] GSA Privacy Impact Assessment (PIA) for USAccess Program (January 1, 2023), https://www.gsa.gov/system/files/GSA-USAccess-%28PIA-391%29.pdf.
[20] Government-Wide System of Records Notice (SORN) GSA/GOVT 7, *HSPD-12 USAccess*, 80 FR 64416 (October 23, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-10-23/pdf/2015-26940.pdf.
[21] For more information about the GSA PKI Shared Service Providers Program, see https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/multiple-award-schedule-it/pki-shared-service-providers-program.

Data Source	Description of Information Provided by Source
Commercial, Open Source, and Other Third-Party Data Sources	FDIC leverages commercial databases to conduct basic fact finding and reference checks for physical security incidents when applicable. In limited cases, FDIC may gather information from open-source databases and publicly available records, such as criminal records and social media posts, as part of researching a security incident or request requiring investigation. Authorized FDIC employees and contractors manually enter notes and/or append relevant information to the case file in VMSIS. Upon receipt of a foreign national visitor request, FDIC checks various commercial, open source and publicly available sources to identify any threat information. FDIC does not ingest records from these sources into VMSIS.

1.3 Has an Authority to Operate (ATO) been granted for the information system or project?

All FDIC information systems must achieve an ATO via the Assessment & Authorization process that aligns with the Risk Management Framework. Information systems that process visitor management and security incident information have been granted ATOs or are in the process to achieve ATO. The ATO for each FDIC system is periodically reviewed as part of the FDIC Ongoing Authorization process.

Section 2.0: Transparency

Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

2.1 How does the agency revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change?

Through the conduct, evaluation, and review of PIAs and SORNs, the FDIC ensures notices are revised to reflect changes in practice or policy that affect PII or changes in activities that may impact Privacy as soon as practicable.

2.2 In the Federal Register, under which Privacy Act Systems of Records Notice (SORN) does this information system or project operate? Provide number and

name.

The following SORNs apply to this project: FDIC-009, *Safety and Security Incident Records*;[22] FDIC-012, *Financial Information Management Records*;[23] FDIC-015, *Personnel Records*;[24] FDIC-027, *Parking Program Records*;[25] FDIC-035, *Credentialing, Facility Access, and Visitor Management Records*;[26] FDIC-040, *Mailing, Event, and Other Contact Lists*;[27] and FDIC-041, *Personal Information Allowing Network Operations.*[28]

The context of the data being processed by the VMSIS tools determines the applicable SORN. For example, any records relating to a physical security incident would be covered by FDIC-009, *Safety and Security Incident Records*,[29] whereas any records relating to visitor badging would be covered by FDIC-035, *Credentialing, Facility Access, and Visitor Management Records*.[30] FDIC-041, *Personal Information Allowing Network Operations*,[31] covers any logs, audits, or other security data regarding use of FDIC information technology resources, including access to and use of VMSIS resources by authorized individuals.

2.3 If the information system or project is being modified, will the Privacy Act SORN require amendment or revision? Explain.

Within VMSIS, EVMS is replacing the legacy visitor management system. FDIC published a modified SORN (FDIC-035) to enhance transparency.

---

[22] FDIC SORN-009, *Safety and Security Incident Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.
[23] FDIC SORN-012, *Financial Information Management Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.
[24] FDIC SORN-015, *Personnel Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.
[25] FDIC SORN-027, *Parking Program Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.
[26] FDIC SORN-035, *Credentialing, Facility Access, and Visitor Management Records*, 91 FR 8239 (February 20, 2026), https://www.fdic.gov/about/system-records-notices.
[27] FDIC-040, *Mailing, Event, and Other Contact Lists*, 87 FR 66696 (November 4, 2022), https://www.fdic.gov/about/system-records-notices.
[28] FDIC SORN-041, *Personal Information Allowing Network Operations*, 88 FR 27509 (May 2, 2023), https://www.fdic.gov/about/system-records-notices.
[29] FDIC SORN-009, *Safety and Security Incident Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.
[30] FDIC SORN-035, *Credentialing, Facility Access, and Visitor Management Records*, 91 FR 8239 (February 20, 2026), https://www.fdic.gov/about/system-records-notices.
[31] FDIC SORN-041, *Personal Information Allowing Network Operations*, 88 FR 27509 (May 2, 2023), https://www.fdic.gov/about/system-records-notices.

Generally, the FDIC conducts reviews of its SORNs every five years or as needed.

2.4 If a Privacy Act Statement[32] is required, how is the Privacy Act Statement provided to individuals before collecting their PII? Explain.

The FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Directive 1213.01 "FDIC Forms Management Program."

VMSIS components do not collect information directly from FDIC visitors, with the exception of EVMS, which will allow visitors to electronically provide their information through a system link in advance of their visit. A Privacy Act Statement will be provided to visitors as part of the digital registration process/form they complete within the new system workflow.

In cases where VMSIS does not collect information directly from individuals, the FDIC provides notice to individuals at the original point of collection wherever possible. For example, a Privacy Act Statement is provided to FDIC visitors who lodge at the SRC on the Code of Conduct form they complete during check-in. When VMSIS receives or derives PII from other FDIC record systems, the FDIC provides notice to individuals at the original point of collection through the respective Privacy Act Statements, SORNs, and PIAs, as applicable, for those source systems. In addition, this PIA serves as notice to the public about FDIC's collection and use of information in VMSIS.

When VMSIS processes data from a government agency or other third-party entity, it is incumbent upon the source entity to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, this PIA serves as the notice of information collection.

When FDIC collects information as part of an ongoing investigation, individuals may not receive notice as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable law, discovery rules, and court orders. When notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

It should be noted that the Privacy Act of 1974 generally protects the privacy of U.S. citizens and lawful permanent residents. FDIC has determined that its collection of information about foreign nationals described in this PIA does not require a Privacy Act SORN or Privacy Act Statement. Nonetheless, the FDIC provides direct notice to

[32] *See* 5 U.S.C. §552a(e)(3). The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.

foreign nationals via the FDIC Foreign National Visitor Notification form, which advises them that FDIC will use the information they provide to vet them and to determine if access may be granted to an FDIC facility and that failure to furnish the requested information may delay or prevent their access. Additionally, this PIA provides constructive notice about FDIC's collection and use of information in VMSIS.

2.5 How does the information system or project ensure that its privacy practices are publicly available through organizational websites or otherwise? How does the information system or project ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)? Explain.

The FDIC Privacy Program page provides access to agency SORNs, PIAs, Privacy Policy, and contact information for the SAOP, the Privacy Program Chief, and the Privacy Program (Privacy@fdic.gov). For more information on how FDIC protects privacy, please visit www.fdic.gov/privacy.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: There is a risk that certain individuals may not be aware that their information is collected and maintained within certain VMSIS components. In particular, visitors who are subjects of FDIC physical security investigations and/or deemed as prohibited from accessing FDIC facilities may not be aware of or have an opportunity to opt out of the collection and use of their information.

Mitigation: FDIC generally collects information directly from FDIC visitors and their sponsors, providing notice and consent opportunities at the time of collection. In some cases, however, it is not practical or feasible to provide advance notice and/or consent opportunities to individuals, such as when an individual is a subject of an FDIC investigation and/or identified as a potential safety or security risk to FDIC personnel or property.

During the course of an investigation, FDIC adheres to its Security Procedural Guide and coordinates closely with the Legal Division and other relevant stakeholders, such as FDIC OIG and law enforcement, as applicable. Depending on the nature of the investigation, FDIC provides notice to individuals when conducting interviews and taking witness statements. They may ask individuals if they wish to consent to particular uses of the information they provide. For example, if an individual requests confidentiality they will be advised of the extent to which confidentiality can be provided under applicable laws and regulations. However, some PII collected and maintained by FDIC may be obtained in connection with investigations of incidents or other potential criminal activity for which prior notification cannot be provided as it could compromise the integrity of the investigation or jeopardize public safety. FDIC refers criminal matters to FDIC OIG and law enforcement for investigation and action, as applicable.

FDIC-009, *Safety and Security Incident Records*,[33] provides exemptions from the Privacy Act requirements related to notification and access with respect to certain investigative information. Access to certain investigative information will be provided to an individual where a lawful requirement to provide such information exists. Additionally, investigative information collected by FDIC may be disclosed to an individual pursuant to federal rules of civil or criminal procedure or court order.

In instances where prior notice is not required or cannot be provided, this PIA and the SORNs referenced in Question 2.2 provide constructive notice and transparency related to the collection and maintenance of PII by VMSIS.

Privacy Risk: Foreign national visitors from whom data is collected may use a representative, such as Embassy staff, to provide their data. There is a risk that the representative may not convey the notice/instructions provided on the FDIC Foreign National Visitor Notification form, which explains why FDIC is requesting the information, how the information will be used, and the consequences of not furnishing the requested information.

Mitigation: The Privacy Act of 1974 generally protects the privacy of U.S. citizens and lawful permanent residents. Accordingly, FDIC has determined that its collection of information about foreign nationals described in this PIA does not require a Privacy Act SORN or Privacy Act Statement. Nonetheless, the FDIC provides direct notice to foreign national visitors invited or requesting to visit FDIC facilities via the FDIC Foreign National Visitor Notification form. The form advises foreign national visitors that FDIC will use the information to vet them to determine if access may be granted to an FDIC facility and that failure to furnish the requested information may delay or prevent their access. In instances where a foreign national visitor uses a representative to coordinate completion of the form, it is the responsibility of that representative to convey the notice to the prospective foreign national visitor. Additionally, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

[33] FDIC SORN-009, *Safety and Security Incident Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.

Section 3.0: Access and Amendment

Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

3.1 What are the procedures that allow individuals to access their information?

The FDIC provides individuals with access to their PII maintained in FDIC's systems of records as specified by the Privacy Act of 1974 and the FDIC's Privacy Act regulations at 12 CFR Part 310. Access procedures for VMSIS are detailed in the SORNs listed in Question 2.2 of this PIA. The FDIC publishes its SORNs on the FDIC public-facing website, and each SORN includes instructions for how individuals may request access to records that are maintained in each system of record, as specified by the Privacy Act and 12 CFR Part 310. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Depending on the nature of the records being processed in VMSIS (and any applicable Privacy Act exemptions), FDIC may be unable to provide individual access to records as they could inform the subject of an ongoing investigation or reveal a prospective investigative interest on the part of FDIC. FDIC-009, *Safety and Security Incident Records*,[34] provides exemptions from Privacy Act requirements related to individual access and amendment with respect to certain investigative-related data maintained by FDIC. While some individuals may not have a formal mechanism for access or redress, FDIC has internal mechanisms to correct inaccuracies and protect against abuse through auditing of security incident records.

In cases where VMSIS receives PII from other government agencies or third parties, individuals should contact the source entities and agencies that originated their data to amend their information.

3.2 What procedures are in place to allow the individuals to correct inaccurate or erroneous information?

Inaccurate or erroneous information will be corrected in VMSIS either by the FDIC security officer or other authorized personnel when the error is discovered upon the visitor's arrival. In the event an error is discovered after the issuance of a badge, the security officer or FDIC personnel will correct the error in the VMSIS database and issue a new badge. For visitors lodging at SRC, SRC Front Desk personnel will update any information related to their stay in VMSIS as part of the check-in process.

---

[34] FDIC SORN-009, *Safety and Security Incident Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.

The FDIC provides individuals with the ability to request amendment of inaccurate information maintained about them in FDIC's systems of records as specified by the Privacy Act of 1974 and the FDIC's Privacy Act regulations at 12 CFR Part 310. Amendment procedures for VMSIS are detailed in the SORNs listed in Question 2.2 of this PIA. The FDIC publishes its SORNs on the FDIC public-facing website, which includes instructions for how individuals may request amendment of records that are maintained in each system of record, as specified by the Privacy Act and 12 CFR Part 310. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Individuals who are subjects of and/or involved in security incidents are not granted direct access to view or amend incident records pertaining to them within VMSIS due to the investigatory nature of the system and records contained therein. As noted above, SORN FDIC-009, *Safety and Security Incident Records*,[35] provides exemptions from the Privacy Act requirements related to individual access and amendment with respect to certain investigative-related data maintained by FDIC. Nonetheless, individuals may submit a Privacy Act request to access and amend their records following the procedures outlined above. Additionally, during the course of documenting and investigating security incidents, FDIC investigators may conduct interviews and validate information directly with individuals, affording them an opportunity to correct inaccurate or erroneous information about themselves at that time.

Depending on the nature of the records being processed in VMSIS (and any applicable Privacy Act exemptions), FDIC may be unable to provide individuals with the ability to amend records as such actions could harm ongoing investigations. While some individuals may not have a formal mechanism for amendment or redress, FDIC has internal mechanisms to correct inaccuracies and protect against abuse through auditing of security incident records.

In cases where VMSIS receives or derives PII from other FDIC Privacy Act systems of records, the FDIC allows these individuals to correct or amend PII maintained by the FDIC in the respective source systems of records as specified by the Privacy Act and 12 CFR Part 310. The procedures for correcting inaccurate data are provided in each related SORN.

---

[35] FDIC SORN-009, *Safety and Security Incident Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.

3.3 How does the information system or project notify individuals about the procedures for correcting their information?

Notice is provided in this PIA, in the applicable SORNs listed in Question 2.2, and in the FDIC's Privacy Act regulations at 12 CFR Part 310.

Upon discovering a discrepancy, the FDIC security officer will either inform the visitor of the nature of the discrepancy or be informed of the discrepancy and explain that the discrepancy will be corrected in the VMSIS prior to issuance of a badge. A similar process is in place for visitors lodging at the SRC during check-in.

For individuals who are involved in security incidents, FDIC investigators who discover discrepancies may notify individuals as part of interview process or other contact with individuals, affording them an opportunity to correct inaccurate or erroneous information about themselves. However, certain investigative data maintained in security incident system has been exempted from the redress requirement.

In cases where VMSIS processes information about individuals derived from other FDIC Privacy Act systems of records, the FDIC provides notice about procedures to correct or amend PII maintained in the respective source systems as specified by the Privacy Act and 12 CFR Part 310. The notification procedures are provided in each related SORN.

Individuals seeking to correct inaccurate data can submit their request to the Legal Division, FOIA & Privacy Act Group, in accordance with FDIC regulations in 12 CFR Part 310. In addition, the VMSIS PIA is published on FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Office.

In some cases, VMSIS processes or derives data from government agencies or other third-party entities. The system or project does not have procedures for individual access in such cases. Individuals should contact these entities directly for access to their personal information.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: There is a risk that individuals may not have the opportunity to access their information or amend inaccurate information contained in certain VMSIS components, particularly the physical security incident system.

Mitigation: With respect to the systems and technologies that support FDIC physical security investigations, SORN FDIC-009, *Safety and Security Incident Records*,[36] provides detailed procedures for access and amendment to the information collected and maintained by those VMSIS components. However, SORN FDIC-009 includes an exemption from Privacy Act requirements related to individual access and amendment with respect to certain investigative-related data maintained by FDIC. While some individuals may not have a formal mechanism for access or redress, FDIC has internal mechanisms to correct inaccuracies through auditing of security incident records.

Section 4.0: Accountability

Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors and should provide appropriate training to all employees and contractors who have access to PII.

4.1 Describe how FDIC's governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy.

FDIC maintains a risk-based, enterprise-wide privacy program that is based upon sound privacy practices. The FDIC Privacy Program is compliant with all applicable laws and is designed to build and sustain public trust, protect and minimize the impacts on the privacy of individuals, while also achieving the FDIC's mission.

The FDIC Privacy Program is led by the FDIC's Chief Information Officer (CIO) and Chief Privacy Officer (CPO), who is also designated as FDIC's Senior Agency Official for Privacy (SAOP). The CIO/CPO reports directly to the FDIC Chairman and is responsible for ensuring compliance with applicable federal privacy requirements, developing and evaluating privacy policy, and managing privacy risks. The program ensures compliance with federal privacy law, policy, and guidance. This includes the Privacy Act of 1974, as amended; Section 208 of the E-Government Act of 2002; Section 522 of the 2005 Consolidated Appropriations Act; Federal Information Security Modernization Act of 2014; Office of Management and Budget (OMB) privacy policies; and standards issued by the National Institute of Standards and Technology (NIST).

[36] FDIC SORN-009, *Safety and Security Incident Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.

The FDIC's Privacy Program supports the SAOP in the management and execution of the FDIC's privacy responsibilities.

4.2 Describe the FDIC privacy risk management process that assesses privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

Risk analyses are an integral component of FDIC's Privacy Program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs). The Privacy Program looks across all FDIC systems and programs to identify potential areas of privacy risk. The PTA is used to assess systems or sub-systems, determine privacy compliance requirements, categorize systems, and determine which privacy controls should be assessed for each system.

4.3 Does this PIA capture privacy risks posed by this information system or project in accordance with applicable law, OMB policy, or any existing organizational policies and procedures?

Yes, this PIA captures privacy risks posed by the VMSIS through the privacy risk analysis sections throughout the document. PIAs are posted on FDIC's public-facing website, https://www.fdic.gov/policies/privacy/index.html.

4.4 What roles, responsibilities and access will contractors have with the design and maintenance of the information system or project?

Contractors are primarily responsible for providing operation support for information technology resources associated with VMSIS.

Due to contractors' access to PII, contractors take mandatory annual information security and privacy training. Privacy and security-related responsibilities are specified in contracts and associated Risk Level Designation documents. Privacy-related roles, responsibilities, and access requirements are documented in relevant PIAs.

4.5 Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been completed and signed for contractors who work on the information system or project? Are privacy requirements included in the contract?

Yes, appropriate Confidentiality Agreements have been completed and signed for contractors who work on VMSIS. Privacy and security requirements for contractors

and service providers are mandated and are documented in relevant contracts.

4.6 How is assurance obtained that the information in the information system or project is used in accordance with the practices described in this PIA and, if applicable, the associated Privacy Act System of Records Notice?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC monitors and audits privacy controls. Internal privacy policies are reviewed and updated as required. The FDIC Privacy Program implements a Privacy Continuous Monitoring (PCM) program in accordance with OMB Circular A-130.

4.7 Describe any privacy-related training (general or specific) that is provided to users of this information system or project.

FDIC provides VMSIS users with facility access and visitor management procedures, resources, and training materials, as applicable. FDIC also provides users with system-specific training for certain VMSIS systems and platforms to which they have access. Additionally, annual Information Security and Privacy Awareness Training is mandatory for all FDIC employees and contractors, and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program as well.

With respect to physical security incident data maintained in VMSIS, FDIC investigators collect and maintain documentation and evidence in accordance with FDIC policy and the FDIC Investigations Procedural Guide. The FDIC investigator role is a contracted job with defined requirements and training. They are required to have sufficient law enforcement and investigative experience to ensure proficient interviewing and research/investigation skills, effective case management, ethical behavior and core values, and other required skills for researching and investigating physical security incidents. Annual refresher training is required for FDIC investigators and ensures that they maintain high standards and needed investigative/research skills.

4.8 Describe how the FDIC develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

The FDIC Privacy Program develops reports both for internal and external oversight bodies through several methods, including the Annual Senior Agency Official for

Privacy (SAOP) Report as required by the Federal Information Security Management Act (FISMA), and regular reporting to the SAOP, the Chief Information Security Officer (CISO), and the Information Technology Risk Advisory Council.

4.9 Explain how this information system or project protects privacy by automating privacy controls?

Privacy has been integrated within the FDIC Systems Development Life Cycle (SDLC), ensuring that stakeholders are aware of, understand, and address Privacy requirements throughout the SDLC, including the automation of privacy controls when possible. Additionally, FDIC has implemented technologies to track, respond, remediate, and report on breaches, as well as to track and manage PII inventory.

4.10 Explain how this information system or project maintains an accounting of disclosures held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made?

The FDIC maintains an accurate accounting of disclosures of information held in each system of records under its control, in accordance with the Privacy Act of 1974 and 12 CFR Part 310.

4.11 Explain how the information system or project retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer?

The FDIC retains the accounting of disclosures as specified by the Privacy Act of 1974 and 12 CFR Part 310.

4.12 Explain how the information system or project makes the accounting of disclosures available to the person named in the record upon request?

The FDIC makes the accounting of disclosures available to the person named in the record upon request as specified by the Privacy Act of 1974 and 12 CFR Part 310.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable privacy risks related to Accountability for VMSIS.

Mitigation: No mitigation actions are recommended.

Section 5.0: Authority

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.

5.1 Provide the legal authority that permits the creation, collection, use, processing, storage, maintenance, dissemination, disclosure and/or disposing of PII within the information system or project. For example, Section 9 of the Federal Deposit Insurance Act (12 United States Code (U.S.C.) 1819).

The FDIC ensures that collections of PII are legally authorized through the conduct and documentation of PIAs and the development and review of SORNs. FDIC Directive 1360.20, "Privacy Program," mandates that the collection of PII be in accordance with Federal laws and guidance. This system or project collects PII pursuant to the following laws and regulations:

FDIC has general legal authority under Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819) to protect the buildings, grounds, and property owned or occupied by the FDIC, and the persons on the property. Additionally, certain VMSIS components collect PII pursuant to the following authorities: Executive Order 9397, as amended, and HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*.[37]

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable privacy risks related to Authority for VMSIS.

Mitigation: No mitigation actions are recommended.

[37] Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 24, 2004), https://www.dhs.gov/homeland-security-presidential-directive-12.

Section 6.0: Minimization

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.

6.1 How does the information system or project ensure that it has identified the minimum PII that are relevant and necessary to accomplish the legally authorized purpose of collection?

VMSIS collects the minimum amount of information necessary to accomplish authorized tasks, including validating the identities of visitors to FDIC facilities, credentialing and issuing badges, and providing support services, such as hospitality and lodging to FDIC employees and their guests/visitors. All FDIC users are required to complete annual Information Security and Privacy Awareness Training, which addresses the creation, maintenance and retention of FDIC records. Additionally, FDIC Directive 1360.09, Protecting Information, requires that information only be collected and retained when it is necessary to satisfy an FDIC business requirement. Further, FDIC users are responsible for complying with FDIC Directive 1210.01, Records and Information Management Program, which is informed by the Federal Records Act and NARA regulations.

In terms of PII collected in the context of FDIC physical security investigations, FDIC investigators collect and maintain documentation and evidence in accordance with FDIC policies and procedures. FDIC investigators are required to have sufficient law enforcement and investigative experience to ensure proficient interviewing and research/investigation skills, effective case management, ethical behavior and core values, and other required skills for researching and investigating physical security incidents. Annual refresher training is required for FDIC investigators and ensures that they maintain high standards and needed investigative/research skills. FDIC investigators are trained to limit information collections to only that which is relevant and necessary to support the investigation and OIG and other law enforcement, if applicable. Accordingly, FDIC investigators restrict the collection of social media and criminal information to rare and limited circumstances where the information is necessary for a physical security purpose (e.g., a photograph for a Do Not Admit request). Similarly, in the case of a health incident, FDIC collects the minimum amount of information necessary to respond to and resolve the incident. Medical details beyond what is operationally necessary for the security record are expressly excluded from collection. Further, FDIC incident reports undergo several levels of review to ensure accuracy and the inclusion of only relevant and necessary information.

Additionally, through the conduct, evaluation, and review of privacy artifacts, [38] the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

6.2 How does the information system or project ensure limits on the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent?

VMSIS generally collects information directly from FDIC visitors and their sponsors, providing notice and consent opportunities at the time of collection. In some cases, however, it is not practical or feasible to provide advance notice and/or consent opportunities to individuals, such as when an individual is a subject of a FDIC investigation or identified as a potential safety or security risk to FDIC personnel or property.

VMSIS collects the minimum PII elements needed to accomplish authorized tasks as explained in Question 6.1. With respect to PII collected in the context of FDIC physical security investigations, FDIC investigators collect and maintain documentation and evidence in accordance with FDIC policy and FDIC's Investigations Procedural Guide. FDIC investigators are required to have sufficient law enforcement and investigative experience to ensure proficient interviewing and research/investigation skills, effective case management, ethical behavior and core values, and other required skills for researching and investigating physical security incidents. Annual refresher training is required for FDIC investigators and ensures that they maintain high standards and needed investigative/research skills. FDIC investigators are trained to limit information collections to only that which is relevant and necessary to support the investigation. Accordingly, FDIC investigators restrict the collection of social media and criminal information to rare and limited circumstances where the information is necessary for a physical security purpose (e.g., obtaining a photograph for a Do Not Admit request). Similarly, in the case of a health incident, FDIC collects the minimum amount of information necessary to document and respond to the incident. Medical details beyond what is operationally necessary for the security record are expressly excluded from collection. Further, FDIC incident reports undergo several levels of review to ensure accuracy and the inclusion of only relevant and necessary information.

Additionally, through the conduct, evaluation, and review of privacy artifacts, the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally

[38] Privacy artifacts include Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Records Notices (SORN).

authorized purpose for which it is collected.

6.3 How often does the information system or project evaluate the PII contained in the information system or project to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose?

The FDIC maintains an inventory of systems that contain PII. The Privacy Program reviews information in the systems at the frequency defined in the FDIC Information Security Continuous Monitoring Strategy. New collections are evaluated to determine if they should be added to the inventory.

6.4 What are the retention periods of the data in this information system or project? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.

Records are retained in accordance with FDIC Directive 1210.01 "Records and Information Management Program," which is informed by the Federal Records Act and NARA regulations, as follows:

- Records relating to FDIC employees, contractors or other individuals who applied for, been issued, and/or used a PIV card or HSPD-12 compliant credentials are maintained for six (6) years after separation from the FDIC and then dispositioned in accordance with approved records retention schedules. PIV cards are destroyed or deactivated after expiration, confiscation, or return.
- Visitor access records are maintained for five (5) years after the requested access date and then dispositioned in accordance with approved records retention schedules. Visitor passes are destroyed or deactivated after expiration, confiscation, or return.
- The Point-of-Sale component within VMSIS maintains information associated with food and beverage items purchased for two (2) years after purchase.
- SRC guest reservation information and accompanying registration cards are destroyed/deleted six (6) years after the guest's visit.
- Records of security incidents involving lost, stolen, damaged, destroyed government or personal property are destroyed after seven (7) years; records of medical illness incidents are destroyed three (3) years after medical illness incident; and information that is collected for investigations are destroyed twenty-five (25) years after the investigation is closed.

Procedures for disposition of the data at the end of the retention period are established in accordance with FDIC Records Schedules in conjunction with NARA

guidance. For example, hard copies of any paper materials scanned into the system will be retained in accordance with FDIC Records Schedules or returned to the originating Division or Office for retention.

Additionally, records are retained in accordance with the FDIC Directive 1210.01 FDIC "Records and Information Management Program," which is informed by the Federal Records Act and NARA regulations Management Policy Manual and NARA-approved record retention schedule. Information related to the retention and disposition of data is captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in FDIC Directives 1210.01 and 1360.09 "Protecting Information."

6.5 What are the policies and procedures that minimize the use of PII for testing, training, and research? Does the information system or project implement controls to protect PII used for testing, training, and research?

The FDIC has developed an enterprise test data strategy to reinforce the need to mask or use synthetic data in the lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system.

Any production data, including PII, may not be used outside of the production environment unless management has approved a waiver, and appropriate controls have been put in place.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: There is a risk that the PII collected within the various VMSIS components, particularly those supporting physical security investigations, may be unnecessary or excessive, or may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: FDIC collects the minimum amount of information necessary to confirm the identities of visitors to FDIC facilities, credential or issue badges, and provide support services, such as hospitality and lodging at the SRC. All FDIC users are required to complete annual Information Security and Privacy Awareness Training, which addresses the creation, maintenance and retention of FDIC records. Additionally, FDIC Directive 1360.09, *Protecting Information*,[39] requires that information only be collected and retained when it is necessary to satisfy an FDIC business requirement. Further, FDIC users are responsible for complying with

[39] FDIC Directive 1360.09, *Protecting Information* (March 2, 2024), available at: https://www.fdic.gov/formsdocuments/d1360-09.pdf

FDIC Directive 1210.01*, Records and Information Management Program*,[40] which is informed by the Federal Records Act and National Archives and Records Administration (NARA) regulations.

In terms of PII collected in the context of physical security investigations, this risk is mitigated by FDIC users being appropriately trained, and by FDIC policies for data minimization, coupled with FDIC's policies, procedures and responsibilities for conducting physical security investigations. FDIC investigators are not law enforcement officers; they are FDIC contractors with defined requirements and training. FDIC investigations are internal, administrative fact-finding and documentation activities to determine the nature of an incident. FDIC investigations may result in a referral to a law enforcement agency for investigation of a potential violation of law or to internal FDIC offices like the Office of Professional Conduct for appropriate follow-up, such as a full administrative investigation into the conduct of an FDIC employee. FDIC investigators are trained to limit information collections to only that which is necessary to support the investigation and OIG and other law enforcement, if applicable. Accordingly, FDIC investigators restrict the collection of social media and criminal information to rare and limited circumstances where the information is necessary for a physical security purpose (e.g., obtaining a photograph for a Do Not Admit request). Similarly, in the case of a health incident or an incident involving workplace violence, FDIC collects the minimum amount of PII necessary to document and respond to the incident. The incident report captures basic facts about the incident, such as the type, location and date/time of the incident; the name of the individual(s) involved if known; and any actions taken by FDIC security officers to respond to the incident. For health incidents, medical details beyond what is operationally necessary for the security record are expressly excluded from collection. Further, physical security incident reports undergo several levels of review to ensure accuracy and the inclusion of only relevant and necessary information. FDIC Physical Security personnel have oversight over the work of the investigators and make all decisions regarding case closures or other next steps.

[40] FDIC Directive 1210.01*, Records and Information Management Program* (November 8, 2024).

Section 7.0: Data Quality and Integrity

Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

7.1 Describe any administrative and technical controls that have been established to ensure and maximize the quality, utility, and objectivity of PII, including its accuracy, relevancy, timeliness, and completeness.

The FDIC reviews privacy artifacts for adequate measures to ensure the accuracy, relevance, timeliness, and completeness of PII in each instance of collection or creation.

FDIC expects visitors and their FDIC sponsors to provide accurate information about themselves. After pre-registering (as described in Section 1.0), FDIC visitors arriving for appointments are processed through designated FDIC security checkpoints in the lobbies of FDIC buildings. FDIC visitors must provide the FDIC security officer with an approved form of government-issued photo identification (e.g., state driver's license, passport, etc.) and identify their FDIC sponsor. The security officer then matches the identification with the appointment information in VMSIS before credentials are provisioned or a badge is issued, as applicable. Inaccuracies are manually corrected in VMSIS by either the security officer or FDIC Physical Security personnel prior to the issuance of the badge. For example, if a visitor's first name on his or her photo identification does not match the first name stored in VMSIS due to a misspelling, the error will be corrected in the computer before badge issuance. In the event an error is discovered after the issuance of the badge, the error will be corrected in the VMSIS and a new badge will be provided, as applicable.

A similar process is followed for visitors who are authorized to lodge at the SRC. Prior to check-in at the SRC, FDIC visitors must complete the badging process and validate their identities as described above. In accordance with FDIC Directive 1800.06, *Special Events and Hospitality Services*,[41] all SRC reservations must be made through designated FDIC Division/Office Lodging Coordinators. Additionally, all FDIC employees and their guests must sign and comply with the SRC Code of Conduct, which establishes the principles and expectations for professional conduct and ethical behavior for all employees and guests of the SRC.[42] Upon check-in at the SRC, FDIC employees and their guests provide their name, contact information, vehicle information (if applicable for parking) to the SRC Front Desk personnel. They also sign

[41] FDIC Directive 1800.06, *Special Events and Hospitality Services* (December 12, 2024).
[42] *Ibid.*

the aforementioned Code of Conduct, provide a form of identification (e.g., driver's license), and swipe their credit/debit card, if they are a paying guest. The SRC Front Desk personnel match the identification with the reservation information in VMSIS. Inaccuracies are manually corrected in VMSIS by the SRC Front Desk personnel during the check-in process.

For foreign national visitors, FDIC collects information directly from them or their representative via an FDIC form (FDIC Foreign National Visitor Notification Form). FDIC reviews and verifies the information for accuracy by checking it against information collected and maintained by U.S. government agencies. To minimize risks associated with translation errors, the FDIC Foreign National Visitor Notification Form requests additional information, such as date of birth and country of citizenship, to validate a foreign national's identity. Further, FDIC trains its personnel on intelligence and information evaluation techniques. Identities are checked against multiple databases to ensure vetting results are attributed correctly.

With respect to PII collected during physical security investigations, FDIC strives to collect the most relevant and accurate information and restricts the collection of social media and criminal information to rare and limited circumstances where the information is necessary for a physical security purpose (e.g., obtaining a photograph for a Do Not Admit request). When applicable, FDIC investigators leverage police reports and victim and witness statements to corroborate the information obtained from social media and other sources during the investigation. Physical security incident reports undergo several levels of review to ensure accuracy and completeness. If any information is inaccurate or missing, an FDIC investigator contacts the witness, complainant, perpetrator, or victim to obtain the correct information.

Additionally, access to VMSIS is restricted to those who need to perform authorized business duties. VMSIS platforms utilize role-based permissions to limit user access to data, including PII, on a need-to-know basis. Further, certain VMSIS platforms have the ability to generate audit trails of user activity, including the viewing of records in the system. Technical controls within certain VMSIS systems, such as EVMS, ensure that required data is collected before a record can be saved. Access is based on a need to know and is controlled by technical controls within the software program. Data modifications are logged to provide usable audit trails.

7.2 Does the information system or project collect PII directly from the individual to the greatest extent practicable?

Yes, the project collects PII directly from FDIC visitors and their FDIC sponsors to the maximum extent possible as detailed above. Additionally, the FDIC reviews privacy

artifacts to ensure each collection of PII is directly from the individual to the greatest extent practicable.

7.3 Describe any administrative and technical controls that have been established to detect and correct PII that is inaccurate or outdated.

The FDIC reviews privacy artifacts to ensure adequate controls to check for and correct any inaccurate or outdated PII in its inventory.

7.4 Describe the guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

The FDIC's guidelines for the disclosure of information is subject to Privacy Act protections that are found in FDIC Regulations at 12 CFR Part 310.

7.5 Describe any administrative and technical controls that have been established to ensure and maximize the integrity of PII through security controls.

Through the PTA adjudication process, the FDIC Privacy Program uses the Federal Information Processing Standards Publication 199 (FIPS 199) methodology to determine the potential impact on the FDIC and individuals should there be a loss of confidentiality, integrity, or availability of the PII. The Office of the Chief Information Security Officer validates the configuration of administrative and technical controls for the system or project based on the FIPS 199 determination.

7.6 Does this information system or project necessitate the establishment of a Data Integrity Board to oversee a Computer Matching Agreements and ensure that such an agreement complies with the computer matching provisions of the Privacy Act?

The FDIC does not maintain any Computer Matching Agreements under the Privacy Act of 1974, as amended, by the Computer Matching and Privacy Protection Act of 1988. Consequently, the FDIC does not need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There is a risk that information about individuals in certain VMSIS components could be inaccurate, particularly information obtained from publicly available social media posts or third-party sources during the course of FDIC investigations of physical security incidents.

Mitigation: FDIC visitors arriving for appointments are processed through designated FDIC security checkpoints in the lobbies of FDIC buildings. The visitor provides the FDIC security officer with an approved form of government-issued photo identification (e.g., state driver's license, passport, etc.). The security officer then matches the identification with the appointment information in VMSIS before credentials are provisioned or a badge is issued, as applicable. Inaccuracies will be manually corrected in VMSIS by either the security officer or FDIC Physical Security personnel prior to the issuance of the badge. For example, if a visitor's first name on his or her photo identification does not match the first name stored in VMSIS due to a misspelling, the error will be corrected in the computer before badge issuance. In the event an error is discovered after the issuance of the badge, the error will be corrected in the VMSIS and a new badge will be provided.

A similar process is followed for visitors who are authorized to lodge at the SRC. Prior to check-in at the SRC, FDIC visitors must complete the badging process and validate their identities as described above. In accordance with FDIC Directive 1800.06, *Special Events and Hospitality Services*,[43] all SRC reservations must be made through designated FDIC Division/Office Lodging Coordinators. Additionally, all FDIC employees and their guests must sign and comply with the SRC Code of Conduct, which establishes the principles and expectations for professional conduct and ethical behavior for all employees and guests of the SRC.[44] Upon check-in at the SRC, FDIC employees and their guests provide their name, contact information, vehicle information (if applicable for parking) to the SRC Front Desk personnel. They also sign the aforementioned Code of Conduct, provide a form of identification (e.g., driver's license), and swipe their credit/debit card, if they are a paying guest. The SRC Front Desk personnel match the identification with the reservation information in VMSIS. Inaccuracies are manually corrected in VMSIS by the SRC Front Desk personnel during the check-in process.

For PII collected during investigations of physical security incidents, FDIC strives to collect the most relevant and accurate information, but there is always a risk that publicly available data or data from third-party sources could be inaccurate. FDIC mitigates this risk by restricting the collection of social media and criminal information to rare and limited circumstances and by leveraging, when applicable, police reports and victim and witness statements to corroborate the information obtained from social media and other sources during the investigation. FDIC further mitigates this risk by having several levels of review to ensure the accuracy and completeness of incident records. If any information is inaccurate or missing, an FDIC investigator contacts the witness, complainant, perpetrator, or victim to obtain the correct information.

Additionally, FDIC restricts access to VMSIS to those who have a need to perform authorized business duties. VMSIS platforms also utilize role-based permissions to limit user access to

---

[43] FDIC Directive 1800.06, *Special Events and Hospitality Services* (December 12, 2024).
[44] *Ibid.*

data, including PII, on a need-to-know basis. Further, certain VMSIS platforms have the ability to generate audit trails of user activity, including the viewing of records in the system.

Privacy Risk: There is a risk associated with the accuracy of foreign national names in VMSIS, as well as a risk that FDIC could obtain inaccurate source data about foreign nationals. Specifically, translation errors may occur when a foreign national name is adapted from its native alphabet. Name translation errors could result in misidentification of the foreign national requesting access to FDIC facilities. Additionally, information obtained by FDIC during the vetting process for foreign nationals could be inaccurate.

Mitigation: To mitigate this risk, FDIC collects information directly from the foreign nationals or their representative via an FDIC form (FDIC Foreign National Visitor Notification Form) and verifies the information for accuracy by checking it against information collected and maintained by U.S. government agencies. To minimize risks associated with translation errors, the FDIC Foreign National Visitor Notification Form requests additional information, such as date of birth and country of citizenship, to validate a foreign national's identity.

Further, FDIC trains its personnel on intelligence and information evaluation techniques and clearly identifies its sources and judgements when providing a final risk assessment for a foreign national visitor. Identities are checked against multiple databases to ensure vetting results are attributed correctly.

Section 8.0: Individual Participation

Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

8.1 Explain how the information system or project provides means, when feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection.

When information is collected directly from the individual, the FDIC Privacy Program ensures that Privacy Act statements or other privacy notices are provided, as necessary, to individuals prior to the collection of PII. This informs them of the purposes of the information collection and whether collection is voluntary or

mandated, and the consequences of not providing the information, such as denial of entry to an FDIC facility. Additionally, this PIA and the SORNs listed in Section 2.2 serve as notice of the information collection. Lastly, the FDIC Privacy Program also reviews PIAs to ensure that PII collection is conducted with the consent of the individual to the greatest extent practicable.

VMSIS generally collects information directly from FDIC visitors and their sponsors and provides notice and consent opportunities at the time of collection. In some cases, however, it is not practical or feasible to provide advance notice and/or consent opportunities to individuals, such as when an individual is a subject of a physical security investigation or identified as a potential safety or security risk to FDIC personnel or property.

With respect to the systems and software that support physical security investigations, this PIA and the SORNs referenced in Section 2.2 provide constructive notice and transparency related to the collection and maintenance of PII by VMSIS. FDIC also limits the collection of an individual's social media posts and police reports to only certain investigations where the information is necessary for a physical security purpose.

During the course of an investigation, FDIC adheres to its Security Procedural Guide and coordinates closely with the Legal Division and other relevant stakeholders, such as FDIC OIG and law enforcement, as applicable. Depending on the nature of the investigation, FDIC provides notice to individuals as part of conducting interviews and taking witness statements, and may ask individuals if they wish to consent to particular uses of the information they provide. For example, if an individual requests confidentiality they will be advised of the extent to which confidentiality can be provided under applicable laws and regulations. However, some PII collected and maintained by FDIC may be obtained in connection with investigations of incidents or potential criminal activity for which prior notification cannot be provided as it could compromise the integrity of the investigation or jeopardize public safety. FDIC refers criminal matters to FDIC OIG and law enforcement for investigation and action, as applicable.

Further, SORN FDIC-009, *Safety and Security Incident Records*,[45] provides exemptions from the Privacy Act requirements related to notification and access with respect to certain investigative information. Access to certain investigative information will be provided to an individual where a lawful requirement to provide such information

[45] FDIC SORN-009, *Safety and Security Incident Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.

exists. Additionally, investigative information collected by FDIC may be disclosed to an individual pursuant to federal rules of civil or criminal procedure or court order.

With respect to PII collected from foreign national visitors, foreign national visitors are required to complete the FDIC Foreign National Visitor Notification form, which advises them that FDIC will use this information to vet them to determine if access may be granted to a FDIC facility and that failure to furnish the requested information may delay or prevent their access. This PIA serves as an additional notice regarding why FDIC is requesting the information and how the information will be used and maintained.

8.2 Explain how the information system or project provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.

When information is collected directly from the individual, the FDIC Privacy Program ensures that Privacy Act Statements or other privacy notices are provided, as necessary, to individuals prior to the collection of PII. This informs them of the purposes of the information collection and whether collection is voluntary or mandated, and the consequences of not providing the information, such as denial of entry to an FDIC facility.

As detailed previously, it is not always practical or feasible to provide advance notice and consent opportunities to individuals, such as when an individual is the subject of a physical security investigation or identified as a potential safety or security risk to FDIC personnel or property. Refer to Question 8.1 for more information.

With respect to PII collected from foreign national visitors, foreign national visitors are required to complete the FDIC Foreign National Visitor Notification form, which advises them that FDIC will use this information to vet them to determine if access may be granted to a FDIC facility and that failure to furnish the requested information may delay or prevent their access. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII.

8.3 Explain how the information system or project obtains consent, when feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

It is not feasible or appropriate to get direct consent prior to any new use or disclosures of previously collected PII. In the event of significant changes to new uses or disclosures of previously collected PII, the FDIC Privacy Program will update the relevant SORNs as well as this PIA, thereby providing public notice of those changes.

SORN modifications are subject to a public comment period and FDIC will review and consider any comments related to new or changed uses or disclosures of PII.

8.4 Explain how the information system or project ensures that individuals are aware of and, when feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the FDIC collected the PII.

The project only uses PII for the purposes listed in Question 9.1. This PIA and the SORNs listed in Question 2.2 serve as notice for all uses of the PII. Additionally, the FDIC ensures that individuals are aware of all uses of PII not initially described in the public notice, at the time of collection, in accordance with the Privacy Act of 1974 and the FDIC Privacy Policy.

8.5 Describe the process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices?

The FDIC Privacy Program website, http://www.fdic.gov/privacy/, instructs individuals to direct privacy questions to the FDIC Privacy Program through the Privacy@fdic.gov email address. Complaints and questions are handled on a case-by-case basis.

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: There is a risk that certain individuals may not be aware that their information is collected and maintained within certain VMSIS components. In particular, visitors who are subjects of physical security investigations and/or deemed as prohibited from accessing FDIC facilities may not be aware of or have an opportunity to opt out of the collection and use of their information.

Mitigation: FDIC generally collects information directly from FDIC visitors and their sponsors and provides notice and consent opportunities at the time of collection. In some cases, however, it is not practical or feasible to provide advance notice and/or consent opportunities to individuals, such as when an individual is a subject of a physical security investigation and/or identified as a potential safety or security risk to FDIC personnel or property.

During the course of an investigation, FDIC adheres to its Security Procedural Guide and coordinates closely with the Legal Division and other relevant stakeholders, such as FDIC OIG and law enforcement, as applicable. Depending on the nature of the investigation, FDIC provides notice to individuals as part of conducting interviews and taking witness statements, and may ask individuals if they wish to consent to particular uses of the information they provide. For example, if an individual requests confidentiality they will be advised of the extent to which confidentiality can be provided under applicable laws and

regulations. However, some PII collected and maintained by FDIC may be obtained in connection with investigations of incidents or other potential criminal activity for which prior notification cannot be provided as it could compromise the integrity of the investigation or jeopardize public safety. FDIC refers criminal matters to FDIC OIG and law enforcement for investigation and action, as applicable.

FDIC-009, *Safety and Security Incident Records*,[46] provides exemptions from the Privacy Act requirements related to notification and access with respect to certain investigative information. Access to certain investigative information will be provided to an individual where a lawful requirement to provide such information exists. Additionally, investigative information collected by FDIC may be disclosed to an individual pursuant to federal rules of civil or criminal procedure or court order.

In instances where prior notice is not required or cannot be provided, this PIA and the SORNs referenced in Section 2.2 provide constructive notice and transparency related to the collection and maintenance of PII by VMSIS.

Section 9.0: Purpose and Use Limitation

Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

9.1 Describe the purpose(s) for which PII is collected, used, maintained, and shared as specified in the relevant privacy notices.

VMSIS collects, processes and maintains PII in order to accomplish authorized tasks, including providing enterprise security, facilities operations, hospitality, and other services detailed in this section. VMSIS supports a range of functions related to managing physical access by visitors to FDIC facilities, such as validating their identities and credentialing and issuing badges to them. VMSIS helps ensure the protection of FDIC employees, visitors, and facilities from internal and external threats (e.g., fire, theft, vandalism, and other security concerns) and the prevention, detection, and investigation of physical security incidents. VMSIS also supports the

[46] FDIC SORN-009, *Safety and Security Incident Records*, 84 FR 35184 (July 22, 2019), https://www.fdic.gov/about/system-records-notices.

administration and management of facilities operations and the hospitality services, including without limitation lodging, cafeteria, and parking services available to FDIC employees, contractors and their visitors.

9.2 Describe how the information system or project uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices? Who is responsible for assuring proper use of data in the information system or project and, if applicable, for determining what data can be shared with other parties and information systems? Have policies and procedures been established for this responsibility and accountability? Explain.

Through the conduct, evaluation, and review of privacy artifacts, and in conjunction with the implementation of applicable privacy controls, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Directive 1360.09 "Protecting Information." Additionally, annual Information Security and Privacy Awareness Training is mandatory for all employees and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

Access to information in VMSIS is based on an official need to know. VMSIS users include authorized FDIC managers, staff and contractors. A limited number of users in the FDIC Division of Information Technology (DIT) system may also have access to VMSIS components to provide system administration and support.

When contractors have access to PII, they are required to take mandatory annual Information Security and Privacy Awareness Training. Privacy and security-related responsibilities are specified in contracts and associated Risk Level Designation documents. Privacy-related roles, responsibilities, and access requirements are documented in relevant PIAs.

VMSIS employs role-based permissions to restrict access to VMSIS and the data contained therein to only authorized FDIC employees and contractors who have a "need-to-know" in order to fulfill their job responsibilities. Note that the FDIC investigator role is a contracted job with defined requirements and training. FDIC Physical Security personnel have oversight over the work of the investigators and make all decisions regarding case closures or other next steps.

The VMSIS system owners/program managers serve as the primary source of information for data definition and data protection requirements and are responsible for supporting FDIC's corporate-wide view of data sharing. Additionally, all FDIC users who have authorized access to information in VMSIS bear responsibility for assuring

proper use of the data and abiding by the FDIC data protection rules. These rules are outlined in any system-specific training provided for the respective VMSIS systems and platforms. Additionally, all VMSIS system administrators with access to the system must complete the FDIC's annual Information Security and Privacy Awareness Training. This training has specific information regarding the compromise of data and the prevention of misuse of data.

9.3 How is access to the data determined and by whom? Explain the criteria, procedures, security requirements, controls, and responsibilities for granting access.

All access is granted on a need-to-know basis. Guidelines established in the Corporation's Access Control Policies and Procedures are also followed. Controls are documented in the system documentation and a user's access is tracked in the Corporation's access control tracking system.

VMSIS users are granted access to specific roles set within the respective VMSIS systems and platforms. All users who have access to VMSIS must have the approval of their manager/supervisor, as applicable, and the FDIC program manager/system owner for the VMSIS platform to which they require access. Additionally, the functional security of certain VMSIS platforms limits a user's access to specific functions and regulates a user's ability to update data for a specific function based on job responsibilities and limited to information needed to perform position duties.

9.4 Do other internal information systems receive data or have access to the data in the information system? If yes, explain.

☐ No
☒ Yes Explain:

VMSIS integrates with other FDIC systems for user authentication, to grant permissions to locations throughout FDIC facilities, and to validate and provision certificates of FDIC employees/contractors and visitor credentials.

Within VMSIS, the property management system interfaces with the hospitality software, transmitting information about group details and associated rooms.

Point-of-Sale terminals and cash registers in the FDIC's SRC and cafeteria allow the clerk at the register to ring up customer/visitor purchases, process the payment via the connected Point-of-Sale credit/debit card terminal, and keep records of all financial transactions. The full debit and credit card information is stored with the Point-of-Sale vendor, not in VMSIS.

9.5 Will the information system or project aggregate or consolidate data in order to make determinations or derive new data about individuals? If so, what controls are in place to protect the newly derived data from unauthorized access or use?

No, the project does not aggregate data to make programmatic level decisions.

9.6 Does the information system or project share PII externally? If so, is the sharing pursuant to a Memorandum of Understanding, Memorandum of Agreement, or similar agreement that specifically describes the PII covered and enumerates the purposes for which the PII may be used? Please explain.

Within VMSIS, ePACS receives data from the GSA USAccess Program,[47] with which the FDIC collaborates to facilitate the issuance of PIV cards to FDIC employee and contractor personnel nationwide. The services provided by USAccess include enrollment services, systems infrastructure, PKI certificates and maintenance of identity accounts, card production, and finalization. ePACS provides the capability to integrate with the central Federal database/repository that maintains PKI certificates[48] for Federal government agency employees and contractors. GSA manages the PKI Shared Service Providers Program, which includes PKI-compliant service offerings to support Federally issued PIV and PIV-I, as well as associated certificates and cryptographic key service programs.[49] The FDIC has executed a Memorandum of Agreement with GSA for USAccess services.

FDIC has executed a contract with the HSC vendor to operate and manage the FDIC SRC and cafeterias. This contract includes privacy and security provisions to ensure the appropriate handling and protection of information, including any external sharing of information, such as the transmission of credit/debit card information when FDIC visitors swipe their cards at Point-of-Sale terminals.

FDIC coordinates with and refers criminal matters to FDIC OIG and other law enforcement agencies for investigation and action, as applicable. Any external sharing, such as with local law enforcement, requires the approval of the FDIC Legal Division and other appropriate FDIC management officials as defined in FDIC policies and procedures.

---

[47] GSA Privacy Impact Assessment (PIA) for USAccess Program (January 1, 2023), https://www.gsa.gov/system/files/GSA-USAccess-%28PIA-391%29.pdf.

[48] Government-Wide System of Records Notice (SORN) GSA/GOVT 7, *HSPD-12 USAccess*, 80 FR 64416 (October 23, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-10-23/pdf/2015-26940.pdf.

[49] For more information about the GSA PKI Shared Service Providers Program, see https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/multiple-award-schedule-it/pki-shared-service-providers-program.

FDIC may share information externally when conducting records checks on foreign national visitors. For example, FDIC may send to or receive information from the Federal Bureau of Investigation, Central Intelligence Agency, National Security Agency, or other U.S. government agencies that collect and retain threat-related information on foreign nationals to identify threats. The U.S. government agency to which the information is sent uses the information to search its records for information about the subject. Each agency maintains its records in accordance with its respective policies. Some record checks are conducted for the FDIC by U.S. government agencies that maintain national security systems consistent with the requirements of Executive Order 12333, as amended, "United States Intelligence Activities;" however, the FDIC does not engage in intelligence activities as defined by that Executive Order.

Additionally, through the conduct, evaluation, and review of PIAs and SORNs, the FDIC ensures that PII shared with third parties is used only for the authorized purposes identified or for a purpose compatible with those purposes, in accordance with the Privacy Act of 1974, FDIC Directive 1360.20 "Privacy Program," and FDIC Directive 1360.17 "Information Technology Security Guidance for FDIC Procurements/Third Party Products." The FDIC also ensures that agreements regarding the sharing of PII with third parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Directive 1360.17 and FDIC Directive 1360.09.

9.7 Describe how the information system or project monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

Annual Information Security and Privacy Awareness Training is mandatory for all employees and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties. Additionally, VMSIS restricts access to data to users with a "need-to-know" who require the information to perform their job responsibilities. Any disclosures outside of VMSIS are initiated by authorized FDIC personnel who have a responsibility to share the information for purposes that are compatible with the purpose for which the PII was originally collected and/or that are otherwise legally authorized or required by statute, federal court rules, or responsive document requests. Any information disclosures or withholdings are made based on the nature of the records and, as applicable, pursuant to the routine uses and exemptions in the SORNs that cover those records.

9.8 Explain how the information system or project evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

The FDIC reviews privacy artifacts to evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: There is a risk that information in VMSIS could be used or disclosed for a purpose not compatible with the original purposes for which the information was collected.

Mitigation: Through the conduct, evaluation, and review of privacy artifacts, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Directive 1360.09, *Protecting Information*.[50] VMSIS restricts access to data to users with a "need-to-know" who require the information to perform their job responsibilities. Any disclosures outside of VMSIS are initiated by authorized FDIC personnel who have a responsibility to share the information for purposes that are compatible with the purpose for which the PII was originally collected and/or that are otherwise legally authorized or required by statute, federal court rules, or responsive document requests. Any information disclosures or withholdings are made based on the nature of the records and, as applicable, pursuant to the routine uses and exemptions in the SORNs that cover those records.

Privacy Risk: There is a risk that PII maintained in VMSIS could be accessed or used inappropriately or for unauthorized purposes.

Mitigation: To help prevent unauthorized access and use of information, VMSIS employs role-based permissions to restrict access to VMSIS and the data contained therein to only authorized FDIC employees and contractors who have a "need-to-know" in order to fulfill their job responsibilities. VMSIS administrators grant access to users, and each individual user must be properly credentialed. In addition, all FDIC users are subject and must adhere to agency policies and procedures for using, sharing and safeguarding PII. All users receive annual Information Security and Privacy Awareness training, as well as specialized training, as applicable, which helps ensure PII is handled and safeguarded appropriately. Certain VMSIS systems and platforms generate and maintain detailed audit logs that are capable of capturing a user's unauthorized use of information contained within the respective platform.

---

[50] FDIC Directive 1360.09, *Protecting Information* (March 2, 2024), available at: https://www.fdic.gov/formsdocuments/d1360-09.pdf

Section 10.0: Security

Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

10.1 Describe the process that establishes, maintains, and updates an inventory that contains a listing of all information systems or projects identified as collecting, using, maintaining, or sharing PII.

The FDIC Privacy Program maintains an inventory of all programs and information systems identified as collecting, using, maintaining, or sharing PII.

10.2 Describe the process that provides each update of the PII inventory to the CIO or information security official to support the establishment of information security requirements for all new or modified information systems or projects containing PII?

The FDIC Privacy Program updates the CISO on PII holdings via the PTA adjudication process. As part of the PTA adjudication process, the FDIC Privacy Program reviews the system or project's FIPS 199 determination. The FDIC Privacy Program will recommend the appropriate determination to the CISO should the potential loss of confidentiality be expected to cause a serious adverse effect on individuals.

10.3 Has a Privacy Incident Response Plan been developed and implemented?

FDIC has developed and implemented a Breach Response Plan in accordance with OMB M-17-12.

10.4 How does the agency provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan?

Responses to privacy breaches are addressed in an organized and effective manner in accordance with the FDIC's Breach Response Plan. Oversight of FDIC's breach response activities occurs through quarterly reporting to both the FDIC's Senior Agency Official for Privacy and the FDIC Information Technology Risk Advisory Council (ITRAC). ITRAC seeks to properly align the management of IT risks with the FDIC's Enterprise Risk Management Program. Additionally, FDIC holds a breach response tabletop exercise every year to test the effectiveness of the Plan and identify improvements or changes needed to the Plan.

Privacy Risk Analysis: Related to Security

Privacy Risk: There are no identifiable privacy risks related to Security for VMSIS.

Mitigation: No mitigation actions are recommended.