FDIC FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Video Surveillance System Monitoring Program (VSSMP)

July 20, 2022

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 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

Describe what this information system[2] does in terms of purpose, functionality, and PII collection/use. What is the goal of the system? What gap does it serve to close?

The Federal Deposit Insurance Corporation (FDIC), Division of Administration (DOA), Security Enterprise Programs Section (SEPS) is responsible for personnel security, physical security, emergency operations, transportation, business continuity, insider threat, counterintelligence and safety of all Corporation personnel, visitors, and sensitive Corporation information. As part of these responsibilities, DOA SEPS deployed a Video Surveillance System Monitoring Program (VSSMP) throughout the Corporation. The VSSMP replaces the legacy closed circuit television (CCTV) monitoring program that consisted of analog technology and infrastructure, limited recorded video storage and retrieval capabilities, and less superior video quality. VSSMP is used to obtain real-time and recorded visual information in and around FDIC worksites and facilities to aid in crime prevention and forensic analysis, increase situational awareness, enhance personnel safety, and secure critical assets. FDIC conducted this Privacy Impact Assessment (PIA) because VSSMP has the ability to capture images of people, license plates, and any other visual information within range of the cameras.

VSSMP is part of SEPS Physical Security Operations and consists of the following components:

[1] www.fdic.gov/privacy

[2] OMB Circular No. A-130, "Managing Information as a Strategic Resource," (July 27, 2016). The Circular defines an information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

- An automated system recording and monitoring real-time activities of various types (fixed, pan tilt zoom, panoramic, etc.) of networked digital cameras located throughout headquarters, Regional and Field offices (owned or leased) and is used to provide increased situational awareness, detect or deter criminal activity and perform investigations. Records activities at a rate of 10-30 frames per second (depending on location). Footage is retained for a minimum of 60 days and a maximum of 120 days for after-action review.

- An enterprise application that provides centralized management for multi-location video surveillance deployments. It helps to streamline IT operations through unified system monitoring and settings management, while allowing automated updates for network cameras and other vendor products.

VSSMP is a closed system with no information provided by external sources.

Some VSSMP cameras use zoom capability with manual tracking (i.e., panning and tilting), which allows the user conducting the monitoring to gain the best image of any activity. Other cameras are set to automatically tour an area. The cameras are placed in various locations on the perimeters or inside of FDIC facilities, such as parking lots, entrances, and secured areas, to provide the greatest possible range and area of monitoring. Cameras contain low-light technology to support detection of unauthorized or suspicious activities at night. The cameras are not placed in areas where there is a reasonable expectation of privacy like bathrooms or changing rooms.

FDIC uses the video feeds to detect and respond to potentially unlawful activities in real time in the areas using VSSMP. The video feeds may also be used to support law enforcement investigations to the extent that they contain information relevant to a criminal (or potential criminal) activity. For example, if a suspicious package is placed outside a FDIC building that uses the system, the cameras will provide an image of this activity and allow FDIC or local law enforcement to take appropriate responsive action.

FDIC may use an image, such as a license plate number, captured by the video feed to identify an individual or link an individual to a specific event or investigation. In general, FDIC will use VSSMP feeds to further investigations, link data elements, and identify individuals.

Privacy protections for VSSMP include limiting access to the video feed to only authorized users and law enforcement partners (if approved), establishing clear auditing systems so every use of the system is logged and reviewable and restricting storage to six months or less. Also, VSSMP users are subject to employee discipline if any misuse occurs.

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:

- Transparency;
- Access and Amendment;
- Data Minimization;
- Individual Participation; and
- Purpose and Use Limitation.

Transparency

Privacy Risk: Members of the public may not see the notice sign or may not be aware of why VSSMP cameras are necessary.

Mitigation: This PIA makes clear that FDIC properties are under surveillance by VSSMP cameras and why the cameras are necessary. Additionally, it has been a requirement since the 1995 Presidential Policy Memorandum for Executive Departments and Agencies titled *Upgrading Security at Federal Facilities* for federal facilities (where feasible) to install VSS cameras. Federal buildings must be protected and VSS is cost efficient. The use of VSS is a common practice throughout the United States in the private, commercial, and federal arenas and is a standard security practice.

Access and Amendment

Privacy Risk: The period of time for redress for an individual is very short. In most cases, video is not retained longer than 120 days.

Mitigation: Given the nature of VSSMP systems in general, a robust program to permit access, review, and correction of the video cannot be provided. This lack of direct access and formal redress mechanism represents a risk to individual privacy, however it is necessary given the utility of VSSMP. While some individuals will not have a formal mechanism for access or redress, FDIC has internal mechanisms to correct inaccuracies and protect against abuse through the auditing of the system.

Data Minimization

Privacy Risk: Video that is not relevant and necessary to accomplishing the mission will be collected.

Mitigation: This risk is mitigated by the placement of cameras in public places as opposed to bathrooms or other areas where individuals have a reasonable expectation of privacy. The purpose of the VSSMP cameras are to protect the buildings, grounds, and property owned, occupied or secured by the FDIC, and the persons on the property. VSSMP cameras are only used to render property safe and secure for FDIC employees and deter against future crime or attack.

Individual Participation

Privacy Risk: Individuals who enter or are near FDIC facilities do not have the ability to consent or opt-out of being recorded.

Mitigation: Individuals who enter into or are near FDIC facilities are not given the opportunity to opt-out of being video recorded by VSSMP. These individuals have no expectation of privacy and therefore no consent is required with respect to the collection, use, and disclosure of PII. However, as a matter of policy, signs are posted to provide notice of surveillance activities via VSSMP cameras.

Purpose and Use Limitation

Privacy Risk: There is a risk that VSSMP cameras could be used for improper surveillance or record more than is necessary.

Mitigation: The purpose behind FDIC use of the VSSMP system is to detect and deter criminal activity, increase situational awareness, and to provide investigatory leads. The VSSMP system is password-protected and access is restricted to only those who monitor the video feeds. The system tracks users and will be periodically reviewed for misuse and discriminatory practices. VSSMP users are subject to employee discipline if any misuse occurs.

Section 1.0: Information System

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

FDIC places the VSSMP cameras around the perimeter and inside of FDIC facilities and buildings, including parking lots, entrance and exits, and secured areas. The VSSMP cameras may capture facial images of employees and visitors to FDIC buildings and images of license plates that are parked or driving through the parking lot.

Additionally, VSSMP collects metadata. Metadata describes other data. It provides information about a certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document. Regarding VSSMP, some examples are camera name, location, time, and date. The data is used to manage the VSSMP feeds and footage files.

FDIC uses the video feeds captured through VSSMP to aid in crime prevention and forensic analysis, increase situational awareness, enhance personnel safety, and secure critical assets. VSSMP recordings may provide investigators with leads when investigating crimes occurring at protected federal facilities. For example, VSSMP records may assist investigators in identifying persons who were in the area when a crime occurred, or identify suspects or vehicles fleeing the area. These videos may also become evidence in a subsequent criminal prosecution.

Cameras are not placed in places with a reasonable expectation of privacy such as inside a bathroom or changing room.

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☐	☒
Place of Birth	☐	☒
Social Security Number	☐	☒
Employment Status, History or Information	☐	☒
Mother's Maiden Name	☐	☒
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☐	☒
Home Address	☐	☒
Phone Number(s) (non-work)	☐	☒
Email Address (non-work)	☐	☒
Employee Identification Number (EIN)	☐	☒
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☐	☒
Driver's License/State Identification Number	☐	☒
Vehicle Identifiers (e.g., license plates)	☒	☐
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☐	☒
Education Records	☐	☒

Criminal Information	❒	☒
Military Status and/or Records	❒	☒
Investigation Report or Database	❒	☒
Biometric Identifiers (e.g., fingerprint, voiceprint)	❒	☒
Photographic Identifiers (e.g., image, x-ray, video)	☒	❒
Other (Specify: Login Credentials)	☒	❒

1.2 Who/what are the sources of the PII in the information system or project?

VSSMP records video from a variety of ranges and with differing zooming capabilities. The cameras may record passersby on public streets and FDIC employees accessing a secured area. VSSMP cameras collect video images through real-time monitoring with streaming and storage onto a storage device.

Zooming capability allows for the recording of textual information such as license plate numbers or text written on a person's belongings. Cameras contain low-light technology to support detection of unauthorized or suspicious activities at night. Most cameras are fixed but others use pan/tilt/zoom capability with manual tracking, which allows the individual monitoring the VSSMP feed to adjust the camera in real time to gain the best image of any suspicious or illegal activity of interest that is occurring. Tracking, which can be manual or occur when the cameras automatically track people or other moving objects in the field of view, is used so security personnel may follow the activity of a single individual within viewing areas that contain a large number of people.

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

The ATO was issued on June 30, 2022 and will be 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 Record Notice (SORN) does this information system or project operate? Provide number and name.

The following SORN(s) apply to the system or project: FDIC 30-64-0009, Safety and Security Incident Records System of Records, which covers s current and past FDIC employees, contractors, volunteers, visitors, and others involved in the investigation of accidents, injury, criminal conduct, and related civil matters involving the FDIC. Generally, VSSMP does not record or retrieve information by personal identifier. It retrieves video by time and date.

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

No, the system is not being modified at this time. Generally, the FDIC conducts reviews of its SORNs every three years or as needed.

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

FDIC facilities with VSSMP provide notice of the surveillance camera. Signs are posted in public areas, in written format or in pictograms. An example of the type of wording provided in such notice signs is: “This Area Under Video Surveillance.”

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 contains policies and information related to SORNs, PIAs, FDIC’s Privacy Policy, and contact information for the SAOP, the Privacy Program Manager, the Privacy Act System of Records (SOR) Clearance Officer, and the Privacy Program (Privacy@fdic.gov). See https://www.fdic.gov/policies/privacy/index.html.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: Members of the public may not see the notice sign or may not be aware of why VSSMP cameras are necessary.

Mitigation: This PIA makes clear that FDIC properties are under surveillance by VSSMP cameras and why the cameras are necessary. Additionally, it has been a requirement since the 1995 Presidential Policy Memorandum for Executive Departments and Agencies titled Upgrading Security at Federal Facilities for federal facilities (where feasible) to install VSS cameras. Federal buildings must be protected and VSS is a cost efficient and useful tool to prevent crime and terrorism. The use of CCTV is a common practice throughout the United States in the private, commercial, and federal arenas and is a standard security practice.

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?

Generally, VSSMP does not record or retrieve information by personal identifiers so it will be difficult for an individual to find and view a particular video. Additionally, videos are only stored for a maximum of 120 days and in some cases, a much shorter period of 60 days, depending on the age and condition of the equipment. The video is then recorded over, which limits the amount of time an individual has to access the video. Accordingly, an individual wishing to access their information should provide a detailed description, such as the address or physical location of the VSSMP system, the date and approximate time the video or image was taken, or other identifying information that will assist FDIC in locating the requested record.

Additionally, the FDIC provides individuals the ability to have access to their PII maintained in its systems of records as specified by the Privacy Act of 1974 and FDIC Circular 1031.1. Access procedures for this information system or projected are detailed in the SORN(s) listed in Question 2.2 of this PIA. The FDIC publishes its System of Records Notices (SORNs) on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

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

Video image cannot be corrected given it captures the events in real time. As such, the PII maintained by the system or project is contained in a Privacy Act System of Record that has been exempted from the redress requirement. However, an individual may complete a FOIA request to view the image. For more information on FOIA requests, please contact the FDIC FOIA & Privacy Act Group, 550 17th Street, NW, Washington, DC 20429, or email efoia@fdic.gov.

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

VSSMP does not notify individuals about the procedures for correcting their information. The PII maintained by the system is contained in a Privacy Act System of Record that has been exempted from the redress requirement.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: The period of time for redress for an individual is very short. In most cases, video is not retained longer than 120 days.

Mitigation: Given the nature of VSSMP systems in general, a robust program to permit access, review, and correction of the video cannot be provided. This lack of direct access and formal redress mechanism represent a risk to individual privacy, however it is necessary given the utility of VSSMP. While some individuals will not have a formal mechanism for access or redress, FDIC has internal mechanisms to correct inaccuracies and protect against abuse through the auditing of the system.

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 also has been 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).

The FDIC's Privacy Program Staff supports the SAOP in carrying out those responsibilities through the management and execution of the FDIC's Privacy Program. The Privacy Program has been fully integrated throughout the agency and is supported on a part-time basis by divisional Information Security Managers located within the agency's divisions and offices.

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. The Privacy Program's goal is to have PTAs in place for all IT systems or collections with PII.

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?

Privacy risks posed by the information system or project are captured in PIAs, when conducted in accordance with applicable law, OMB policy, and FDIC policy. 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 a contractor have with the design and maintenance of the information system or project?

Contractors have been the main source for system design and construction tasks. Contractors will support the maintenance of the system, but will not have access to the production environment.

Contractors are required to 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, a confidentiality agreement has been completed and signed for contractors who work on the information system or project. 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 is currently in the process of implementing 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.

The FDIC Privacy Program maintains an ongoing Privacy Training Plan that documents the development, implementation, and update of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. Annual Security and Privacy 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 staff as well.

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 following: Annual Senior Agency Official for Privacy Report (SAOP) as required by FISMA; and regular reporting to the SAOP, the CISO, and the Information Security Manager's 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 if 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 record under its control, as mandated by the Privacy Act of 1974 and 12 C.F.R. § 310. Disclosures are tracked and managed using the FDIC's FOIA solution.

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 C.F.R. § 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 C.F.R. § 310.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable privacy risks related to accountability for VSSMP.

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 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 Circular 1360.20, "FDIC Privacy Program," mandates that the collection of PII be in accordance with Federal laws and guidance. This particular 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; and

- Interagency Security Committee (ISC) Risk Management Process, 41 CFR Part 102-81, requires CCTV monitors for the majority of federal buildings from low security requirements to very high.

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable privacy risks related to authority for VSSMP.

Mitigation: No mitigation actions are recommended.

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 personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection?

VSSMP only collects the minimum PII elements needed to accomplish authorized tasks. VSSMP only collects PII that is directly relevant and necessary to accomplish specified purpose(s). Cameras are not placed in places with a reasonable expectation of privacy such as inside a bathroom or changing room.

Additionally, through the conduct, evaluation and review of privacy artifacts,[3] 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?

VSSMP only collects the minimum PII elements needed to accomplish authorized tasks. VSSMP only collects PII that is directly relevant and necessary to accomplish specified purpose(s). Cameras are not placed in places with a reasonable expectation of privacy such as inside a bathroom or changing room.

Additionally, through the conduct, evaluation and review of privacy artifacts,[4] the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

6.3 How often does the information system or project evaluate the PII holding 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?

FDIC maintains an inventory of systems that contain PII. On a semi-annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

---

[3] Privacy artifacts include Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Record Notices (SORNs).

[4] Privacy artifacts include Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Record Notices (SORNs).

6.4 What are the retention periods of 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.

In accordance with FDIC Records Retention Schedule EIS1064, the video recordings are maintained for approximately 60 to 120 days then recorded over. Retention periods are a direct result of limited storage space, recording rate and FDIC security requirements. The Assistant Director, Security Enterprise Programs Section has decided that, based on industry standards, a 120 day retention period is adequate for the overall security of FDIC facilities.

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

Use of sensitive data outside the production environment requires the management approval via a waiver. 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: Video that is not relevant and necessary to accomplishing the mission will be collected and not recorded over.

Mitigation: This risk is mitigated by the placement of cameras in public places as opposed to bathrooms or other areas where individuals have a reasonable expectation of privacy. The purpose of the VSSMP cameras are to protect the buildings, grounds, and property owned, occupied or secured by the FDIC, and the persons on the property. VSSMP cameras are only used to render property safe and secure for FDIC employees and deter against future crime or attack.

Privacy Risk: There is a privacy risk that storing video for 120 days is too long.

Mitigation: The retention period is appropriately limited to only retain images for a short length of time, while still allowing FDIC to identify potentially relevant video when an incident has occurred but is not immediately reported.

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.

VSSMP cameras collect real-time video of the activities occurring within their viewing space in or near FDIC buildings. The videos are altered through a compression algorithm in order to be stored in an array of hard drives but otherwise are not modified or changed to alter the recorded activities. VSSMP cameras only record what is occurring in real time; there is no editing feature or ability to change the image. Users can zoom or pan the cameras to follow one individual but it is unlikely that incorrect information about a person is produced from the VSSMP cameras. Only authorized personnel have access to the stored video data, and VSSMP is password protected.

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

DOA SEPS collects real-time video of individuals for use in VSSMP. VSSMP records video from a variety of ranges and with differing zooming capabilities. The cameras may record passersby on public streets and FDIC employees/contractors accessing secured areas. VSSMP cameras collect video images through real-time monitoring with streaming and storage onto a storage device.

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 measures to check for and correct any inaccurate or outdated PII in its holdings.

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 subject to Privacy Act protections are found in Part 310 of the FDIC Rules and Regulations.

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

Through its PTA adjudication process, the FDIC Privacy Program utilizes 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, and consequently does not have a need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There are no identifiable privacy risks related to Data Quality and Integrity for VSSMP.

Mitigation: No mitigation actions are recommended.

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, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection.

Individuals who enter into or are near FDIC facilities do not have a reasonable expectation of privacy and therefore no consent is required. However, as a matter of policy, signs are posted to provide notice of surveillance activities via VSSMP cameras.

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.

Individuals who enter into or are near FDIC facilities are not given the opportunity to opt-out of being video recorded by VSSMP. These individuals have no expectation of privacy and therefore no consent is required with respect to the collection, use, and disclosure of PII.

8.3 Explain how the information system or project obtains consent, where 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. If applicable, the FDIC Privacy Program will update the relevant Privacy Act SORN(s) as well as the relevant PIA.

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

The project or system only uses PII for the purposes listed in Section 9.1. This PIA and the SORN(s) listed in 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, https://www.fdic.gov/policies/privacy/index.html, 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: Individuals who enter or are near FDIC facilities do not have the ability to consent or opt-out of being recorded.

Mitigation: Individuals who enter into or are near FDIC facilities are not given the opportunity to opt-out of being video recorded by VSSMP. These individuals have no expectation of privacy and therefore no consent is required with respect to the collection, use, and disclosure of PII.

However, as a matter of policy, signs are posted to provide notice of surveillance activities via VSSMP cameras.

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.

Information on the video is used by FDIC and federal, state and local law enforcement to detect and respond to potentially unlawful activities in real time in the areas surrounding FDIC facilities. The information may also be used to support law enforcement investigations and prosecutions to the extent it contains information relevant to a criminal or potentially criminal activity. For example, if a suspicious package is placed outside a FDIC building that uses VSSMP, the system would provide a real-time notification of this activity and allow FDIC and federal, state and local law enforcement to take appropriate responsive action. Additionally, if the package is determined to be an explosive device, the recordings could be used to further investigate this criminal activity, assist in identifying the perpetrators, and/or provide evidence that may be used in court.

9.2 Describe how the information system or project uses personally identifiable information (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, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Circular 1360.9 "Protecting Sensitive Information" with the use of various privacy controls. Additionally, annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

The VSSMP systems are password-protected and access is restricted to only those who monitor the video feeds. The system tracks the users and will be periodically reviewed for misuse and discriminatory practices.

Contractors are required to 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.

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

Only authorized users are allowed to view the video feeds of VSSMP. The log-in and use of the system is traceable to a particular user and periodically audited for misuse and discriminatory practices. The DVRs themselves are also physically protected against unauthorized access.

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.

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, FDIC does not aggregate data to make programmatic level decisions.

9.6 Does the information system or project share personally identifiable information (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.

The Corporation shares PII only for authorized purposes identified or for a purpose compatible with those purposes, in accordance with the Privacy Act of 1974, FDIC Circular 1031.1 "Administration of the Privacy Act," and FDIC Circular 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 Circular 1360.17 and FDIC Circular 1360.9.

FDIC shares information contained in VSSMP with local, state, and federal law enforcement agencies. Additionally, individuals who were victims of a crime, criminal defendants, or members of the public may request copies of the video via FOIA request.

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 staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

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: VSSMP cameras may be used for improper surveillance or record more than is necessary.

Mitigation: The purpose behind FDIC use of the VSSMP system is to detect and deter criminal activity, increase situational awareness, and to provide investigatory leads. The VSSMP system is password-protected and access is restricted to only those who monitor the video feeds. The system tracks users and will be periodically reviewed for misuse and discriminatory practices. VSSMP users are subject to employee discipline if any misuse occurs.

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 personally identifiable information (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.

Privacy Risk Analysis: Related to Security

Privacy Risk: There are no identifiable privacy risks related to security for VSSMP.

Mitigation: No mitigation actions are recommended.