FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Office of Inspector General Information Management Systems (OIMS)

OCISO

December 3, 2024

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

The FDIC Office of Inspector General (OIG) is an independent office that conducts audits, evaluations, investigations, and other reviews of FDIC programs and operations to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations, and to promote economy, efficiency and effectiveness at the agency. The OIG has two primary functional areas:

- Conducting investigations
- Conducting audits, evaluations and other reviews

This PIA is being updated to address the OIG's implementation and use of FDIC's Data Lake (Data Lake) to support the OIG's audit, evaluations and cyber activities, as well as OIG's investigative activities.

Investigations

The Office of Investigations (OI) carries out a nationwide program to prevent, detect, and investigate criminal, civil, or administrative wrongdoing and misconduct by FDIC employees and contractors. OI also assists in responding to OIG Hotline allegations of suspected fraud, waste, abuse, and mismanagement. OIG investigations typically involve bank fraud, wire fraud, procurement fraud, securities fraud, fraudulent representations of the FDIC insurance, money laundering, obstruction of bank examinations, criminal concealment of assets, theft of government property, and employee misconduct.

OIG investigative efforts are concentrated on those cases of most significance or potential impact to the FDIC and its programs. The goal, in part, is to a halt the fraudulent conduct

[1] www.fdic.gov/privacy

under investigation, protect the FDIC and other victims from further harm, and assist the FDIC in recovery of its losses. Pursuing appropriate criminal penalties not only serves to punish the offender but can also deter others from participating in similar crimes.

OI maintains close and continuous working relationships with the U.S. Department of Justice; the Federal Bureau of Investigation; other Offices of Inspector General; and federal, state, and local law enforcement agencies. OI participates in numerous working groups throughout the country to keep current with emerging issues and trends affecting the FDIC and the banking system.

Audits, Evaluations, and Other Reviews

The OIG's Office of Audits, Evaluations, and Cyber (AEC) conducts audits, evaluations, and reviews to examine FDIC programs and operations, assess their efficiency and effectiveness, and make recommendations to improve the agency. AEC engagements may involve:

- assessing the effectiveness and efficiency of FDIC programs and operations;
- assessing the FDIC's compliance with laws, regulations, and best practices;
- assessing the FDIC's IT programs and information/cyber security;
- reviewing failed banks; and
- alerting management to concerns.

Technologies Supporting the OIG

The OIG employs various technologies in carrying out its mission for conducting investigations, audits, evaluations, and other reviews. Those technologies are collectively identified in this document as the OIG Information Management Systems (OIMS), and include the following components:

- An investigative tracking and support (ITS) application maintained for the purpose of documenting, tracking, reviewing and reporting on all phases of OI investigative and litigation activities that serves as a repository and source for information necessary to fulfill statutory reporting, access and disclosure requirements, including those pertaining to the Inspector General Act.
- A Body Camera System (BCS) used by OIG criminal investigators to gather and preserve evidence during specified investigative activities. OIG criminal investigators may wear body cameras during the execution of search and arrest warrants, including during interviews with individuals that take place during investigative operations. Body cameras capture audio and video recordings that may be used as evidence in OIG investigations and for OIG investigative training purposes. OIG criminal investigators are Federal Law Enforcement Officers.
- A Hotline application (Hotline) used to document and track information received via the OIG Hotline website, telephone, mail, or email, which are operated by the OIG to provide a convenient way for FDIC employees, its contractors, and members of the

public to report allegations of fraud, waste, abuse, and mismanagement within FDIC programs, activities, contractor operations, or FDIC-regulated and FDIC-insured financial institutions (FI). The information collected by the Hotline could potentially be used for audit, administrative, and investigative purposes.

- An Electronic Crimes Unit Forensics Lab (ECUFL) system that supports the OIG in carrying out its investigative mission. The ECUFL system is a logically separate environment that is maintained and used by OI personnel to carry out digital forensics and related activities.
- An audit tracking and support (ATS) application maintained for the purpose of documenting, tracking, reviewing and reporting on all phases of OIG audits, evaluations, and other reviews, thereby supporting the OIG's responsibilities under the Inspector General Act of 1978, as amended (IG Act). The ATS application documents the audit process, including planning, preparation, review, and storage, in an electronic format.
- A Data Lake to supporting the OIG's Audit, Evaluations and Cyber activities, as well as OIG investigative activities. This data will be used to perform analytics and to garner additional insight related to OIG Audit, Evaluation, Cyber, and Investigative casework. The OIG uses the FDIC's Data Lake to support its mission with appropriate protections and controls to restrict data access to OIG personnel.
- A public website (OIGWIS) maintained by the OIG that provides general information about the OIG, whistleblower protections, and the OIG's Hotline, as well as access to public non-sensitive information that includes: press releases, OIG reports, Inspector General testimonies, and OIG contact information.

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 and Individual Participation Risk:

Privacy Risk: There is a risk that individuals may not be aware that their information is collected and maintained within the various OIMS components, nor be provided with an opportunity to authorize or opt out of any new uses of data pertaining to them.

Mitigation: With respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, the Hotline application, and investigative data maintained within the Data Lake), this PIA and the SORNs referenced in section 2.2 provide transparency related to the collection and maintenance of PII by those OIMS components. Additionally, the

Hotline application provides a Privacy Act Statement to individuals prior to their input and submission of any information.

Depending on the nature of the investigation, OIG criminal investigators 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.

Generally, most investigative PII that is collected and maintained is obtained during the course of a criminal investigation. Providing notice to individuals at the point of collection may not be feasible. Notice provided to individuals could interfere with OIG's ability to obtain, serve, and issue subpoenas, warrants and other law enforcement mechanisms, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice to subjects of investigations would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

With respect to BCS, cameras worn by OIG criminal investigators will be positioned in obvious places on the criminal investigators without compromising the criminal investigator's safety so that the public can visually determine if a criminal investigator is using a camera, as follows:

- If a tactical ballistic vest (body armor) is worn, the camera will be worn on the outside/front of the body armor. Body armor is worn over the criminal investigator's clothing.
- In the event a camera is deployed when body armor is not worn, the camera will be secured to the criminal investigator's outer clothing, lanyard, or belt.

Cameras also have indicator lights that indicate when they are recording.

It should be noted that SORN FDIC-010, reflects exemptions from the Privacy Act requirements related to notification and access with respect to the ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake, while information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

Additionally, access to certain investigative information, such as the particulars concerning civil or criminal proceedings, will be provided to an individual where a lawful requirement to provide such information exists. Further, investigative information collected by FDIC may be disclosed to an individual pursuant to federal rules of civil or criminal procedure or appropriate order of a court.

The ATS application, OIGWIS, and non-investigative data maintained within the Data Lake do not operate as Privacy Act systems of records. Therefore, they are not subject to the notification requirements of the Privacy Act of 1974. However, this PIA provides transparency that mitigates the risk of individuals not being aware that their information is collected and maintained by those OIMS components.

Access and Amendment Risk:

Privacy Risk: There is a risk that individuals may not have the opportunity to access their information or amend inaccurate information contained in the various OIMS components.

Mitigation: With respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, the Hotline application, and investigative data maintained within the Data Lake), SORN FDIC-010 and SORN FDIC-034 provide detailed procedures for access and amendment to the information collected and maintained by those OIMS components. However, SORN FDIC-010 reflects an exemption from Privacy Act requirements related to individual access and amendment with respect to the OIMS ITS application, the BCS, the ECUFL, and investigative related data maintained within the Data Lake, while information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

The ATS application, OIGWIS, and related information maintained within the Data Lake do not operate as Privacy Act systems of records. Therefore, they are not subject to the Privacy Act access and amendment requirements.

Data Minimization Risk:

Privacy Risk: There is a risk that the PII collected within the various OIMS components in the course of an investigation, audit, evaluation, or other review may be unnecessary or excessive, or may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: This risk is mitigated by OIMS users being appropriately trained, and by FDIC and OIG policies regarding the collection, use, and retention of information in conjunction with the OIG's responsibilities for conducting investigations, audits, evaluations, and other reviews.

For instance, OIG criminal investigators undergo rigorous training to become proficient law enforcement officers. The majority of FDIC criminal investigator training is provided by the Federal Law Enforcement Training Centers (FLETC) and the Inspector General Criminal Investigator Academy (IGCIA). Criminal investigator training for criminal investigators helps develop interviewing skills; case management; search warrants; physical evidence; undercover electronic surveillance; and ethical behavior and core values. Required periodic training ensures that criminal investigators maintain high standards, comply with Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement (Attorney General Guidelines), and maintain needed investigative skills.

Additionally, OIG criminal investigators that are assigned body cameras are required to undergo mandatory initial training, as well as annual and periodic refresher training regarding proper use of the devices, adherence to OIG's BCS policy, legal considerations, and privacy, civil rights, and civil liberties safeguards.

OIG auditors collect and maintain documentation and evidence in conjunction with the conduct of audits, evaluations, and other reviews in accordance with Government Accountability Office's (GAO) Generally Accepted Government Auditing Standards (GAGAS), evaluations in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) Quality Standards for Inspection and Evaluation, and other reviews in accordance with CIGIE's Quality Standards for Federal Offices of Inspector General.

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 sensitive 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 National Archives and Records Administration (NARA) regulations.

Purpose and Use Limitation Risk:

Privacy Risk: There is a limited, potential risk associated with purpose and use limitation for OIMS because sensitive information, including PII, stored within the various components of OIMS could potentially be used or shared for a purpose not compatible with the original purpose for which the information was collected.

Mitigation: This risk is mitigated by OIG staff being appropriately trained and limiting OIG employee access to only that for which there is a business need. This risk is further mitigated by OIG policies and procedures that address the appropriate release of information.

With respect to the BCS, the OIG's BCS policy prohibits the use of body cameras for personal use or for purposes other than those related to official law enforcement duties. The OIG's BCS policy restricts personnel from recording events that are not law enforcement encounters and governs the use of recorded data. Since unauthorized use or release of body camera recorded data may compromise ongoing criminal investigations and administrative proceedings, or violate the privacy rights of recorded individuals, any unauthorized access, use, or release of recorded data or other violation of confidentiality laws and OIG policies may result in disciplinary action.

Privacy Risk: With respect to the BCS, there is a risk that individuals may not receive adequate notice that their images and voice communications may be recorded when they are in close proximity to a law enforcement encounter, regardless of whether they are directly or indirectly involved.

Mitigation: Cameras worn by OIG criminal investigators will be positioned in obvious places on the criminal investigators, without compromising the criminal investigator's safety, so that the public can visually determine if a criminal investigator is using a camera, as follows:

- If body armor is worn, the camera will be worn on the outside/front of the body armor. Body armor is worn over the criminal investigator's clothing.

- In the event a camera is deployed when body armor is not worn, the camera will be secured to the criminal investigator's outer clothing, lanyard, or belt.

Cameras also have indicator lights that indicate when they are recording. Additionally, the FDIC also provides general notice to the public through this Privacy Impact Assessment.

It should be noted, however, that SORN FDIC-010 reflects an exemption from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the BCS.

Privacy Risk: There is a potential risk associated with purpose and use limitation that OIG data maintained in the FDIC Data Lake could be accessed by OIG and FDIC employees or contractors who are not properly authorized to access the OIG's information in the Data Lake.

Mitigation: This risk is mitigated through the controls the OIG has established to ensure that access to the OIG's data within the Data Lake is restricted to OIG staff having an official need-to-know. FDIC's Access Request and Certification System (ARCS) is used to facilitate the tracking and management of OIG employees that are authorized users of the OIG's data in the Data Lake. ARCS requests must be submitted by OIG users and approved by their managers in order to gain access to the OIG's data in the Data Lake. User access is further controlled and restricted according to specific user and administrative roles that have been defined and established by the OIG for the OIG's data within the Data Lake, and access to the OIG's data in the Data Lake is logged and monitored by OIG staff.

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?

OIMS may collect and maintain various types of PII as indicated in the table below. For a member of the public's PII to be included within OIMS, that individual must be associated with an OIG investigation, audit, evaluation, or other review. In addition, OIMS may include the PII of FDIC employees, including that of OIG employees.

PII Element	- Investigative Tracking and Support Application -Body Camera System - Hotline Application - Electronic Crimes Unit Forensics Lab - Copying and Transcription Services -Data Lake	Audit Tracking and Support Application	OIG Public Website (OIGWIS)
Full Name	☒	☒	☒
Date of Birth (DOB)	☒	☒	☐
Place of Birth	☒	☐	☐
Social Security number (SSN)	☒	☒	☐
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)	☒	☒	☐
Email Address	☒	☒	☐
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)	☒	☐	☐
Audio and Video recordings and Photographic Identifiers (e.g., image, x-ray)	☒	☐	☐
Other (Other potential investigative sources such as social media)	☒	☐	☐

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

Data Source	Description of Information Provided by Source
Members of the General Public	Members of the public may provide information via the Hotline application, or otherwise, regarding wrongdoing by individuals or banking institutions. The extent of the information provided greatly varies, but usually includes, at a minimum, names and addresses.
FDIC Employees	FDIC employees, including FDIC OIG employees, may provide information to the OIG in conjunction with an OIG investigation, audit, evaluation, or other review, and may also provide information through the Hotline application or otherwise. The extent of the information provided varies, but may include, at a minimum, an individual's name, job position, and contact information. FDIC OIG personnel will also input PII for subjects and witnesses for ongoing investigations.
Financial Institutions (FI)	Bank records, loan files, and other financial information that may contain PII may be obtained from FIs in conjunction with OIG investigative matters, audits, evaluations, or other reviews, and through the Hotline application, or otherwise.
Federal, State, Local agencies and Employees	Information related to investigations is often received from Federal, State and local agencies, including law enforcement partners. This information may include: names, addresses, DOBs, SSNs, and financial account data and other identifiers. Information about individuals related to an audit, evaluation or other review conducted by the OIG may be obtained from other federal agencies if deemed necessary and depending on the type and scope of an audit, evaluation, or other review.
Publicly Available Sources	PII may be obtained from public sources that include local, state and national media in electronic form, consumer reporting agencies, vendors providing support for investigations, and Internet sources, if deemed necessary for investigative, audit, evaluation, or other reviews.
Body Cameras	OIG body cameras may capture PII when recording devices are activated during investigative interactions with individuals, which may include FDIC employee/contractors, FI employee/contractors, or other members of the public. The data recorded is directly related to law enforcement activities and may include audio and video recordings of people and various other PII captured during recorded interactions.

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 FDIC's Assessment and Authorization process, which aligns with the Risk Management Framework. Information systems that process OIG investigative, audit, evaluation and other review information have been granted an ATO. The ATO for each FDIC information 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 Record Notice (SORN) does this information system or project operate? Provide number and name.

The applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake) operate under SORN FDIC-010, "Investigative Files of the Office of Inspector General," which covers investigative files, including memoranda, computer-generated background information, correspondence including payroll records, call records, email records, electronic case management, forensic, and tracking files, Hotline related records, reports of investigations with related exhibits, statements, affidavits, records or other pertinent documents, reports from or to other law enforcement bodies, pertaining to violations or potential violations of criminal laws, fraud, waste, and abuse with respect to administration of FDIC programs and operations, and violations of employee and contractor Standards of Conduct as set forth in section 12(f) of the Federal Deposit Insurance Act (12 U.S.C. 1822(f)), 12 CFR parts 336, 366, and 5 CFR parts 2634, 2635, and 3201. Records in this system may contain PII provided or obtained in connection with an investigation, such as names, social security numbers, dates of birth and addresses. This system may also contain such information as employment history, bank account numbers and information, drivers' licenses, educational records, criminal history, photographs, audio and video recordings, and other information of a personal nature provided or obtained in connection with an investigation

The Hotline application operates under SORN FDIC-034, "Office of Inspector General Inquiry Records," which covers individuals, including, but not limited to, members of the public, the media, contractors and subcontractors, Congressional sources, and employees of the FDIC or of other governmental agencies, who communicate with the OIG through written or electronic correspondence or telephonically, including the OIG

Hotline. The SORN also covers individuals who receive correspondence from the OIG and those who are the subject of correspondence to or from the OIG. Records transferred from the Hotline application to the ITS application are subject to the exemptions claimed under SORN FDIC-010 referenced above.

The applications and systems that support OIG audits, evaluations, and other reviews (the ATS application, OIGWIS, and related information maintained within the Data Lake) are not subject to the requirements of the Privacy Act of 1974 because the information is not retrieved by personal identifier. Therefore, a SORN is not required.

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

Neither SORN FDIC-010, "Investigative Files of the Office of Inspector General" nor SORN FDIC-034, "Office of Inspector General Inquiry Records" require amendment or revision. Generally, the FDIC conducts reviews of its SORNs every five years or as needed.

2.4 If a Privacy Act Statement[2] 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, "Forms Management Program."

Most PII collected and maintained by the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake) is obtained during the course of a criminal investigation. Providing a Privacy Act notice to individuals at the point of collection may not be feasible. Notice provided to individuals could interfere with the OIG's ability to obtain, serve, and issue subpoenas, warrants and other law enforcement mechanisms, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice to subjects of investigations would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

[2] *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.

With respect to the BCS, cameras will be positioned in obvious places on criminal investigators without compromising the criminal investigator's safety so that the public can visually determine if a criminal investigator is using a camera, as follows:

- If body armor is worn, the camera will be worn on the outside/front of the body armor. Body armor is worn over the criminal investigator's clothing.
- In the event a camera is deployed when body armor is not worn, the camera will be secured to the criminal investigator's outer clothing, lanyard, or belt.

Cameras also have indicator lights that indicate when they are recording.

OIG criminal investigators undergo rigorous training to become proficient law enforcement officers. The majority of FDIC criminal investigator training is provided by FLETC and the IGCIA. Criminal investigator training for criminal investigators helps develop interviewing skills; case management; search warrants; physical evidence; undercover electronic surveillance; and ethical behavior and core values. Required periodic training ensures that criminal investigators maintain high standards, comply with Attorney General Guidelines, and maintain needed investigative skills. OIG criminal investigators that are assigned body cameras are required to undergo mandatory initial training, as well as annual and periodic refresher training regarding proper use of the devices, adherence to OIG's BCS policy, legal considerations, and privacy, civil rights, and civil liberties safeguards.

The public facing Hotline application provides individuals with the ability to input various types of information, including PII, the extent of which may vary greatly. The Hotline application provides a Privacy Act Statement prior to the input and submission of any information. Callers to the OIG Hotline telephone number are directed via recorded message to access the Hotline application website to provide information, to provide the information via U.S. Mail, or to leave a voicemail. When Hotline-related information is received by means other than the online web portal, an OIG staff member will manually input the pertinent information provided to the Hotline application.

SORN FDIC-010, "Investigative Files of the Office of Inspector General," reflects an exemption from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake.) Additionally, information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

The information collected, used, maintained, and disseminated by the applications and systems that support OIG audits, evaluations, and other reviews (ATS application, OIGWIS, and related information maintained within the Data Lake) are not subject to

the requirements of the Privacy Act of 1974 because they do not retrieve information by personal identifier. Therefore, a Privacy Act Statement is not required.

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 individuals may not be aware that their information is collected and maintained within the various OIMS components.

Mitigation: With respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, the Hotline application, and investigative data maintained within the Data Lake), this PIA and the SORNs referenced in section 2.2 provide transparency related to the collection and maintenance of PII by those OIMS components. Additionally, the Hotline application provides a Privacy Act Statement to individuals prior to their input and submission of any information.

Depending on the nature of the investigation, OIG criminal investigators may ask persons 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.

Generally, most investigative PII that is collected and maintained is obtained during the course of a criminal investigation. Providing notice to individuals at the point of collection may not be feasible in some instances. Notice provided to individuals could interfere with OIG's ability to obtain, serve, and issue subpoenas, warrants and other law enforcement mechanisms, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice to subjects of investigations would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

With respect to the BCS, cameras will be positioned in obvious places on criminal investigators without compromising the criminal investigator's safety so that the public can visually determine if a criminal investigator is using a camera, as follows:

- If body armor is worn, the camera will be worn on the outside/front of the body armor. Body armor is worn over the criminal investigator's clothing.
- In the event a camera is deployed when body armor is not worn, the camera will be secured to the criminal investigator's outer clothing, lanyard, or belt.

Cameras also have indicator lights that indicate when they are recording.

It should be noted that SORN FDIC-010, reflects exemptions from the Privacy Act requirements related to notification and access with respect to the applications and systems that support OIG investigations, while information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

Additionally, access to certain investigative information, such as the particulars concerning civil or criminal proceedings, will be provided to an individual where a lawful requirement to provide such information exists. Further, investigative information collected by FDIC may be disclosed to an individual pursuant to federal rules of civil or criminal procedure or the appropriate order of a court.

The applications and systems that support OIG audits, evaluations, and other reviews (ATS application, OIGWIS, and related information maintained within the Data Lake) do not operate as Privacy Act systems of records. Therefore, they are not subject to the notification requirements of the Privacy Act of 1974. However, this PIA provides transparency that mitigates the risk of individuals not being aware that their information is collected and maintained by those OIMS components.

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 ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake do not have procedures for individual access. The PII maintained within the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake) is contained in Privacy Act systems of records that have been exempted from the Privacy Act individual access requirement. Providing access to the records contained in these applications and systems could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of FDIC or another agency. Additionally, access to the records could permit the individual who is the subject of an investigation to impede the investigation, tamper with witnesses or evidence, and avoid detection

or apprehension. In addition, permitting access to such information could disclose security-sensitive information that could be detrimental to the FDIC.

Access procedures for the Hotline application are detailed in SORN FDIC-034. However, as noted in that SORN, records transferred from the Hotline application to the ITS application are subject to the exemptions claimed under SORN FDIC-010, which includes an exemption from the Privacy Act individual access requirement.

Access to certain investigative information, such as the particulars concerning civil or criminal proceedings will be provided to an individual where a lawful requirement to provide such information exists. In addition, investigative information collected by FDIC may be disclosed to an individual pursuant to federal rules of civil or criminal procedure upon the appropriate discovery order of a court.

There are not procedures for individual access for the applications and systems that support OIG audits, evaluations, and other reviews (ATS application, OIGWIS, and related information maintained within the Data Lake). The PII maintained by these applications and systems is not contained in a Privacy Act system of record, and therefore, is not subject to the Privacy Act individual access requirement.

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

The applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake) do not have procedures to allow individuals to correct inaccurate or erroneous information. The PII maintained by these applications and systems is contained in Privacy Act systems of records that have been exempted from the Privacy Act individual access and amendment requirement.

During the course of investigations, the accuracy of information obtained or introduced may be unclear or the relevance of the information may not be immediately apparent. In the interest of effective law enforcement, it is appropriate to retain all possibly relevant information that may aid in establishing patterns of unlawful activity. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continuously reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to the FDIC.

Procedures for correcting records associated with the Hotline application are detailed in SORN FDIC-034. However, as noted in that SORN, records transferred from the

Hotline application to the ITS application are subject to the exemptions claimed under SORN FDIC-010, which includes an exemption to the individual access and amendment requirement of the Privacy Act.

The applications and systems that support OIG audits, evaluations, and other reviews (ATS application, OIGWIS, and related information maintained within the Data Lake) do not have procedures to correct inaccurate or erroneous information. The PII maintained by these applications and systems is not contained in a Privacy Act system of records. Therefore, they are not subject to the Privacy Act individual access and amendment requirement.

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

The applications and systems that support OIG investigations (ITS application, the BCS, and ECUFL and investigative data maintained within the Data Lake) do not have procedures to allow individuals to correct inaccurate or erroneous information. The PII maintained by these applications and systems is contained in Privacy Act systems of records that have been exempted from the Privacy Act individual access and amendment requirement.

Procedures for correcting records associated with the Hotline application are detailed in SORN FDIC-034. However, as noted in that SORN, records transferred from the Hotline application to the ITS application are subject to the exemptions claimed under SORN FDIC-010, which include an exemption from the Privacy Act individual access and amendment requirement.

Individuals are not notified about the procedures for correcting their information maintained within the applications and systems that support OIG audits, evaluations, and other reviews (ATS application, OIGWIS, and related information maintained within the Data Lake). The PII maintained by these applications and systems is not contained in a Privacy Act system of record. Therefore, they are not subject to the Privacy Act individual access and amendment requirement.

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 within the various components of OIMS.

Mitigation: With respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake) and the Hotline application, SORN FDIC-010 and SORN FDIC-034 provide detailed procedures for

access and amendment to the information collected and maintained by those OIMS components. However, SORN FDIC-010 reflects an exemption from Privacy Act requirements related to individual access and amendment with respect to the ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake, while information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

The applications and systems that support OIG audits, evaluations, and other reviews (ATS application, OIGWIS, and related information maintained within the Data Lake) do not operate as Privacy Act systems of records. Therefore, they are not subject to the Privacy Act individual access and amendment requirement.

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

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 OIMS 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?

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 OIMS components. 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.

OIG criminal investigators undergo rigorous training to become proficient law enforcement officers. The majority of FDIC criminal investigator training is provided by FLETC and the IGCIA. Criminal investigator training for criminal investigators helps develop interviewing skills; case management; search warrants; physical evidence; undercover electronic surveillance; and ethical behavior and core values. Required periodic training ensures that criminal investigators maintain high standards, comply with Attorney General Guidelines, and maintain needed investigative skills.

With respect to the BCS, OIG criminal investigators that are assigned body cameras are required to undergo mandatory initial training, as well as annual and periodic refresher training regarding proper use of the devices, adherence to OIG's BCS policy, legal considerations, and privacy, civil rights, and civil liberties safeguards.

Additionally, the OIG conducts performance audits in accordance with GAGAS, evaluations in accordance with the CIGIE Quality Standards for Inspection and Evaluation, and other reviews in accordance with CIGIE's Quality Standards for Federal Offices of Inspector General. These standards require that OIG personnel collectively possess the skills and abilities to perform assigned tasks and require ongoing continuing professional education.

Further, 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 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 Annual Senior Agency Official for Privacy (SAOP) Report as required by 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.

For instance, access to the ITS application, the ATS application, the BCS, the Hotline application, and data maintained within the Data Lake requires individuals to be active users of the FDIC network. The FDIC's Access Request and Certification System (ARCS) is used to facilitate the tracking and management of FDIC employees that are users of the ITS application, the BCS, the ATS application, the Hotline application and the Data Lake. ARCS requests must be submitted by users and approved by managers in order to gain access to those applications. User access is further controlled and restricted according to specific user and administrative roles that have been defined and established within the ITS, ATS, the BCS, the Hotline application and the Data Lake. Each record within the applications and the Data Lake has an audit trail to track the modification and who made the changes (by person and date/time stamp).

Additionally, FDIC has implemented technologies to track and manage PII inventory, as well as to track, respond, remediate and report on breaches. Breaches are handled in accord with FDIC’s Breach Response Plan.

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, in accordance with the Privacy Act of 1974 and 12 C.F.R. part 310. Disclosures are not made directly from the various OIMS components. Disclosures of information held under SORN FDIC-010 and SORN FDIC-034 are made pursuant to the established routine uses as documented in the SORNs and other provisions of the Privacy Act which permit the sharing of information from a system of records. Accounting for disclosures occurs through notations within the various OIMS components, such as the notation of a referral of a Hotline report to another agency with jurisdiction to respond or investigate.

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. part 310. Because the accounting for disclosures is documented within the OIMS component records / case files, the accounting information will be retained for the life of the record.

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. part 310. SORN FDIC-010 and FDIC-034 each contain information on how an individual may request access to information in the system of records, including a request for an accounting of disclosures. SORN FDIC-010 provides an exemption from making accounting of disclosures available to individuals. Additionally, as noted in SORN FDIC-034, records transferred from the Hotline application to the ITS application are subject to the exemptions claimed under SORN FDIC-010.

Privacy Risk Analysis: Related to Accountability

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

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 Directive 1360.20, "FDIC Privacy Program," mandates that the collection of PII be in accordance with Federal laws and guidance. The OIMS components collect PII pursuant to the following laws and regulations:

- The IG Act of 1978, as amended, provides the FDIC OIG with oversight responsibility of the programs and operations of the FDIC.
- Executive Order 14074, *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety* (May 25, 2022).
- 12 U.S.C. § 1819: states that FDIC can make examinations of and to require information and reports from depository institutions.
- 12 U.S.C. § 1820: discusses examinations and the authority of FDIC to make and keep copies of information for FDIC's use.
- 12 U.S.C. § 1821: deals with Deposit Insurance, the Deposit Insurance Fund and closing and resolving financial institutions. The Corporation shall insure the deposits of all insured depository institutions as provided in this chapter.
- 12 U.S.C. § 1822: deals with FDIC as a Receiver of failed financial institutions.
- Executive Order 9397: stipulates the requirement for the use of SSNs by President Roosevelt.
- 12 C.F.R. § 330: clarifies the rules and define the terms necessary to afford deposit insurance coverage under the Act and provide rules for the recognition of deposit ownership in various circumstances.
- 12 C.F.R. § 366: deals with FDIC contractors.
- 5 C.F.R. § 720: deals with Affirmative Action.
- 5 U.S.C. § 7201: deals with antidiscrimination policy; minority recruitment program.

Privacy Risk Analysis: Related to Authority

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

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 PII that are relevant and necessary to accomplish the legally authorized purpose of collection?

The PII elements collected and maintained within the various OIMS components are relevant and necessary to support the functions and activities associated with OIG investigations, audits, evaluations, and other reviews.

It should be noted, however, that SORN FDIC-010 reflects an exemption from the Privacy Act requirement regarding the maintenance of records that are relevant and necessary with respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake). Additionally, information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

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?

The PII elements collected and maintained within the various components of OIMS are relevant and necessary to support OIG investigations, audits, evaluations, and other

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

reviews. OIG criminal investigators undergo extensive training, including federal law enforcement training, specific to individuals' rights and obligations in the context of responding to OIG investigative inquiries, and OIG has policies and procedures in place addressing individuals' rights and obligations that vary depending on the type of investigation and on whether the individual is a federal employee. In turn, OIG auditors collect and maintain only that PII which is required to meet the objective of the audits, evaluations or other reviews that they conduct. OIG auditors are required to maintain continuing professional education in accordance with GAGAS, the CIGIE Quality Standards for Inspection and Evaluation, and/or CIGIE's Quality Standards for Federal Offices of Inspector General.

It should be noted, however, that SORN FDIC-010 reflects an exemption from Privacy Act requirements related to notification and the maintenance of records that are relevant and necessary with respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake). Additionally, information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

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 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, and the OIG's policies and procedures related to the OIG Records Disposition Program, as follows:

- Files of internal audits, evaluations, and other reviews of FDIC programs, operations, and procedures; external audits and other reviews of contractors and grantees; and quality reviews of OIG activities are deleted/destroyed after eight years.

- Records having national media attention, involving a Congressional investigation, and/or that have been deemed to have historical value, may be held permanently.

- Files containing information or allegations which are of an investigative nature, but do not relate to a specific investigation, are deleted/destroyed after five years.

- Files developed during investigations are deleted/destroyed ten years after the cases are closed. These records include cases of known or alleged fraud and abuse, and irregularities and violations of laws and regulations, including hotline cases related to specific investigations.

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.

With respect to the BCS, OIG criminal investigators may review audio/video recordings for teachable scenarios. If a teachable scenario is found in a particular recording, a copy of the recording will be made for training purposes. OIG personnel included in such recordings will be given the option to have their faces redacted and/or voices changed in the recording. The un-redacted BWC recording will be deleted after all changes are made to the training video.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: There is a risk that the PII collected within the various OIMS components in the course of an investigation, audit, evaluation, or other review may be unnecessary or excessive, or may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: This risk is mitigated by OIMS users being appropriately trained, and by FDIC and OIG policies regarding the collection, use, and retention of information in conjunction with

the OIG's responsibilities for conducting investigations, audits, evaluations, and other reviews.

For instance, OIG criminal investigators undergo rigorous training to become proficient law enforcement officers. The majority of FDIC criminal investigator training is provided by FLETC and the IGCIA, which is part of FLETC. Criminal investigator training for criminal investigators helps develop interviewing skills; case management; search warrants; physical evidence; undercover electronic surveillance; and ethical behavior and core values. Required periodic training ensures that criminal investigators maintain high standards, comply with Attorney General Guidelines, and maintain needed investigative skills.

Additionally, OIG criminal investigators that are assigned body cameras are required to undergo mandatory initial training, as well as annual and periodic refresher training regarding proper use of the devices, adherence to OIG's BCS policy, legal considerations, and privacy, civil rights, and civil liberties safeguards. Additionally, the OIG's BCS policy stipulates when criminal investigators should activate and deactivate cameras during law enforcement operations, and also addresses approved exceptions to those requirements, such as de-activating cameras when obtaining emergency medical attention or using the restroom. An intentional failure to activate a camera recording or the unauthorized termination of a camera recording may result in disciplinary action.

OIG Auditors collect and maintain documentation and evidence in conjunction with the conduct of audits, evaluations, and other reviews in accordance with GAGAS, evaluations in accordance with the CIGIE Quality Standards for Inspection and Evaluation, and other reviews in accordance with CIGIE's Quality Standards for Federal Offices of Inspector General.

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 sensitive 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."

Privacy Risk: There is a potential risk that PII could be used in the test or lower environments beyond that which is necessary.

Mitigation: The FDIC has developed an enterprise test data strategy to mask or utilize synthetic data in the test and lower environments whenever possible, and to ensure all environments are secured appropriately based on the impact level of the information and the information system. Project teams are required to consult with the FDIC Privacy Program to identity PII and ensure it is adequately protected or transformed before it is used in test or lower environments.

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.

With respect to investigative functions and activities, the OIG's OI has an editing and review process for all OIG Reports of Investigations. Criminal investigators are instructed to ensure accuracy and thoroughness through the investigative process; to consider confidentiality and security issues; to include disclosure caveats where appropriate; and to use electronic and other verification services to verify information as appropriate. The particular methods used to verify information compiled during the course of an investigative matters vary considerably depending on the type of investigation.

Methods may include reference to commercial databases to: obtain background information; verify addresses, identities, and contact information; trace proceeds from illegal activities; identify possible witnesses; and for other investigative purposes. In addition, each record has a unique file number to prevent duplication. OIG verifies records by checking every incoming complaint to ensure that OIG has not received the same complaint previously. If so, OIG cross-references the two complaints; if not, the complaint is processed as a new entry. Information contained in the complaint is verified through the investigative process, which varies depending on the allegation and information at issue. OIG also updates the ITS application with timely information on referrals, administrative actions, prosecutions, civil enforcements, and other information addressing the status of, or results of, an investigation or complaint review.

A web-based evidence management component of BCS is used to manage BCS audio/video files, as well as other investigative documentation. Permissions for the evidence management component are managed in tandem with FDIC's ARCS. Users of the evidence management component are assigned a role with specific permissions limiting access to information on a need-to-know basis. The evidence management component includes safeguards and audit trails to restrict and log the access to those having a need-to-know. Additionally, with respect to BCS, users are prohibited from

deleting, editing, or modifying any recording maintained in the evidence management component unless expressly permitted by OIG's BCS policy.

With respect to the ECUFL, the Electronic Crimes Unit (ECU) is a group of criminal investigators and analysts within the OI that conducts and provides effective and timely forensic accounting and digital evidence acquisition/analysis support for criminal investigative activity nationwide. ECU investigations are governed by OI policy and are conducted in compliance with Department of Justice Guidance; Federal Rules of Evidence; the CIGIE Quality Standards for Investigation; and CIGIE Quality Standards for Digital Forensics.

The ECUFL system is a separate environment designed to support the acquisition, preservation, and analysis of Electronically Stored Information (ESI) in support of OIG authorities pursuant to the IG Act. The ECUFL consists of various workstations, servers, forensic software and tools that support digital forensics collection and analysis. ESI is collected following best computer forensics processes for analyzing digital evidence through various legal processes and authorities. ESI may contain PII due to the nature of forensic analysis and is not known prior to collection and analysis of the ESI. Only authorized ECU criminal investigators and analysts have access to the data within the logically separated environment. Information in the ECUFL may also be shared with others on a need-to-know basis in order to fulfill OIG requirements pursuant to the IG Act.

With respect to the functions and activities associated with the OIG's audits, evaluations, and other reviews, the rigor and depth of the OIG's validation of information, including PII, is required by GAGAS to be appropriate to the scope of the audit. The level of data validation may vary depending on the nature of a particular review. Data validation is necessary when the information itself is intended to materially support conclusions regarding the audit's objectives. Typically, the integrity of data is validated by processes such as (1) gaining an understanding of controls relating to the data itself through interviews, policy reviews, and observation; (2) use of corroborating evidence - for example, tracing a sample of records back to original sources or comparing data from different systems; and/or (3) testing of the data itself for things like completeness, duplication, outliers, or expected relationships.

With respect to the Data Lake, the OIG manages all permissions for access to its data within the Data Lake in tandem with FDIC's ARCS. The OIG assigns OIG personnel as users of the Data Lake with specific permissions limiting access to information on a need-to-know basis. Access to the Data Lake is logged and monitored to ensure access is restricted to those within the OIG having a need-to-know.

With respect to OIGWIS, content that is uploaded to the site is reviewed to ensure that all information is publicly releasable in accord with OIG's policies and procedures that address the release of information and reports to the public, the media, and Congress.

Generally, it should be noted that SORN FDIC-010 reflects an exemption from the Privacy Act requirement related to the accuracy, relevance, timeliness, and completeness of records maintained with respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake). Additionally, information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

Additionally, 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.

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

With respect to investigative functions and activities, OIG criminal investigators collect and analyze evidence through a number of techniques, including: interviews of complainants, witnesses, victims, and subjects; reviews of records (e.g., personnel files, contract, financial records, etc.); collection of forensic evidence; surveillance and consensual monitoring; and use of computer technology (e.g., link analysis, databases, spreadsheets, cyber forensics, data mining, etc.). The decision-making process with respect to what information is required for a specific investigation and how that information should be obtained, varies considerably depending on the type of investigation underway.

Additionally, OIG criminal investigators undergo extensive training, including federal law enforcement training, specific to individuals' rights and obligations in the context of responding to OIG investigative inquiries. The OIG has policies and procedures in place addressing individuals' rights and obligations that vary depending on the type of investigation and on whether the individual is a federal employee.

OIG auditors may request records from an auditee that include PII that the auditee has collected or has been provided. The OIG may collect and maintain those records if the PII is necessary to meet the audit's objective. OIG uses PII in the records obtained from auditees and maintained in the ATS application to assess auditee compliance or performance relative to those audit objectives.

It should be noted, however, that SORN FDIC-010 reflects an exemption from the Privacy Act requirement related to the collection of PII directly from individuals with respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake). Additionally, information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

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.

With respect to investigative functions and activities, OIG's OI has an editing and review process for all OIG Reports of Investigations. Criminal investigators are instructed to ensure accuracy and thoroughness through the investigative process; to consider confidentiality and security issues; to include disclosure caveats where appropriate; and to use electronic and other verification services to verify information as appropriate. The particular methods used to verify information compiled during the course of an investigation vary considerably depending on the type of investigation. Methods may include reference to commercial databases to: obtain background information; verify addresses, identities, and contact information; trace proceeds from illegal activities; identify possible witnesses; and for other investigative purposes. In addition, each record has a unique file number to prevent duplication. OIG verifies records by checking every incoming complaint to ensure that OIG has not received the same complaint previously. If so, OIG cross-references the two complaints; if not, the complaint is processed as a new entry. Information contained in the complaint is verified through the investigative process, which varies depending on the allegation and information at issue. OIG also updates ITS with timely information on referrals, administrative actions, prosecutions, civil enforcements, and other information addressing the status of, or results of, an investigation or complaint review.

With respect to the BCS, cameras are used to record interactions in real-time to maintain an audio/video record of law enforcement operations. The use of body cameras is governed by OIG policy.

With respect to the ECUFL, the ECU is a group of criminal investigators and analysts within the OI that conducts and provides effective and timely forensic accounting and digital evidence acquisition/analysis support for criminal investigative activity nationwide. ECU investigations are governed by OI policy and are conducted in compliance with Department of Justice Guidance; Federal Rules of Evidence; the CIGIE Quality Standards for Investigation; and CIGIE Quality Standards for Digital Forensics.

The ECUFL is separate environment designed to support the acquisition, preservation, and analysis of ESI in support of OIG authorities pursuant to the IG Act. The ECUFL consists of various workstations, servers, forensic software and tools that support digital forensics collection and analysis. ESI is collected following best computer forensics processes for analyzing digital evidence through various legal processes and authorities. ESI may contain PII due to the nature of forensic analysis and is not known prior to collection and analysis of the ESI. Only authorized ECU criminal investigators and analysts have access to the data within the logically separated environment. Information in the ECUFL may also be shared with others on a need-to-know basis in order to fulfill OIG requirements pursuant to the IG Act.

With respect to information collected through audits, evaluations, and other reviews, data is verified for accuracy as part of the audit process, in accord with the OIG's quality assurance policies and procedures. The exact methods will depend upon the nature of the data and the objectives of the audit.

With respect to the Data Lake, the OIG manages all permissions for access to its data within the Data Lake in tandem with FDIC's ARCS. The OIG assigns OIG personnel as users of the Data Lake with specific permissions limiting access to OIG information on a need-to-know basis. Access to the Data Lake is logged and monitored to ensure access is restricted to those within the OIG having a need-to-know.

With respect to OIGWIS content that is uploaded to the site is reviewed to ensure that all information is publicly releasable in accord with OIG's policies and procedures.

It should be noted, however, that SORN FDIC-010 reflects an exemption from the Privacy Act requirement related to the accuracy, relevance, timeliness, and completeness of records maintained with respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake). Additionally, information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

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

The ITS application, the ATS application, the Hotline application, and the Data Lake have technical security measures and controls in place to prevent the misuse of data. Such security measures and controls consist of: user identification and authentication, network/database permissions, automatic session lockout after a period of inactivity, automatic account lockout after a specified number of failed logon attempts, strong password requirements, and the deployment of firewalls that protect network connections and prevent unauthorized access. These applications also use data encryption when data is transferred to and from the applications database and user workstations. System user access to information is controlled using access lists that are based on a person's business need to know. Further, FDIC employees must complete FDIC's Corporate Information Security and Privacy Awareness Training on an annual basis.

A web-based evidence management component of BCS is used to manage BCS audio/video files, as well as other investigative documentation. Permissions for the evidence management component are managed in tandem with FDIC's ARCS. Users of the evidence management component are assigned a role with specific permissions limiting access to information on a need-to-know basis. The evidence management component includes safeguards and audit trails to restrict and log the access to those having a need-to-know. Additionally, with respect to BCS, users are prohibited from deleting, editing, or modifying any recording maintained in the evidence management component unless expressly permitted by OIG's BCS policy.

The ECUFL is separate environment designed to support the acquisition, preservation, and analysis of ESI in support of OIG authorities pursuant to the IG Act. The ECUFL consists of various workstations, servers, forensic software and tools that support digital forensics collection and analysis. ESI is collected following best computer forensics processes for analyzing digital evidence through various legal processes and authorities. ESI may contain PII due to the nature of forensic analysis and is not known prior to collection and analysis of the ESI. Only authorized ECU criminal investigators and analysts have access to the data within the logically separated environment.

With respect to OIGWIS, content that is uploaded to the site is reviewed to ensure that all information is publicly releasable in accord with OIG's policies and procedures.

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 are no identifiable privacy risks related to data quality and integrity for OIMS.

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, when feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection.

Most investigative PII that is collected and maintained is obtained during the course of a criminal investigation. Providing notice to individuals at the point of collection may not be feasible in some instances. Notice provided to individuals could interfere with OIG's ability to obtain, serve, and issue subpoenas, warrants and other law enforcement mechanisms, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice to subjects of investigations would impede law enforcement in that it could compromise the existence of a

confidential investigation or reveal the identity of witnesses or confidential informants.

Depending on the nature of the investigation, OIG criminal investigators may ask persons 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.

With respect to the BCS, cameras will be positioned in obvious places on criminal investigators without compromising the criminal investigator's safety so that the public can visually determine if a criminal investigator is using a camera, as follows:

- If body armor is worn, the camera will be worn on the outside/front of the body armor. Body armor is worn over the criminal investigator's clothing.
- In the event a camera is deployed when body armor is not worn, the camera will be secured to the criminal investigator's outer clothing, lanyard, or belt.

Cameras also have indicator lights that indicate when they are recording.

With respect to the Hotline application, the OIG provides information about the Privacy Act to complainants on the online form, which provide individuals with an understanding of the consequences of approving or declining the authorization of the collection, use, dissemination, and retention of PII. If a Hotline complainant wishes to remain anonymous, the complaint can be submitted without the inclusion of any PII.

With respect to OIG audits, evaluations, and other reviews, auditors may request records from an auditee that include PII that an auditee has collected, or which has been provided to them by others. OIG auditors collect those records, which may contain PII, from the auditee only if the records are necessary to meet the audit's objective. Notice is provided during the initiation of an audit, and also through the publication of this PIA.

With respect to OIGWIS, information is not collected from site visitors, however, links are provided that enable visitors to access the OIG's Hotline application discussed above. OIGWIS also includes a link to FDIC's privacy policy.

With respect to the Data Lake, information maintained in the Data Lake is sourced from other OIMS components or from publicly available record sources. Notice is provided for the information subsequently maintained in the Data Lake when originally collected through the various OIMS components as described in this section.

Additionally, the SORNs referenced in Section 2.2 serve as notice of the information collections related to investigative and Hotline activities, while this PIA serves as notice of information collections related to the OIG's investigations, audits,

evaluations, and other reviews. Lastly, the FDIC Privacy Program reviews PIAs to ensure that PII collection is conducted with the consent of the individual to the greatest extent practicable.

It should be noted that SORN FDIC-010 reflects an exemption from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake). Additionally, information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

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.

Most investigative PII that is collected and maintained is obtained during a criminal investigation. Providing notice to individuals at the point of collection may not be feasible in some instances. Notice provided to individuals could interfere with OIG's ability to obtain, serve, and issue subpoenas, warrants and other law enforcement mechanisms, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice to subjects of investigations would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

Depending on the nature of the investigation, OIG criminal investigators may ask persons 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.

With respect to the BCS, cameras will be positioned in obvious places on criminal investigators without compromising the criminal investigator's safety so that the public can visually determine if a criminal investigator is using a camera, as follows:

- If body armor is worn, the camera will be worn on the outside/front of the body armor. Body armor is worn over the criminal investigator's clothing.
- In the event a camera is deployed when body armor is not worn, the camera will be secured to the criminal investigator's outer clothing, lanyard, or belt.

Cameras also have indicator lights that indicate when they are recording.

With respect to the Hotline application, the OIG provides information about the Privacy Act to complainants on the online form, which provide individuals with an understanding of the consequences of approving or declining the authorization of the

collection, use, dissemination, and retention of PII. If a Hotline complainant wishes to remain anonymous, the complaint can be submitted without the inclusion of any PII.

With respect to OIG audits, evaluations, and other reviews, auditors may request records from an auditee that include PII that an auditee has collected, or which has been provided to them by others. OIG Auditors collect those records, which may contain PII, from the auditee only if the records are necessary to meet the audit's objective. Notice is provided during the initiation of an audit, and also through the publication of this PIA.

With respect to OIGWIS, information is not collected from site visitors, however, links are provided enabling visitors to access the OIG's Hotline application discussed above. OIGWIS also includes a link to FDIC's privacy policy.

With respect to the Data Lake, information maintained in the Data Lake is sourced from other OIMS components or from publicly available record sources. Notice is provided for the information subsequently maintained in the Data Lake when originally collected through the various OIMS components as described in this section.

Additionally, the SORNs referenced in Section 2.2 serve as notice of the information collections related to investigative and Hotline activities, while this PIA serves as notice regarding information collections related to OIG investigations, audits, evaluations, and other reviews. 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.

It should be noted that SORN FDIC-010 reflects an exemption from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the applications and systems that support OIG investigations (ITS application, the BCS the ECUFL, and investigative data in the Data Lake). Additionally, information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

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 SORN(s) 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.

It should be noted that SORN FDIC-010 reflects exemptions from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake). Additionally, information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

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 various OIMS components only use PII for the purposes listed in Section 9.1 of this PIA. This PIA and SORNs FDIC-010 and FDIC-034 serve as notice for all uses of that PII.

It should be noted, however, that SORN FDIC-010 reflects an exemption from the Privacy Act requirements related to obtaining consent from or informing individuals of the authority, purpose, and routine uses of the information collected with respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake). Additionally, information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the ITS application.

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 individuals will not know how their data is being used or shared, nor be provided with an opportunity to authorize or opt out of any new uses of data pertaining to them.

Mitigation: With respect to the applications and systems that support OIG investigations (ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake) and the Hotline application, this PIA and SORNs FDIC-010 and FDIC-034 provide detailed information to the public regarding how that information will be used and shared.

Additionally, the Hotline application provides a Privacy Act Statement to individuals prior to their input and submission of any information.

Additionally, access to certain investigative information, such as the particulars concerning civil or criminal proceedings, will be provided to an individual where a lawful requirement to provide such information exists. Further, information collected by OIG may be disclosed to an individual pursuant to federal rules of civil or criminal procedure upon the appropriate discovery order of a court.

It should be noted, however, that SORN FDIC-010 reflects an exemption from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the ITS application, the BCS, the ECUFL, and investigative data maintained within the Data Lake, while information collected through the Hotline application may also be exempt, as stipulated in SORN FDIC-034, if the records are transferred to the OIG ITS application.

With respect to the applications and systems that support OIG audits, evaluations, and other reviews (ATS application, OIGWIS, and non-investigative data maintained within the Data Lake), they do not operate as Privacy Act systems of records. Therefore, they are not subject to the notice requirements of the Privacy Act of 1974. However, this PIA serves as notice with respect to the collection, use, and disclosure of PII by those OIMS components.

Privacy Risk: With respect to the BCS, there is a risk that individuals may not receive adequate notice that their images and voice communications may be recorded when they are in close proximity to a law enforcement encounter, regardless of whether they are directly or indirectly involved.

Mitigation: Cameras worn by OIG criminal investigators will be positioned in obvious places on the criminal investigators, without compromising the criminal investigator's safety, so that the public can visually determine if a criminal investigator is using a camera, as follows:

- If a body armor is worn, the camera will be worn on the outside/front of the body armor. Body armor is worn over the criminal investigator's clothing.
- In the event a camera is deployed when body armor is not worn, the camera will be secured to the criminal investigator's outer clothing, lanyard, or belt.

Cameras also have indicator lights that indicate when they are recording. Additionally, the FDIC also provides general notice to the public through this Privacy Impact Assessment.

It should be noted, however, that SORN FDIC-010 reflects an exemption from the Privacy Act requirements related to informing individuals of the authority, purpose, and routine uses of the information collected with respect to the BCS.

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.

The OIG collects information in order to meet its responsibilities under the IG Act to conduct investigations, audits, evaluations and other reviews relating to FDIC programs and operations. The OIG collects information only where the OIG has specific legal authority to do so and the information is required to meet the OIG's responsibilities, including those expressly established under the IG Act. Commercial data is sometimes collected as background information; to verify addresses, identities, and business data. BCS information may be used as evidence in OIG investigations and for OIG investigative training purposes. Investigative data may be shared within and among other law enforcement agencies as needed to further an investigation. Information collected and maintained for audit, evaluation, and other review purposes may be shared with other federal OIGs in conjunction with periodic peer review requirements stipulated in GAGAS.

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, 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" 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.

Access to all investigative, audit, evaluation, and other review information is based on an official need to know. OIMS users include authorized OIG Investigations, Audit, and Evaluation staff and authorized OIG Executive Management and Counsel to the Inspector General. Information Technology staff of the OIG's Office of Management

have access to OIMS components for system support purposes. A limited number of FDIC Division of Information Technology (DIT) LAN Management system administrators and support staff also have access to various OIMS components for the purpose of supporting hardware and network services.

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

Access to OIMS information is based on an official need to know. OIG user access to the ITS, the BCS, the Hotline application, the ATS application, and the Data Lake requires individuals to be active users of the FDIC network. The FDIC's ARCS is used to facilitate the tracking and management of FDIC employees that are users of those applications. ARCS requests must be submitted by users and approved by managers in order to gain access to those applications. User access is further controlled and restricted according to specific user and administrative roles that have been defined and established within those applications.

A web-based evidence management component of BCS is used to manage BCS audio/video files, as well as other investigative documentation. Permissions for the evidence management component are managed in tandem with FDIC's ARCS. Users of the evidence management component are assigned a role with specific permissions limiting access to information on a need-to-know basis. The evidence management component includes safeguards and audit trails to restrict and log the access to those having a need-to-know. Additionally, with respect to BCS, users are prohibited from deleting, editing, or modifying any recording maintained in the evidence management component unless expressly permitted by OIG's BCS policy.

With respect to the ECUFL, only authorized ECU criminal investigators and analysts have access to the data within the logically separated environment.

The information on OIGWIS is available to the public. Content that is uploaded to the site is reviewed to ensure that all information is publicly releasable in accord with OIG's policies and procedures.

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. [If the system exchanges information, please detail the information that is being exchanged as well as the rationale for the exchange].

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?

With the exception of the Data Lake, the various OIMS components do not aggregate or consolidate data in order to make determinations or derive new data about individuals. With respect to the Data Lake, information aggregated or consolidated in the Data Lake is pertinent to OIG investigative and audit casework. Access to OIG information in the Data Lake is logged and monitored and is restricted to those OIG personnel having a need-to-know.

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.

Information collected and maintained by the ITS application, the BCS, the Hotline application, the ECUFL, and investigative data maintained within the Data Lake may be shared externally pursuant to the routine uses described in the SORNs referenced in Section 2.2. Some of this external sharing may also be supported by information sharing agreements with other agencies or foreign governments.

Information collected and maintained by the ATS application and related information maintained in the Data Lake may be shared with other Federal OIGs in conjunction with periodic peer review requirements stipulated within the GAGAS and CIGIE's Quality Standards for Inspection and Evaluation.

Additionally, information collected and maintained in conjunction with the OIG's responsibilities for investigations, audits, evaluations and other reviews may be shared on OIGWIS. Information shared on the website is reviewed prior to publication to ensure that all information is publicly releasable in accord with OIG's policies and procedures.

Further, 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 and FDIC Directive 1360.20 "Privacy Program." 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 1360.09.

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.

OIG criminal investigators undergo extensive training, including Federal law enforcement training, specific to individuals' rights and obligations in the context of responding to OIG investigative inquiries. OIG criminal investigators that are assigned body cameras are required to undergo mandatory training regarding proper use of the devices, adherence to OIG's BCS policy, legal considerations, and privacy, civil rights, and civil liberties safeguards. The OIG has policies and procedures in place addressing the rights and obligations of individuals that vary depending on the type of investigation and on whether the individual is a federal employee.

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.

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.

OIG criminal investigators undergo extensive training, including federal law enforcement training, specific to individuals' rights and obligations in the context of responding to OIG investigative inquiries. OIG criminal investigators that are assigned body cameras are required to undergo mandatory training regarding proper use of the devices, adherence to OIG's BCS policy, legal considerations, and privacy, civil rights, and civil liberties safeguards. The OIG has policies and procedures in place addressing the release of information and the rights and obligations of individuals that vary depending on the type of investigation and on whether the individual is a federal employee.

Additionally, annual Information Security and Privacy Awareness Training is mandatory for all FDIC staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: There is a potential risk associated with purpose and use limitation for OIMS because sensitive information, including PII, stored in the various components of OIMS could potentially be used or shared for a purpose not compatible with the original purpose for which the information was collected.

Mitigation: This risk is mitigated by OIG staff being appropriately trained and limiting OIG employee access to only that information for which there is a business need. This risk is further mitigated by OIG policies and procedures that address the appropriate release of information.

With respect to the BCS, the OIG's BCS policy prohibits the use of body cameras for personal use or for purposes other than those related to official law enforcement duties. The OIG's BCS policy restricts personnel from recording events that are not law enforcement encounters and governs the use of recorded data. Additionally, the OIG may use redaction software to blur images or portions of images, or minimize audio content, when making copies of BCS recordings for disclosure or sharing where the content contains law enforcement sensitivities or privacy concerns, including recordings of undercover personnel, confidential informants, sensitive investigative techniques or equipment, minors, injured or incapacitated individuals, or sensitive locations such as restrooms, locker rooms, or medical facilities.

Further, since unauthorized use or release of body camera recorded data may compromise ongoing criminal investigations and administrative proceedings, or violate the privacy rights of recorded individuals, any unauthorized access, use, or release of recorded data or other violation of confidentiality laws and OIG policies may result in disciplinary action.

Privacy Risk: There is a risk that OIG criminal investigators may record facial and video images outside the scope of a law enforcement encounter.

Mitigation: The OIG's BCS policy limits recordings to official law enforcement encounters that support the OIG's investigative mission, in accordance with the OIG's BCS policy. OIG criminal investigators are trained in the operation and care of body cameras, appropriate handling of body camera evidence, privacy procedures, civil rights and civil liberties restrictions, and the appropriate and permissible use of body camera evidence. Misuse of body camera data, including improper recording, improper dissemination, or tampering with data may result in disciplinary action.

Privacy Risk: There is a potential risk associated with purpose and use limitation that OIG data maintained in the Data Lake could be accessed by OIG staff and FDIC employees or contractors that are not properly authorized to access the OIG's data in the Data Lake.

Mitigation: This risk is mitigated through the controls the OIG has established to ensure that access to the OIG's data within the Data Lake is restricted to OIG staff having an official need-to-know. ARCS is used to facilitate the tracking and management of OIG employees that are users of the OIG's data in the Data Lake. ARCS requests must be submitted by OIG users and

approved by their managers to gain access to the OIG's data in the Data Lake. User access is further controlled and restricted according to specific user and administrative roles that have been defined and established by the OIG for the OIG's data within the Data Lake, and access to the OIG's information in the Data Lake is logged and monitored by OIG staff.

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 seeks to properly align the management of IT risks with the FDIC's Enterprise Risk Management (ERM) 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 OIMS.

Mitigation: No mitigation actions are recommended.