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

March 31, 2022
PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

An FDIC Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) the FDIC collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. The FDIC publishes its PIAs, as well as its system of records Notices (SORNs), on the FDIC'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

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 halt the fraudulent conduct 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

\(^1\) [www.fdic.gov/privacy](http://www.fdic.gov/privacy)
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 OIG 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 Hotline application (Hotline)** used to record and track information received via the OIG Hotline website, telephone 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)** that supports the OIG in carrying out its investigative mission. The ECUFL is a logically separate environment that is maintained and used by OIG 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 contractor-supported copying and transcription service (CTS)** that may be used by the OIG in instances where records related to an investigation or audit require copying/scanning or when interviews conducted and recorded by the OIG in conjunction with an investigation or audit require transcription.
- **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 of OIMS, we 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 ITS application, the ECUFL, and the Hotline application, 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. It should be noted, however, that SORN FDIC-010 reflects exemptions from the Privacy Act requirements related to notification and access with respect to the ITS application and the ECUFL, 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.
Access to certain 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, most or all of the information collected by the OIG may be disclosed to an individual pursuant to federal rules of civil or criminal procedure upon the appropriate discovery order of a court.

With respect to the ATS application, the CTS, and OIGWIS, they 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 serves as notice with respect to the collection, use, and disclosure of PII 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 ITS application, the ECUFL, 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 OIMS ITS application and the ECUFL, 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, in the event of criminal or civil proceedings, an individual may challenge user mistakes and the errors or untruthfulness of a witness in the evidence and testimony presented in those proceedings. The individual may also petition a court to direct FDIC to expunge or correct an error in an OIMS investigative-related record.

With respect to the ATS application, the CTS, and OIGWIS, they do not operate as Privacy Act systems of records. Therefore, they are not subject to the Privacy Act redress requirement.

**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 investigator training is provided by the Federal Law Enforcement Training Centers (FLETC) and the Inspector General Criminal Investigator Academy (IGCIA). Criminal investigator training for investigators helps develop interview skills; case management; search warrants; physical evidence; undercover electronic surveillance; and ethical behavior and core values. Required periodic training ensures that 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.

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 1360.9, “Protecting Sensitive 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 Circular 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.

---

**Section 1.0: Information System**

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

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.

<table>
<thead>
<tr>
<th>PII Element</th>
<th>Investigative Tracking and Support Application</th>
<th>Hotline Application</th>
<th>Electronic Crimes Unit Forensics Lab</th>
<th>Copying and Transcription Services</th>
<th>Audit Tracking and Support Application</th>
<th>OIG Public Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Name</td>
<td>☒</td>
<td>☒</td>
<td></td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Date of Birth (DOB)</td>
<td>☒</td>
<td>☒</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Place of Birth</td>
<td>☒</td>
<td>☐</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Social Security number (SSN)</td>
<td>☒</td>
<td>☒</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Employment Status, History or Information</td>
<td>☒</td>
<td>☒</td>
<td></td>
<td></td>
<td></td>
<td>☒</td>
</tr>
<tr>
<td>Mother’s Maiden Name</td>
<td>☒</td>
<td>☐</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Certificates (e.g., birth, death, naturalization, marriage, etc.)</td>
<td>☒</td>
<td>☐</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Medical Information (Medical Records Numbers, Medical Notes, or X-rays)</td>
<td>☒</td>
<td>☒</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Home Address</td>
<td>☒</td>
<td>☒</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Phone Number(s)</td>
<td>☒</td>
<td>☒</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Email Address</td>
<td>☒</td>
<td>☒</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Employee Identification Number (EIN)</td>
<td>☒</td>
<td>☒</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)</td>
<td>☒</td>
<td>☒</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Driver’s License/State Identification Number</td>
<td>☒</td>
<td>☐</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Vehicle Identifiers (e.g., license plates)</td>
<td>☒</td>
<td>☐</td>
<td></td>
<td></td>
<td></td>
<td>☐</td>
</tr>
<tr>
<td>Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)</td>
<td>☒</td>
<td>☒</td>
<td></td>
<td></td>
<td></td>
<td>☒</td>
</tr>
</tbody>
</table>
### PII Element

<table>
<thead>
<tr>
<th>PII Element</th>
<th>- Investigative Tracking and Support Application</th>
<th>Audit Tracking and Support Application</th>
<th>OIG Public Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education Records</td>
<td>☒</td>
<td>☒</td>
<td>☐</td>
</tr>
<tr>
<td>Criminal Information</td>
<td>☒</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Military Status and/or Records</td>
<td>☒</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Investigation Report or Database</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Biometric Identifiers (e.g., fingerprint, voiceprint)</td>
<td>☒</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Photographic Identifiers (e.g., image, x-ray, video)</td>
<td>☒</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Other (Other potential investigative sources such as social media)</td>
<td>☒</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Description of Information Provided by Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Members of the General Public</td>
<td>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.</td>
</tr>
<tr>
<td>FDIC Employees</td>
<td>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.</td>
</tr>
<tr>
<td>Financial Institutions (FI)</td>
<td>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.</td>
</tr>
<tr>
<td>Federal, State, Local agencies and Employees</td>
<td>Information related to investigations is often received from Federal, State and local 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.</td>
</tr>
</tbody>
</table>

#### 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 or are in the process of achieving 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 ITS application and the ECUFL 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.

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 information collected, used, maintained, or disseminated by the ATS application, the CTS, and OIGWIS is not subject to the requirements of the Privacy Act of 1974 because they do not retrieve information 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.**

The SORNs referenced in 2.2 do not require amendment or revision. Generally, the FDIC conducts reviews of its SORNs every three years or as needed.

2.4 **If a Privacy Act Statement is required, how is the Privacy Act Statement provided to individuals before collecting their PII? (The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.) Explain.**

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 Circular 1213.01, “Forms Management Program.”

Most PII collected and maintained by the ITS application and the ECUFL 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 in some instances. 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.

OIG criminal investigators undergo rigorous training to become proficient law enforcement officers. The majority of FDIC investigator training is provided by FLET and the IGCA. Criminal investigator training for 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 investigators maintain high standards, comply with Attorney General Guidelines, and maintain needed investigative skills.

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, “Exemptions Promulgated for This System,” 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 and the ECUFL. 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 ATS application, the CTS, and OIGWIS 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, FDIC’s 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 ITS application, the ECUFL, and the Hotline application, 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. It should be noted, however, that SORN FDIC-010, reflects exemptions from the Privacy Act requirements related to notification and access with respect to the ITS application and the ECUFL, 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-related 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, most or all of the investigative-related 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.
With respect to the ATS application, the CTS, and OIGWIS, they 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 and the ECUFL do not have procedures for individual access. The PII maintained within the ITS application and the ECUFL 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 the ITS application and the ECUFL 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-related 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.

The ATS application, the CTS, and OIGWIS do not have procedures for individual access. The PII maintained by the ATS application, the CTS, and OIGWIS 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 subject individual to correct inaccurate or erroneous information?

The ITS application and the ECUFL do not have procedures to allow individuals to correct inaccurate or erroneous information. The PII maintained by the ITS application and the ECUFL 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.

Additionally, an individual may challenge user mistakes and the errors or untruthfulness of a witness in the evidence and testimony presented in relevant criminal or civil proceedings. The individual may also petition a court to direct FDIC to expunge or correct an error in an ITS record.

The ATS application, the CTS, and OIGWIS do not have procedures to correct inaccurate or erroneous information. The PII maintained by the ATS application, the CTS, and OIGWIS 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 ITS application and the ECUFL do not have procedures to allow individuals to correct inaccurate or erroneous information. The PII maintained by the ITS application and the ECUFL 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.

The ATS application, the CTS, and OIGWIS do not notify individuals about the procedures for correcting their information. The PII maintained by the ATS application, the ECUFL, the CTS, and OIGWIS 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 ITS application, the ECUFL, 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 OIMS ITS application and the ECUFL, 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, in the event of criminal or civil proceedings, an individual may challenge user mistakes and the errors or untruthfulness of a witness in the evidence and testimony presented in those proceedings. The individual may also petition a court to direct FDIC to expunge or correct an error in an OIMS investigative-related record.

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

The FDIC’s Privacy Program staff supports the SAOP in carrying out those responsibilities through the management and execution of the FDIC’s Privacy Program. The Privacy Program has been fully integrated throughout the agency and is supported on a part-time basis by divisional information security managers located within the agency’s divisions and offices.

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

Risk analyses are an integral component of FDIC’s Privacy program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and PIAs. A PTA is used to determine whether a PIA is required under the E-Government Act of 2002 and the Consolidated Appropriations Act of 2005. A PIA is required for: (1) a new information technology (IT) system developed or procured by FDIC that collects or processes PII; (2) a substantially changed or modified system that may create a new privacy risk; (3) a new or updated rulemaking that may affect the privacy of PII in some manner; or (4) any other internal or external electronic collection activity or process that involves PII.

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

Privacy risks posed by the project are captured in PIAs, when conducted in accordance with applicable law, OMB policy, and FDIC policy. PIAs are posted on FDIC’s public-facing website, www.fdic.gov/privacy/.

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

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

---

4 Consolidated Appropriations Act, 2005, Public Law No. 108-447, Division H, Title V, Section 522.
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 is currently in the process of implementing a Privacy Continuous Monitoring (PCM) program in accordance with OMB Circular A-130.

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

The FDIC Privacy Program maintains an ongoing Privacy Training Plan that documents the development, implementation, and update of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. Annual Security and Privacy Training is mandatory for all FDIC employees and contractors and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program staff as well.

Additionally, OIG criminal investigators undergo rigorous training to become proficient law enforcement officers. The majority of FDIC investigator training is provided by FLETC and the IGCA. Criminal investigator training for 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 investigators maintain high standards, comply with Attorney General Guidelines, and maintain needed investigative skills.

Further, 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.

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

The FDIC Privacy Program develops reports both for internal and external oversight bodies through several methods, including the following: Annual SAOP report as required by FISMA; weekly reports to the SAOP; bi-weekly reports to the CISO, monthly meetings with the SAOP and CISO; Information Security Manager's Monthly meetings.

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

Privacy has been integrated within the FDIC Systems Development Life Cycle (SDLC), ensuring that stakeholders are aware of, understand, and address Privacy requirements throughout the SDLC, including the automation of privacy controls if possible.
For instance, access to the ITS application, the ATS application, and the Hotline application 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 ATS application, and the Hotline application. 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, and the Hotline applications. Each record within those applications 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?

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. 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.

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?

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 established routine uses as documented in the SORNs. 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.

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

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 established routine uses as documented in the SORNs. 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. 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 risks associated with 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 Circular 1360.20, “Privacy Program,” mandates that the collection of PII be in accordance with Federal laws and guidance. This particular project collects PII pursuant to the following laws:

- The IG Act of 1978, as amended, provides the FDIC OIG with oversight responsibility of the programs and operations of the FDIC.
- 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 banks. The Corporation shall insure the deposits of all insured depository institutions as provided in this chapter.
- 12 CFR § 330 clarifies the rules and defines the terms necessary to afford deposit insurance coverage under the Act and provide rules for the recognition of deposit ownership in various circumstances.
- 12 CFR § 366 deals with FDIC contractors.
- 5 CFR § 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 risks associated with 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 elements 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 ITS application and the ECUFL. 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 and retention of PII is limited to the PII that has been legally authorized to collect.

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 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 ITS application and the ECUFL. 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 and retention of PII is limited to the PII that has been legally authorized to collect.

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

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

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

Records are retained in accordance with FDIC Circular 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 is in the process of developing an enterprise test data strategy to reinforce the need to mask or utilize 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. Project teams are required to consult with the FDIC Privacy Program to identify PII and ensure it is adequately protected or transformed before it is used in test or lower environments.

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 investigator training is provided by FLETC and the IGCA, which is part of FLETC. Criminal investigator training for 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 investigators maintain high standards, comply with Attorney General Guidelines, and maintain needed investigative skills.

OIG Auditors collect and maintain documentation and evidence in conjunction with the conduct of audits, evaluations, and other reviews in accordance with GAS, 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 1360.9, “Protecting Sensitive 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 Circular 1210.01, “Records and Information Management Program,” which is informed by the Federal Records Act and NARA regulations.

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 is in the process of developing 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. 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 matter 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.

With respect to the ECUFL, the Electronic Crimes Unit (ECU) is a group of 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 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 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 CTS, access to data is limited to contractor staff having a business need, and in accord with their contractual requirements and signed confidentiality agreements with FDIC. Per the contractual agreement with FDIC, the contractor takes full responsibility for the conduct of its personnel to ensure the confidentiality, integrity and safeguarding of sensitive information and PII.
handled on behalf of FDIC. In addition, all contractor personnel must undergo FDIC background investigations prior to accessing FDIC data.

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 ITS application and the ECUFL. 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 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 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 ITS application and the ECUFL. 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 measures to check for and correct any inaccurate or outdated PII in its holdings.

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

With respect to investigative functions and activities, OIG’s OI has an editing and review process for all OIG Reports of Investigations. 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 ECUFL, the ECU is a group of 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 a 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 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 CTS, access to data is limited to contractor staff having a business need, and in accord with their contractual requirements and signed confidentiality agreements with FDIC. Per the contractual agreement with FDIC, the contractor takes full responsibility for the conduct of its personnel to ensure the confidentiality, integrity and safeguarding of sensitive information and PII handled on behalf of FDIC. In addition, all contractor personnel must undergo FDIC background investigations prior to accessing FDIC data.

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 ITS application and the ECUFL. 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, and the Hotline application 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.

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 investigators and analysts have access to the data within the logically separated environment.

With respect to the CTS, access to data is limited to contractor staff having a business need, and in accord with their contractual requirements and signed confidentiality agreements with FDIC. Per the contractual agreement with FDIC, the contractor takes full responsibility for the conduct of its personnel to ensure the confidentiality, integrity and safeguarding of sensitive information and PII handled on behalf of FDIC. In addition, all contractor personnel must undergo FDIC background investigations prior to accessing FDIC data.

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 its 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 systems or projects based on the FIPS 199 determination.

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

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

**Privacy Risk Analysis: Related to Data Quality and Integrity**

**Privacy Risk:** There are no identifiable risks associated with 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, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection.
Most investigative-related 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 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 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.

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 ITS application and the ECUIFL. 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-related 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 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 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.

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 ITS application and the ECUFL. 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, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

As appropriate, the FDIC Privacy Program will update and publish the relevant Privacy Act SORN(s), as well as the relevant PIA, to reflect any new uses or disclosures.

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 ITS application and the ECUFL. 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, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

The 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 informing individuals of the authority, purpose, and routine uses of the information collected with respect to the ITS application and the ECUFL. 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, 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 ITS application, the Hotline application, and the ECUFL, 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-related 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, most or all of the 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 and the ECUFL, 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 ATS application, the CTS, and OIGWIS, 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.

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. 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 Circular 1360.9 “Protecting Sensitive Information” with the use of various privacy controls. Additionally, annual
Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

Access to all investigative, audit, evaluation, and other review information is based on a business 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 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 a business need to know. Access to the ITS, the Hotline application, and the ATS applications 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.

With respect to the ECUFL, only authorized ECU Special Investigators/Analysts have access to the data within the logically separated environment.

With respect to CTS, access to data is limited to contractor staff with a business need to know and in accord with their contractual requirements and signed Confidentiality Agreements with FDIC. Per the contractual agreement with FDIC, the contractor takes full responsibility for the conduct of its personnel to ensure the confidentiality, integrity and safeguarding of sensitive information and PII handled on behalf of FDIC. In addition, all contractor personnel must undergo FDIC background investigations prior to accessing FDIC data.

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.

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

No, the various OIMS components do not aggregate or consolidate data in order to make determinations or derive new data about individuals.

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 Hotline application, and the ECUFL may be shared externally pursuant to the routine uses described in the SORNs referenced in Section 2.2.
Information collected and maintained by the ATS application 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.

Information collected and maintained by CTS may potentially be transferred to either the ITS application, where it could potentially be shared externally pursuant to the routine uses described in SORN FDIC-010 referenced in Section 2.2, or the ATS application, where it may be shared externally with other Federal OIGs in conjunction with periodic peer review requirements stipulated in 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, FDIC Circular 1360.20, “FDIC Privacy Program,” and FDIC Circular 1360.17, “Information Technology Security Guidance for FDIC Procurements/Third Party Products.” The FDIC also ensures that agreements regarding the sharing of PII with third parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Circular 1360.17 and FDIC Circular 1360.9.

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

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

Additionally, OIG 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 the rights and obligations of individuals that vary depending on the type of investigation and on whether the individual is a Federal employee.

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 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 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 Purpose and 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.

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 Section 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 project’s FIPS 199 determination. The FDIC Privacy Program will recommend the appropriate determination to the CISO should the potential loss of confidentiality be expected to cause a serious adverse effect on individuals.

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

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

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

Responses to privacy breaches are addressed in an organized and effective manner in accordance with the FDIC’s Breach Response Plan.

Privacy Risk Analysis: Related to Security

Privacy Risk: There are no identifiable risks associated with security for OIMS.

Mitigation: No mitigation actions are recommended.