Office of Information Technology (OIT)

Privacy Impact Assessment

eCase

July 7, 2023

1100 New York Ave NW
Washington, DC 20527

Overview

The U.S. International Development Finance Corporation (DFC) Office of Inspector General (OIG) uses an audit documentation management software, eCase, to document audit work as part of its overall mission to prevent, detect, and deter fraud, waste, and abuse in DFC's programs and operations around the world. eCase is a product of the Washington, D.C.-based company OPEXUS. The DFC OIG instance of eCase is used primarily as a repository of audit documentation gathered and documented during an audit. It provides a dynamic case management framework with the capability to power a wide range of workflow-driven processes and core case management functions, including the tracking and reporting of audits. The documentation retained will vary based on the objectives of the audit but may contain information such as financial data, date of birth, mailing addresses, telephone number, bank account numbers, zip codes and various other personally identifiable information (PII). eCase is a subscription-based software as a service solution that is authorized to operate as a federal Cloud Service Offering by the Federal Risk and Authorization Management Program (FedRAMP). This Privacy Impact Assessment (PIA) is being conducted because the DFC OIG uses eCase to collect, maintain, or disseminate information in identifiable form from or about members of the public as well as sensitive PII from or about members of the public, DFC employees, and/or contractors.

Section 1. Characterization of the Personally Identifiable Information (PII)

The following questions are intended to define the scope of the PII requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What PII is collected, used, disseminated, or maintained by the system? Indicate all that apply.

☒ Name
☒ Social Security Number (SSN)
☒ Date of Birth
☐ Place of Birth
☒ Driver's License
☐ Race/Ethnicity
☒ Passport Number
☐ Personal Bank Account Number
☒ Business Bank Account Number
☐ Gender
☐ Religion
☐ Security Clearance
☐ Personal Phone Number
☒ Business Phone Number
☐ Personal Email Address
☒ Business Email Address
☐ Personal Mailing Address
☒ Business Mailing Address
☐ Spouse Information
☐ ID Number
☒ Financial Information
☐ Group Affiliation
☐ Medical Information
☐ Mother's Maiden Name
☐ Marital Status
☐ Disability Information
☐ Biometrics
☐ Fax Number
☐ Health Plan Number
☐ Civil or Criminal History
☒ Alien Registration Number
☐ Photograph
☒ Credit Card Number
☐ Child or Dependent Information
☐ Other Names Used
☐ Law Enforcement
☐ Employment Information
☐ Truncated SSN
☐ Education Information
☐ Military Status/Service
☐ Legal Status
☐ Emergency Contact
☐ Internet Protocol (IP) Address
☐ Account Password
☐ Citizenship or Immigration Status
☐ Retirement Information

☒ Taxpayer Identification Number (TIN)
☐ Other: *Specify the PII collected*.

1.2 What are the sources of the PII in the system?

The PII is contained in information or documentation gathered during audits. It may be collected directly from the individual, from documents that were submitted to the agency for a separate business purpose, or from other source systems within DFC.

1.3 Why is the PII being collected, used, disseminated, or maintained?

During an audit, OIG will gather, analyze, and store documentation in support of the accomplishment of the audit. PII may or may not be present in the documentation that is uploaded to eCase. If PII is being collected, it shall be relevant and necessary for the purpose of the audit and will be used in accordance with the Generally Accepted Government Auditing Standards (GAGAS). Commonly known as the "Yellow Book" and disseminated by the U.S. Government Accountability Office, auditors around the world use the GAGAS to perform audits. These standards provide the foundation for government auditors to lead by example in the areas of independence, transparency, accountability, and quality through the audit process.

1.4 How is the PII collected?

The PII may be collected in several ways, such as through (1) personal interviews, (2) documentation request, (3) observation, or (4) e-file download. The DFC OIG would then upload relevant documents to eCase. The system will not interface with other systems, but the information gathered, stored, and documented in eCase may come from another source system within DFC.

1.5 How will the PII be checked for accuracy?

All workpapers and documentation collected in eCase will require a second level (supervisory) review as required by the GAGAS.

1.6 If the information is retrieved by a personal identifier, what System of Records Notice (SORN) applies to the information. If a SORN is not required, what specific legal authorities, arrangements, and agreements define the collection of PII?

A System of Records Notice (SORN) does not apply to eCase because the records are not retrieved by personal identifier; rather, they are indexed and retrieved by project number and, to a lesser extent, project title. The Inspector General Act of 1978, as amended (5 U.S.C. § 406) (IG Act), grants OIGs the administrative authority to, among other things, receive full access to all records and materials available to the agency; determine which audits, investigations, inspections, and reviews are necessary and issue appropriate reports; and issue subpoenas for non-federal records.

1.7 Privacy Impact Analysis: Related to Characterization of the PII

Privacy Risk: There is a risk that more PII will be collected than is relevant and necessary.

Mitigation: This risk is partially mitigated. The DFC OIG makes every effort to ensure that any PII that is uploaded to eCase is relevant and necessary to meet the purpose of the audit. DFC OIG employees will review all information collected from both primary (i.e., the individual) and secondary (i.e., documentation) sources to determine whether the information is pertinent to the underlying case. If DFC OIG employees find that PII is present but is not germane to the audit, then they will not upload it to eCase or may upload a redacted version of the document.

Privacy Risk: There is a risk that the PII collected will be inaccurate or incomplete.

Mitigation: This risk is partially mitigated. PII is verified for accuracy and completeness during the fact-finding process, when reasonable. However, because the objective of DFC OIG audits will mostly be to measure the effectiveness of DFC programs and operations as opposed to investigating employee wrongdoing, there may not be a need to verify PII in some cases as the goal of the audit does not involve making a determination on an individual (i.e., an individual would not be denied a benefit as a result of an audit). Nonetheless, whether documentation contains PII or not, the DFC OIG follows the GAGAS, which ensure that any evidence obtained is sufficient and appropriate to provide auditors with a reasonable basis for findings and conclusions that are valid, accurate, appropriate, and complete with respect to the audit objectives.

Section 2. Uses of the PII

The following questions are intended to clearly delineate the use of PII, and the accuracy of the data being used.

2.1 Describe how the PII in the system will be used in support of the program's business purpose.

The information is gathered by DFC OIG auditors to support the accomplishment of audit objectives and to document the planning and conduct of the audits in accordance with the GAGAS. For example, if the OIG is evaluating whether a particular contract for goods and services complies with the Federal Acquisition Regulation (FAR), the OIG would obtain the contract documents, which might contain PII, to evaluate compliance with the FAR. As another example, if the OIG is auditing DFC's charge card program, the OIG would obtain specific transactions for a card holder, which might have PII, to determine if the charges are properly supported and in compliance with agency policies. Additionally, if evidence is uncovered during an audit that may suggest employee or contractor malfeasance, then the PII and supporting evidence may be forwarded to the DFC OIG investigations team to examine outside of the scope of the audit.

2.2 What types of tools are used to analyze data and what type of data may be produced?

The software will utilize the standard Microsoft suite of products (e.g., Microsoft Excel and Word) and Adobe Acrobat. DFC OIG auditors will use these products to analyze and document information. The methods used to analyze information include the ability to link events, documents, and/or occurrences together in a logical format for the purpose of showing patterns that demonstrate the effectiveness or ineffectiveness of DFC's programs and operations. The results of this analysis will result in the production of an audit report that is presented in accordance with the GAGAS.

2.3 If the system uses commercial or publicly available data, explain why and how it is used.

The eCase system will not interface with commercial or publicly available data sources directly, but it may be used to store and document commercial or publicly available data that is gathered during an audit (e.g., from LexisNexis or open-source searches).

2.4 Privacy Impact Analysis: Related to Uses of the PII

Privacy Risk: There is a risk that PII will be used inappropriately.

Mitigation: This risk is partially mitigated. As the objective of DFC OIG audits is to measure the effectiveness of DFC programs and operations, any PII collected is likely to be incidental and will not constitute the focal point of the audit report. In fact, DFC's published audit reports do not contain names of individuals (although they may contain job titles) to preserve the privacy of individuals. Additionally, as an administrative matter, all DFC personnel are required to take annual privacy awareness training and sign the DFC Privacy Rules of Behavior to attest that they will handle PII appropriately.

Section 3. Retention of PII

The following questions are intended to outline how long PII will be retained after the initial collection.

3.1 Has the retention schedule been approved by the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

Yes, there is a NARA-approved records retention schedule under which DFC OIG audit records are retained. This records retention schedule is specific to the DFC OIG. The applicable item from the records retention schedule is titled "Audit, Inspection, and Evaluation Files."

3.2 For what reason is the PII retained?

PII is retained to fulfill the objective of the audit and to maintain documentation in accordance with GAGAS requirements. As described in the records retention schedule, these records consist of:

> Files produced during audits, inspections, evaluations, and other reviews that assist management in identifying, analyzing, and resolving office and Agency issues. These include final reports and correspondence, resolution files, and work papers. Audits can include internal audits of programs and operations as well as peer review audits of other OIGs.

3.3 How long is the PII retained?

Information gathered will be considered temporary records and retained for seven years (cutoff at the end of the calendar year) to comply with the GAGAS.

3.4 How is the PII disposed of at the end of the retention period?

At the end of the retention period, projects will be electronically deleted from eCase.

3.5 Privacy Impact Analysis: Related to Retention of PII

Privacy Risk: There is a risk that PII may be retained for a longer period than necessary.

Mitigation: This risk is partially mitigated. The DFC OIG has a NARA-approved records retention schedule under which their audit documentation is maintained. After seven years, the audit records will be electronically deleted from eCase to prevent PII from being retained in the system for a longer period than necessary. In addition, the DFC privacy program conducts intermittent privacy reviews of DFC systems to see that programs are properly disposing of PII at the end of their retention periods.

Section 4. Internal Sharing and Disclosure

The following questions are intended to define the scope of PII sharing within DFC.

4.1 With which internal organizations is PII shared? What PII is shared, and for what purpose?

The PII in the documentation that is uploaded to eCase will only be viewable by DFC OIG employees who have a need to know to perform their official duties. However, as required by the IG Act, the results of the analysis of information/documentation will be shared with various DFC components (without PII, except for job title) in the form of memorandums or official audit reports that would be shared via email as well as posted on the DFC OIG external website.

4.2 How is the PII transmitted or disclosed internally?

The PII in the documentation that is uploaded to eCase will not be transmitted to others who are not a part of the audit team or a peer review team. However, as required by the IG Act, the results of the analysis of information/documentation will be shared with various DFC components (without PII, except for job title) in the form of memorandums or official audit reports that would be transmitted via e-mail as well as posted on the DFC OIG external website.

4.3 Privacy Impact Analysis: Related to Internal Sharing and Disclosure

Privacy Risk: There is a risk that PII may be shared internally with individuals who do not have a need to know.

Mitigation: This risk is partially mitigated. Access to information in eCase is limited to DFC OIG employees who have been approved by their supervisor to have access to perform their official duties. No contractors have access to eCase, and accounts are reviewed periodically to ensure that proper roles are assigned to each account to limit the unnecessary sharing of PII. Furthermore, the DFC OIG ensures that the results of their analysis of information/documentation are bereft of PII (except for maybe job title) to preserve individual privacy when producing final audit reports.

Section 5. External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for PII sharing external to DFC, which includes federal, state, and local governments, and the private sector.

5.1 With which external organizations is PII shared? What information is shared, and for what purpose?

The PII in the documentation uploaded to eCase will not be shared with or disclosed to others outside of DFC without a valid need to know (e.g., a peer review team or official audit work/collaboration with other OIGs). As required by the IG Act, the DFC OIG's official audit reports will be posted to the DFC OIG external website and shared with the public. The audit reports may contain job titles but will not contain other types of PII.

Note: In ancillary documents to the audit report, the names and job titles of individuals who are key stakeholders to the audit report will be made publicly available. For example, names and job titles will be contained in the address line and signature/cc line of the memorandum that introduces the audit report. This includes who the report was prepared for (i.e., name and job title of the Vice President(s) of the DFC office(s) being audited), who sponsored the audit report (i.e., name and job title of the DFC Inspector General), and who was provided a carbon copy of the report (i.e., names and/or job titles of DFC officials). In addition, DFC may provide a response letter to the audit report, which contains the name and job title of the DFC official providing the response (i.e., usually the Vice President of the DFC office being audited) and to whom the letter is addressed (i.e., name and job title of the DFC Inspector General).

5.2 Is the sharing of PII outside the agency compatible with the original purpose for the collection?

As noted above, the PII in the documentation uploaded to eCase will not be shared with or disclosed to others outside of DFC without a valid need to know. Any sharing of PII outside the agency will be compatible with the purpose for the collection in the sense that each OIG is subject to peer reviews from external OIGs to ensure that their quality control system is adequate and to provide reasonable assurances that they follow applicable government auditing standards, policies, and procedures.

5.3 Is the external sharing covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form outside of DFC.

As information stored in eCase is not retrieved by personal identifier, a SORN does not apply to the system. The external sharing of audit documentation with other OIGs is permitted under the GAGAS (2018), which state:

> The audit organization should establish policies and procedures that require retention of engagement documentation for a period of time sufficient to permit those performing monitoring procedures and peer reviews of the organization to evaluate its compliance with its system of quality control or for a longer period if required by law or regulation (p. 92).

5.4 How is the PII shared outside the agency and what security measures safeguard its transmission?

For onsite reviews, the DFC OIG will work with the DFC Office of Information Technology to securely grant access to PII that has been uploaded to eCase. This may involve downloading the files from eCase and putting them into a dedicated file share on the DFC network for only the external OIG to review. If the documentation will be transmitted outside the DFC network, the DFC OIG may use DFC's Box.com solution to securely share the information. Alternatively, the DFC OIG may also share the information by encrypting it in Microsoft Outlook and sending it via email to an external OIG email address. Box and encrypting in Outlook are the two approved DFC methods for sharing information outside the DFC network and ensure that the information is protected in transit.

5.5 Privacy Impact Analysis: Related to External Sharing and Disclosure

Privacy Risk: There is a risk that PII may be shared externally with individuals who do not have a need to know.

Mitigation: This risk is partially mitigated. No external entities have access to DFC's instance of eCase. Secure methods of sharing will be utilized to ensure that any PII transmitted to external parties will be protected in transit. By using DFC's secure Box.com solution to transmit data, external parties will be required to sign up for their own Box account and must be added as "collaborators" by the sharing party. Box contains a full audit log of user activities taken on files stored in the system. As a result, DFC would be able to see who accessed a file in Box and track each subsequent action in which they took on the file while it is stored in Box (e.g., view, edit, download, etc.).

Information may also be shared via encrypted email in Microsoft Outlook. Sensitive PII must be encrypted in Microsoft Outlook and cannot be encrypted through other methods. This ensures that DFC's Data Loss Prevention (DLP) tool is capable of decrypting any information transmitted via email. The DLP would block attachments encrypted outside of Outlook (such as through Adobe Acrobat, Microsoft Word, WinZip, etc.) as well as unencrypted emails containing sensitive PII. This policy guards against the illicit transfer of sensitive agency data outside the DFC network.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the PII?

If collecting PII from a primary source through a personal interview, verbal notice is provided to the individual. In addition, an engagement letter is issued at the beginning of each audit to provide formal notice to the agency as to why an audit is taking place. For PII collected from a secondary source (i.e., documentation), the PII would have first been collected by DFC for its specific business purpose, and a privacy notice should have been provided, ideally at the point of collection. The IG Act allows each Inspector General "to have timely access to all records, reports, audits, reviews, documents, papers, recommendations, or other materials available to the applicable establishment which relate to the programs and operations with respect to which that Inspector General has

responsibilities under [the] Act." Therefore, while the PII may have initially been collected for a separate business reason, the IG Act allows OIGs to have access to these records to conduct audits and other OIG functions. The IG Act is described on the DFC OIG external website as well as in this PIA.

6.2 Do individuals have the opportunity and right to decline to provide PII? If so, is a penalty or denial of service attached?

Employees may assert their Fifth Amendment right to refuse to provide information on the grounds that the information might be used against them in a criminal proceeding. An OIG investigation can result in a criminal proceeding only if the U.S. Department of Justice (DOJ) accepts it for criminal prosecution. For a case that has been declined for potential criminal prosecution by DOJ or did not require referral to DOJ, the employee may receive a written advisement to such effect, and the employee must then fully cooperate with the OIG. Therefore, any DFC official who initially refuses to be interviewed for an audit would eventually be compelled to provide their information as a condition of their employment with the U.S. federal government. However, it should be noted that the objective of a DFC OIG audit is usually not to collect PII but rather to measure the effectiveness of DFC programs and operations; therefore, any collection of PII through a personal interview would likely be limited to PII used to conduct business transactions. Additionally, the DFC OIG reviews every document before uploading it to eCase and makes every effort not to upload documents where PII is determined not to be relevant and necessary to the audit.

6.3 Do individuals have the right to consent to particular uses of the PII? If so, how does the individual exercise the right?

There is no option for an individual to consent to particular uses of the PII due to the already limited scope in which it is used by the DFC OIG. PII collected would only be used to fulfill the objectives of the audit and to comply with GAGAS requirements. In addition, if evidence is uncovered that suggests employee or contractor malfeasance, then the PII and supporting evidence may be forwarded to the DFC OIG investigations team to examine.

6.4 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that notice has not been given to individuals on the use of collected PII.

Mitigation: This risk is partially mitigated. The DFC OIG external website and this PIA provide notice to individuals on how their information may be used as part of an audit. In addition, for PII that is collected directly from the source through a personal interview, a verbal notice will be given to the individual as to why their PII is being collected. Furthermore, before an audit kicks off, the DFC OIG provides an engagement letter to the agency outlining the purpose for the audit and its objectives.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the PII collected about him or her.

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

Individuals may request access to their information by following DFC's Privacy Act request process (Note: Although eCase does not constitute a Privacy Act system of records, the same procedures may be used to request access to personal information from a non-Privacy Act system as a Privacy Act system).

To make a Privacy Act request, a requester may submit a written request to the Director of Human Resources Management, either by mail or delivery, to U.S. International Development Finance Corporation, 1100 New York Ave NW, Washington, DC 20527 or electronic mail to privacy@dfc.gov. The envelope or subject line should read "Privacy Act Request" to ensure proper routing. Individuals requesting access must comply with DFC's Privacy Act regulations regarding what information to include in the request and provide the proper verification of identity (22 CFR Part 707). To protect PII in transit, individuals should encrypt any sensitive PII sent to the agency over email or request to submit it to through DFC's secure Box.com portal.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals may request correction of inaccurate or erroneous information about themselves by making a Privacy Act amendment request (Note: Although eCase does not constitute a Privacy Act system of records, the same procedures may be used to request correction of personal information from a non-Privacy Act system as a Privacy Act system).

To make a Privacy Act amendment request, a requester may submit a written request to the Director of Human Resources Management, either by mail or delivery, to U.S. International Development Finance Corporation, 1100 New York Ave NW, Washington, DC 20527 or electronic mail to privacy@dfc.gov. The envelope or subject line should read "Privacy Act Request" to ensure proper routing. Individuals requesting amendment must comply with DFC's Privacy Act regulations regarding what information to include in the amendment request and provide the proper verification of identity (22 CFR Part 707). To protect PII in transit, individuals should encrypt any sensitive PII sent to the agency over email or request to submit it to through DFC's secure Box.com portal.

7.3 How are individuals notified of the procedures for correcting their information?

This PIA provides notice to individuals on how to correct their information. Additional notice is provided by DFC's Privacy Act regulations, which can be found at https://www.dfc.gov/privacy.

7.4 If no formal redress is provided, what alternatives are available to the individual?

N/A; formal redress is provided through the Privacy Act request process.

7.5 Privacy Impact Analysis: Related to Access, Redress, and Correction

Privacy Risk: There is a risk that individuals will not be able to access or correct any information maintained on them by DFC.

Mitigation: This risk is partially mitigated. For any information that DFC collects about individuals that is maintained in a Privacy Act system of records (which may apply to information that the DFC OIG gathers from secondary sources), the agency has published its Privacy Act regulations on the DFC website. For information not

maintained in a system of records, as is the case with eCase, individuals can still seek access to or correction of their information by submitting a Privacy Act request to DFC.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☐ Security Guards
☐ Key Guards
☐ Locked File Cabinets
☐ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☐ Identification Badges
☐ Safes
☐ Combination Locks
☐ Locked Offices
☒ Other. No physical controls apply; system is a cloud application service.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☐ Intrusion Detection System (IDS)
☐ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. Okta Multi-Factor Authentication Enforced

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☐ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☐ Encryption of Backups Containing Sensitive Data

☒ Mandatory Security, Privacy, and Records Management Training
☐ Other. *Describe*

8.2 Will DFC contractors have access to the system? If so, how frequently are contracts reviewed and by whom?

No, DFC contractors will not have access to the DFC OIG's instance of eCase.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All DFC personnel must take annual privacy awareness training and information security awareness training, which instruct users on the need to protect agency data and provide best practices for handling PII.

8.4 Has Assessment and Authorization (A&A) been completed for the system?

Yes, Assessment and Authorization (A&A) was completed on eCase in March 2023 by the DFC Chief Information Security Officer team. In addition, A&A was completed for eCase by an independent assessor as part of the FedRAMP authorization process. The FedRAMP authorization to operate (ATO) for eCase was first authorized on February 21, 2014, with subsequent annual assessments completed, which allows eCase to maintain its FedRAMP ATO.

8.5 Privacy Impact Analysis: Related to Technical Access and Security

Privacy Risk: There is a risk that PII will not be properly secured.

Mitigation: This risk is partially mitigated. All DFC personnel must take annual privacy awareness and information security awareness training, which educate users on properly securing PII. In addition, eCase is a role-based information technology system in which users are assigned access based on their specific job responsibilities and in accordance with the principle of least privilege. Only authorized users are permitted to view information in eCase, and the DFC OIG eCase administrator conducts periodic reviews of user accounts to ensure proper access privileges are in place. Furthermore, logging into eCase requires the use of multi-factor authentication to provide an additional layer of security before a user can gain access to the system.