U.S. Small Business Administration
409 3rd Street, S.W.
Washington, DC 20416

Office of Inspector General
eCase Audit Management System

Privacy Impact Assessment
February 7, 2023

System Owner
Thomas Rosado
Audit Operations Manager
Office of Inspector General
Thomas.Rosado@sba.gov

Reviewer
LaWanda Burnette
Chief Privacy Officer
Office of the Chief Information Officer
LaWanda.Burnette@sba.gov

Approved by the Senior Agency Official for Privacy
Stephen W. Kucharski
Acting Chief Information Officer
Office of the Chief Information Officer
PrivacyOfficer@sba.gov

I. System Description/General Information

The Office of the Inspector General's (OIG) mission is to provide independent, objective oversight to improve the integrity, accountability, and performance of the SBA and its programs for the benefit of taxpayers. The auditing division supports this mission by conducting audits and evaluations of SBA programs. The eCase is the audit management information system for the OIG. The purchase of this system is authorized by Section 2 subsection (1) of the Inspector General Act of 1978, (as amended). Public Las 95-452; 5 U.S.C. App.] [As amended through P.L. 113-126, Enacted July 7, 2014].

The eCase Audit Management System (eCase) is a Commercial Off-the-Shelf software package that enables SBA Office of the Inspector General to conduct audits, follow-up on audit recommendations, and track auditor professional training. The system allows auditors to plan, schedule, conduct, track and report on audit and inspection projects. As such, eCase system is organized into discrete projects representing individual audits or inspections. Each project serves as a repository for audit documentation and evidence obtained during the audit, analysis artifacts, created by the auditors during audit performance, and documentation supervisory review o the work performed. The eCase also contains modules to tract the outcomes of OIG audit recommendations and to document the professional training obtained by auditors.

This system may collect and contain information about individuals. Although the system is not designed to be a Personally identifiable information system with designated PII fields or organized with search capabilities based on PII elements; some PII information may be collected on a case by case basis depending on the objectives of the engagement and the audit evidence collected, SBA OIG may audit SBA Programs, SBA service delivery partners, and SBA Program Participants in which eCase may store document containing information about SBA Program Participants – including PII. Some examples of PII documents that could be obtained during the course of an audit are loan applications, contracting program applications, extracts from SBA information systems such as the loan accounting system that contains borrower name, address, and social security numbers, or information voluntarily and directly provided by program participants to the OIG. The collection of any replicated documents has a PIA from their originating source system.

II. System Data

The categories of individuals covered in the system are SBA Program participants which also includes small businesses. Information on program participants may be provided by SBA, SBA service delivery partners, or the program participants themselves. Rarely, information may be provided by external government agencies. There are no standard forms or collection instruments used, the data collected is dependent on the objectives of the audit or inspection project. OIG may also obtain information from Dunn and Bradstreet or Unique Entity Identifier. The information obtained from these sources is generally business information and not considered PII.

Data collected from sources other than SBA records are verified for accuracy through extensive controls to ensure the sufficiency and appropriateness for the evidence obtained – including control to ensure the accuracy of the data obtained. In general, the process entails assessing risk and the significance of the data to the objectives, and tracing data – on a sample basis, to source documents, or vouching source documents to the summarized data. Discrepancies are researched to arrive at an overall conclusion whether the data can e relied on.

Data is checked for completeness as specified by Government Accounting Office in "Assessing Data Reliability GAO-20-283G, where two general areas of data testing may be conducted: 1) test of whether expected data were received; and 2) test of whether there may be data reliability issues. Data used in the eCase system is current.

III. Data Attributes

The use of the data is both relevant and necessary for the purpose of the eCase. The eCase is an audit management system used to collect, manage, analyze, and store information directly related to fulfillment of the OIG mission. The system will not derive any new data or create previously unavailable data about an individual. No new data will be placed in the individual's record and the system can't make determinations about employees or members of the public that would not be possible without new data.

Data in the eCase is retrieved using the audit project number. No individual identifiers are used to retrieve data from eCase. The audit report does not contain PII. No reports are produced on individuals. OIG produces reports related to the economy and efficiency of SBA programs – including fraud, waste, and abuse. These reports are used by SBA management to improve the performance of its programs, by Congress to inform their decision making and by the American public to provide transparency into their government's processes. Access to OIG reports are normally available to the public. OIG does not publish individual PII information in its audit reports and all reports are reviewed by OIG Counsel to determine whether sensitive business information should be redacted.

OIG audit do not normally request program participants to provide information for audit projects. Program participants may voluntarily contact OIG auditors to provide information and implied consent.

IV. Maintenance and Administrative Controls

The eCase system will be maintained on one site and is not considered a Privacy Act systems of records. The retention periods of data in this system are in compliance with SBA policy and the National Archives and Records Administration's General Schedule. The procedures for disposition of the records are applicable to the current Standards Operating Procedures of Records Management. Additional procedures for disposing data are executed in accordance with National Institute of Standards and Technology Special Publication 800-88, as amended.
The system does not use any technologies in ways that SBA has not previously employed, for example, no monitoring software, caller -identification, etc. This system does not provide the capability to identify, locate, or monitor individuals in real time. designated for disposal.

V. Data Access

Designated OIG staff, system administrators, database administrators, IT security, contractor working on behalf of OIG SBA, and end users will have access to the data in the system based upon their specific role. Access to the eCase system is granted to specific authorized users with a need to know by the OIG management. Access to the system data is restricted based upon role based permissions. Contractors are involved in the design, development, and maintenance of eCase. Privacy Act clauses were included in their contract. Other systems do not have access to the system.

Responsibility for protecting the privacy rights of the public and employees consists of the information system owner, Senior Agency Official for Privacy/Chief Information Officer, Chief Information Security Officer, and the Chief Privacy Officer as designated by the SAOP.

SBA OIG undergoes Peer Review by an external federal OIG once every three years. This entails sharing the project files for approximately 3 projects conducted during the three-year period. The detailed Memorandum of Understanding signed by the externa federal OIG encompasses the acceptable use of the information, including Privacy Act information and the prohibition of its disclosure. The external federal OIG will use the shared project information to determine whether SBA OIG complied with applicable Government Auditing Standards or Quality Standards for Inspections and Evaluations during the covered period. A Memorandum of Understanding covering the proper use of the shared data is signed prior to sharing of data. Peer review teams are members of the Federal OIG Community and must comply with all relevant statutes, rules and procedures related to sensitive data. The Peer review process is governed by the Council of Inspectors General for Integrity and Efficiency.

OIG staff employees and contractors are adjudicated during the hiring process. Access is limited and restricted by Role Based access. Agency staff are required to take SBA annual Cyber Security Awareness training which includes the Privacy module.

VI. Privacy Impact Analysis

There are risks related to disclosure of individuals' privacy. Risks to the type of data, ensure information used as intended, safeguard unauthorized monitoring of privacy data, and protect information shared internal and external. The sensitivity of the eCase data elements is mitigated using access controls, auditing, monitoring, authentication, encryption, and boundary protection. Disclosure of data may adversely affect individuals but not focused on any vulnerable populations.

Privacy risks are mitigated through access control, auditing, monitoring, encryption, authentication, and boundary protection. Mitigation also includes ensuring collection is comparable to its' collection; ensuring collection follows statutory authority to collect, encryption of data in transit and at rest; incremental and full backups, data integrity checks, and data redundancy.

Regarding the relevance of data, data are kept current and remain relevant over time.

Lastly, mitigation is also through signing Rules of Behavior, education via annual Cybersecurity Awareness and Privacy Training.