Treasury Office of Inspector General (OIG) Privacy and Civil Liberties Impact Assessment (PCLIA)

Name of System: OIG General Support System (OGSS)

Date of Submission:

Contact: Nancy Osborn, Acting Assistant Inspector General for Management/CIO, 202-927-5835, OsbornN@oig.treas.gov

Kester Buckmire, Director IT & Cybersecurity
202-927-6524, BuckmireK@oig.treas.gov

1. What is the purpose of the system?

The Office of Inspector General (OIG) General Support System (OGSS) is the OIG's principal infrastructure that supports the offices of Audit, Management, Council, and Investigations.

The system contains data extracts obtained from various electronic systems maintained by federal agencies and other authorized entities. This information supports OIG's audit, investigative, and oversight activities by enabling the identification, detection, and prevention of fraud, waste, abuse, and misconduct affecting the programs and operations of the Department of the Treasury and related entities. The data also supports efforts to promote economy, efficiency, effectiveness, and integrity in the administration of applicable laws, while deterring and detecting wrongdoing by Treasury and OIG employees, contractors, and other parties subject to OIG oversight.

OGSS hosts two major applications:

i) Office of Investigations, Investigations Management Information System - This system maintains personally identifiable information about individuals, including name, home address, home telephone and fax numbers, personal email address, and other relevant information necessary for processing and responding to investigations and allegations related to the Department of the Treasury.

ii) Office of Audit, TeamMate – This system is used for storing audit-related documents that may contain information such as an individual's name, employee identification number, gender, business address, business telephone number, group identification, educational background, résumé, IP address, username, password, geolocation, password hashes, and records of files accessed.

2. What legal authority authorizes the purchase or development of this system?

The nature and scope of OIG's oversight and investigative responsibilities are established in the Inspector General Act of 1978, as amended, 5 U.S.C. Appendix 3; 5 U.S.C. 301; 31 U.S.C. 321; and Treasury Order 114-01. To enable the OIG to effectively perform its oversight and investigative functions, the Inspector General Act authorizes the OIG to access "all records, reports, audits, reviews, documents, papers, recommendations, or other material" maintained by the Department of the Treasury.

3. Under which Privacy Act SORN does the system operate?

Treasury/DO .190 - Office of Inspector General Investigations Management Information System - 81 FR 78298

4. **What categories of individuals are covered by the data in the system?**
    - Treasury Employees
    - Contractors, Interns, grantees working on behalf of Treasury
    - Members of the public
5. **What are the sources of information in the system?**

Data extracts from electronic systems maintained by governmental agencies and other entities.

6. **How is the data in the system verified for accuracy, timeliness, and reliability?**

See attached Investigations Management Information System and TeamMate PCLIAs.

7. **Is the use of the data both relevant and necessary to the purpose for which the system is designed?**

See attached Investigations Management Information System and TeamMate PCLIAs.

8. **What are the retention periods and procedures for disposition of the data in the system?**

See attached Investigations Management Information System and TeamMate PCLIAs.

9. **Will this system provide the capability to identify, locate, and monitor individuals?**

See attached Investigations Management Information System and TeamMate PCLIAs.

10. **What controls will be used to prevent unauthorized monitoring?**

OIG implements a comprehensive set of technical, administrative, and operational controls to protect the confidentiality, integrity, and availability of information maintained within the OGSS. All requests for access to data must be properly authorized and verified before access is granted. OIG employees and contractors are required to complete annual cybersecurity, privacy, and ethics training to maintain awareness of their security responsibilities. System activity is continuously monitored to detect and respond to unauthorized or inappropriate activity. Violations of security policies or procedures by users or administrators may result in disciplinary action, up to and including termination of employment. As trusted custodians of sensitive information, OGSS users and administrators serve as the first line of defense in supporting the OIG's cybersecurity and incident response efforts.

11. **Who will have access to the data in the system and what controls are in place to prevent misuse?**

OGSS is an internal system that is not accessible to the public and contains sensitive information requiring protection in accordance with applicable federal laws, regulations, and OIG policies. All personnel granted access are responsible for safeguarding information under their control. The Privacy Officer, System Owners, managers, and authorized users share responsibility for ensuring the proper use and protection of OGSS data. Access is granted based on the principles of least privilege and need-to-know, with users and administrators limited to only the access required to perform their official duties. Additional application-level controls further restrict access to particularly sensitive data.

The Following Officials Have Approved this Document

1. **Chief Information Officer**

Name: Nancy Osborn **Title:** Acting Assistant Inspector General for Management/CIO

Signature: Nancy N. Osborn Digitally signed by Nancy N. Osborn Date: 2026.07.17 08:40:54 -05'00'

2. **Information Systems Owner**

Name: Kester Buckmire **Title:** Director, IT & Cybersecurity

Signature: Kester G. Buckmire Digitally signed by Kester G. Buckmire Date: 2026.07.16 14:35:52 -04'00'

3. **Information Systems Security Manager**

Name: Said Nurhussein **Title:** Information Systems Security Manager

Signature: Said Nurhussein Digitally signed by Said Nurhussein Date: 2026.07.16 13:45:46 -04'00'

4. **Privacy Act Officer**

Name: Amy Altemus **Title:** Counsel to the Inspector General

Signature: Amy J. Altemus Digitally signed by Amy J. Altemus Date: 2026.07.17 13:17:11 -04'00'

Attachment I - Name of System, Project or Program: Office of Investigations, Investigations Management Information System
Attachment II – Name of System, Project or Program: Office of Audit, TeamMate