



UNITED STATES
FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT (PIA) FOR THE OFFICE OF INSPECTOR GENERAL (OIG) BOUNDARY


MAY 2023

OFFICE OF GENERAL COUNSEL

Washington DC, 20554

Next Review Cycle: May 2024

Record of Approval

Document Approval	
Drafter Name: Shannon Kendall	Bureau/Office: Office of Managing Director (OMD) Office: Information Resiliency (IR)
SAOP Approval	
Printed Name: Elliot S. Tarloff	Senior Agency Official for Privacy
<div></div> Signature & Date	

Record of Approval

Date	Description	Author
1/2023	Validation of information – System Owner	Johnny Drake
1/2023	Validation of completeness – IT Compliance Lead	Thad Massagee

Revision History

Date	Description	Name
10/6/2020	Original Document Created	Privacy Team – Bahareh Moradi
1/10/2023	Template revision for annual verification	ISSO – Shannon Kendall
3/14/2023	Revisions to Sections 1.2, 1.2B-C, 1.3A-C, 1.4A-B, and 1.6A	Privacy Advisor – Katherine Morehead Senior Agency Official for Privacy (SAOP) – Elliot S. Tarloff
05/03/2020	Clerical edits and revisions to Sections 1.2, 1.3A-D, 1.4A, and 1.5C	SAOP

Office of Inspector General System Boundary

1.1. Introduction

Section 208 of the E-Government Act of 2002¹ requires agencies to conduct a **Privacy Impact Assessment (PIA)** whenever they procure or develop an information technology system that will collect, maintain, or disseminate information about individual people. The PIA must document how the system will use information it collects about individuals and, unless it contains classified or sensitive information, it must be made available to the public. The PIA was intended to be a tool for agencies to protect personal information throughout a technology system's life cycle. The Office of Management and Budget (OMB) has commented: *"In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks."*²

The FCC is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below explore important privacy issues identified in the Act and in later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). A longer discussion of the FCC's PIA policies can be found in Chapter 9 of the FCC's Privacy Act Manual (FCC Inst. 1113.1).

System owners, in collaboration with the Information System Security Officers (ISSOs) should complete the **Initial Privacy Assessment (IPA)** prior to filling out the PIA. The FCC Senior Agency Official for Privacy (SAOP) uses the IPA to determine whether a system will collect the kind of information that would make it subject to the requirements of Section 208, including a PIA. A PIA should not be completed until an IPA is completed and the SAOP makes a determination.

If you have any questions, please contact the Privacy Team at privacy@fcc.gov.

¹ 44 U.S.C. § 3501 note.

² OMB Memorandum No. M-03-22 (Sep. 26, 2003), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf.

1.2. Authority To Operate (ATO) Boundary Overview

For each IT system that resides within the ATO Boundary, please use the table below to provide the system name, a brief description of the what the system does, whether it contains Personally Identifiable Information (PII) and a brief description of the PII (if applicable), the applicable System of Records Notice, the legal authorities to collect and maintain the PII, and whether the PII is shared with other systems (internal or external).

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Case Management System (CMS)
NAME OF BUREAU Office of Inspector General
DOES THE SYSTEM CONTAIN PII? Yes. All forms of PII that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual is retrievable and retrieved through various measures of identification.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) CMS contains PII related to formal OIG case files. Because of its law enforcement purpose, CMS may contain a broad range of PII elements including medical, biometric, financial, legal, employment, photographic, educational, and contact information about FCC employees, contractors, and others related to investigations.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? FCC/OIG-3 Investigative Files 76 Fed. Reg. 53454 (Aug. 26, 2011)
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The information in this system is collected, maintained, and disseminated pursuant to the Inspector General Act of 1978, as amended; the Communications Act of 1934, as amended; and other rules and regulations the FCC enforces.
DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (C) OF THE PRIVACY ACT? Yes. The Privacy Team keeps an accurate accounting of disclosures of information.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Concordance
NAME OF BUREAU Office of Inspector General
DOES THE SYSTEM CONTAIN PII? Yes. All forms of PII that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual is retrievable and retrieved through various measures of identification.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Due to its law enforcement purpose, Concordance contains a broad range of PII that is related to OIG investigations and varies in nature, including medical, biometric, financial, legal, employment, photographic, educational, and contact information about FCC employees, contractors, and others related to investigations. The system may also contain information collected through discovery and stored for case management and legal research functions.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? FCC/OIG-3 Investigative Files 76 Fed. Reg. 53454 (Aug. 26, 2011)
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The information in this system is collected, maintained, and disseminated pursuant to the Inspector General Act of 1978, as amended; the Communications Act of 1934, as amended; and other rules and regulations the FCC enforces.
DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT? Yes. The Privacy Team keeps an accurate accounting of disclosures of information.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes. The system may contain information collected through discovery and stored for case management and legal research functions. Portions of pertinent information in Concordance supporting ongoing investigations may be migrated to CMS, which could contain PII related to formal OIG case files.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM TeamMate
NAME OF BUREAU Office of Inspector General
DOES THE SYSTEM CONTAIN PII? Yes. All forms of PII that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual is retrievable and retrieved through various measures of identification.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) TeamMate may contain contact information to support Audit, Evaluation, Inspection, and Review reports. While the PII is redacted from final publicly releasable reports, the PII can potentially be retained in the Teammate database and nonpublic releasable reports.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? FCC/OIG-3 Investigative Files 76 Fed. Reg. 53454 (Aug. 26, 2011)
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The information in this system is collected, maintained, and disseminated pursuant to the Inspector General Act of 1978, as amended; the Communications Act of 1934, as amended; and other rules and regulations the FCC enforces.
DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT? Yes. The Privacy Team keeps an accurate accounting of disclosures of information.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM AWS GovCloud West
NAME OF BUREAU Office of Inspector General
DOES THE SYSTEM CONTAIN PII? Yes. All forms of PII that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual is retrievable and retrieved through various measures of identification.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) The database enclave contains PII that is related to the full spectrum of OIG investigations. Because of its law enforcement purpose, the database enclave may contain a broad range of PII elements.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? FCC/OIG-3 Investigative Files 76 Fed. Reg. 53454 (Aug. 26, 2011)
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The information in this system is collected, maintained, and disseminated pursuant to the Inspector General Act of 1978, as amended; the Communications Act of 1934, as amended; and other rules and regulations the FCC enforces.
DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT? Yes. The Privacy Team keeps an accurate accounting of disclosures of information.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes. The database system may contain information collected through discovery and used to support data analysis. Information culled from the data analysis process may migrate to Concordance eDiscovery application and/or become part of investigative reports tracked in CMS.

A. Is this a new ATO Boundary or an existing ATO Boundary?

- ☐ New Boundary
☒ Existing Boundary

B. If the ATO Boundary is/will consist of cloud-based computing system(s), please check the box that best describes the service the FCC receives/will receive from the cloud computing provider:

- ☐ The FCC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS) [list applicable system(s)]
- ☐ The FCC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service or PaaS) [list applicable system(s)]
- ☒ The FCC has deployed its own application/s on the cloud network and controls how these application/s are configured and operate (Infrastructure as a Service or IaaS):

AWS GovCloud West is hosted on the cloud. CMS, Concordance, and TeamMate are not hosted in the Cloud. These OIG systems are hosted in FCC.Net/Enterprise Support Infrastructure.

C. If the IT systems in the ATO Boundary are in the cloud, are they FedRAMP certified?

- ☐ Yes, all the IT systems are FedRAMP certified
- ☒ No, none, or only some, of the IT systems are FedRAMP certified
- ☐ Not applicable, ATO boundary is not Cloud based.

1.3 Collection of Data

A. Please explain why it is necessary to collect PII to carry out the purpose of each of the system(s) that maintain PII within this Boundary.

All of the OIG System applications (collectively, the OIG System) support the OIG's mission to detect and prevent fraud, waste, and abuse in FCC programs and operations. The OIG's investigative and audit functions require the collection of PII from and about witnesses, individuals involved in FCC programs, and others. The Inspector General reports the results of investigations, audits, and reviews semi-annually to the FCC Chair and to the United States Congress. These reports, in turn, inform the Chair, Commissioners, and Congress of any potential programmatic or operational deficiency at the FCC. The applications in the OIG system also streamline and simplify case management, litigation support, and auditing by providing collaborative environments to analyze information.

- B. For each system within this Boundary, will this PII be collected from individuals themselves, or from third parties? If collected from individuals themselves, link to the Privacy Act Statement³ for each system that is included with the online or paper form the system(s) use(s) to collect the PII.**

FCC OIG staff and contractors upload data that has been created or obtained in connection with the OIG's law enforcement and auditing activities. In the course of OIG investigations, information may be collected from law enforcement sources or directly from individuals or third parties and uploaded to the OIG System. The OIG System does not collect PII directly from the public; however, information provided by and pertaining to members of the public may be stored in the OIG System. For example, members of public may report suspicion of waste, fraud, or abuse to the OIG by Phone, FAX, Email or direct mail. An OIG investigative analyst reviews each submission for validity. Valid submissions, which may be made anonymously, in confidence, or without restriction, are passed to the appropriate section for further investigation. Information sharing with other law enforcement entities does not occur via OIG systems.

- C. What steps is the FCC taking to limit the collection of PII to only that which is necessary?**

The information collected is that which is required to conduct IG investigations and audits, and to refer any potential violations that are revealed throughout the course of the investigation. The OIG does not request information that is beyond the scope of requirements for the investigation, or beyond the issues revealed in the investigation.

- D. What steps will the FCC take to make sure this PII is accurate, complete, and up to date?**

All collected information is subject to evaluation and scrutiny by OIG investigative staff and verified against information collected from other records sources. There are also built in audit logs to monitor disclosures and determine who had access during this time. These logs are checked regularly to ensure that the system is accessed appropriately.

⁴ A Privacy Act Statement must inform individuals about (1) the authority to solicit information, (2) the principal purpose(s) for collecting the information, (3) the routine uses for disclosing the information, and (4) whether providing the information is mandatory or voluntary.

1.4 Use of the Data

- A. Please explain the data flow, including whether the PII will be ingested from, or shared with, another system. Are internal connections reflected in the Cyber Security Asset Management tool (CSAM)? Are Information Sharing Agreements (ISAs) in CSAM for external connections?**

Personally Identifiable Information (PII) is not ingested from, or shared with, another system through a system connection, and thus there are no internal connections to document within the Cyber Security Asset Management (CSAM) tool or in Information Sharing Agreements. If PII must be entered into an OIG system that data entry must be performed manually.

- B. Will the information be shared with third parties as part of the operations of the information system (e.g., through an application programming interface or “API”)?**

Extracts of the data may be shared with other law enforcement organizations to support ongoing investigations through a manual, not automatic, process.

- C. How long will the PII be retained and how will it be disposed of?**

The PII is retained as long as the investigations and audits are active. Some PII may be retained as part of the final report. The OIG follows the record retention policies outlined by National Archives and Records Administration (NARA) schedule.

1.5 Data Security and Privacy

- A. What are the system’s ratings for confidentiality, integrity, and availability?**

Confidentiality	<input type="checkbox"/> High	<input checked="" type="checkbox"/> Moderate	<input type="checkbox"/> Low
Integrity	<input type="checkbox"/> High	<input checked="" type="checkbox"/> Moderate	<input type="checkbox"/> Low
Availability	<input type="checkbox"/> High	<input checked="" type="checkbox"/> Moderate	<input type="checkbox"/> Low

- B. Discuss the physical, administrative, and technical controls in place to protect the data in the system.**

The FCC protects its information resources with a dynamic set of security measures. Some of these measures (e.g., network firewalls, physical security) protect the entire FCC enterprise, while other measures (e.g., user access restrictions, encryption) are applied to specific information systems. Following the risk-based policy established in the Federal Information Modernization Act (FISMA), the FCC applies more security measures (also known as security “controls”) to information systems that present higher operational risks. Consistent with this policy, the FCC applies specific security controls to systems that collect and process PII. A comprehensive list of the security and privacy

controls the FCC may apply to its information systems can be found in National Institute of Standards and Technology (NIST) Special Publication No. 800-53, Revision 5 [[NIST](#)].

C. Does the system inherit privacy controls from an external provider? If an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or similar document is in place, please summarize the privacy applicable portions of the document.

The OIG inherits certain controls from the FedRAMP-authorized AWS environment on which they are maintained (including encryption of data at rest and in transit). But the AWS FedRAMP package has not been updated to reflect the NIST SP 800-53 rev 5 families, and therefore PT controls are not specifically identified.

1.6 Access to the Information

A. Which FCC employees and contractors will have access to the PII in this information system?

Access to the systems within the OIG Boundary is restricted to authorized FCC system owners and end users. All system owners and end users must adhere to the FCC Rules of Behavior and ensure that access to any PII stored in the OIG System is appropriately limited. Access to the information stored within the OIG System is dependent on the particular business purpose and the access permissions granted to a specific user. For example, system administrators may have access to system data and system audit logs in order to manage access roles, monitor system usage, perform system audits, and complete other necessary job functions.

Authorized FCC contractors have access to information in the OIG Boundary when necessary. Some authorized FCC contractors have access to the applications simply as users, and one or more authorized FCC contractors have access to certain administrative functions. All FCC contractors are required to complete security and privacy training, and complete annual security and privacy training to maintain network access and access to those systems.

Contractors who access the OIG System are subject to the same rules and policies as FCC staff. Contractors must also follow the reporting and other procedures in the FCC's Breach Notification Policy.

B. Does this system leverage Enterprise Access Controls?

Yes. OIG leverages Enterprise Support Infrastructure and Enterprise Inheritance Access controls.