UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

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

October 6, 2020

OFFICE OF THE GENERAL COUNSEL

WASHINGTON, DC 20554

Record of Approval

Document Approval		
Privacy POC		
Printed Name: Bahareh Moradi		**Privacy Legal Advisor, Office of General Counsel**
Approval Structure		
Printed Name: Margaret Drake		**Senior Agency Official for Privacy**
Signature: Margaret Drake	**Date** 10/6/2020	

Record of Approval

Date	Description	Author

Table of Contents

OIG

1.1. Introduction

Section 208 of the E-Government Act of 2002[1] 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).

Please copy the table as necessary to complete the information for each system within the boundary.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Case Management System (CMS)
DOES THE SYSTEM CONTAIN PII? Yes
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 APPPLICABLE)? 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 THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Concordance
DOES THE SYSTEM CONTAIN PII? Yes
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 APPPLICABLE)? 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 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. Because of its law enforcement eDiscovery purpose, Concordance may contain a broad range of PII elements.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM TeamMate
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) TeamMate may contain individuals' names, addresses, and phone numbers 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 non-public releasable reports.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? 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 THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM AWS GovCloud Database enclave
DOES THE SYSTEM CONTAIN PII? Yes
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 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 APPPLICABLE)?
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 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),[3] 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)]

AWS GovCloud Database enclave

[3] *See* NIST, *The NIST Definition of Cloud Computing*, Special Pub. No. 800-145 (Sep. 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final.

☒ 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) [list applicable system(s)]

AWS GovCloud Database enclave

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

☒ Yes, all the IT systems are FedRAMP certified
☐ No, none, or only some, of the IT systems are FedRAMP certified

The only OIG system in the cloud is the database enclave, which resides on the FCC's FedRAMP compliant AWS.gov cloud.

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.

The OIG System applications support the OIG's mission to detect and prevent fraud, waste and abuse in FCC programs and operations. The Inspector General reports the results of investigations, audits, and reviews semi-annually to the Chairman and to the United States Congress. These reports, in turn, inform the Chairman, 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 Statement[4] 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

[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.

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.

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 the referral of any potential violations that are revealed throughout the course of the investigation. We do not request information that is beyond the scope of requirements for the investigation completed, or beyond the issues revealed in the investigation.

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. Social Security Numbers (SSNs) are also used to confirm identities of individuals pursuant to standard law enforcement procedures. SSNs may also be used to meet certain law enforcement matching requirements and where necessary to facilitate certain law enforcement requests.

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. Internal connections are not reflected within the Cyber Security Asset Management (CSAM) tool due to the fact that there aren't any internal connections. There aren't any Information Sharing Agreements (ISA) in place.

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 process and not an automatic system to system connection.

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 polices 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	**__High**	**_X__Moderate**	**___Low**
Integrity	**__High**	**_X__Moderate**	**___Low**
Availability	**__High**	**_X__Moderate**	**___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, like those in the OIG Boundary. 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 4), https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

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 system does not inherit privacy controls from an external provider.

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 prior to obtaining access to any FCC systems, 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**.**

C. Does the system leverage the FCC's Accounting for Disclosure control?

N/A – the systems in this Boundary are exempt from disclosure.