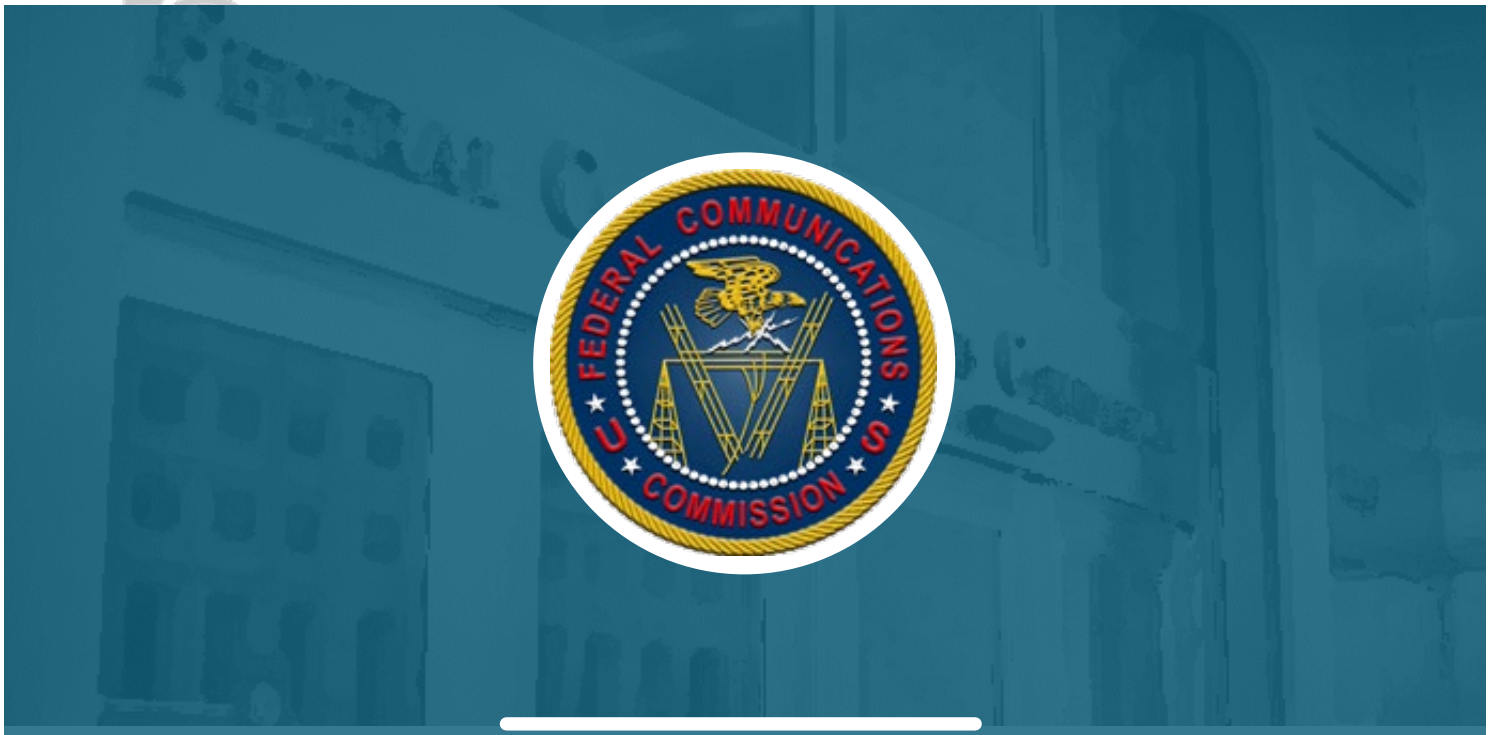

UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT FOR THE ENFORCMENT BUREAU (EB) BOUNDARY

12/16/2020

OFFICE OF THE GENERAL COUNSEL

WASHINGTON, DC 20554

Record of Approval

Document Approval		
Privacy POC		
Printed Name: Bahareh Moradi		**Privacy Legal Advisor, OGC**
Approval Structure		
Printed Name: Margaret Drake		**Senior Agency Official for Privacy**
Signature: Margaret E Drake Digitally signed by Margaret E Drake DN: cn=Margaret E Drake, o=Federal Communications Commission, ou=Privacy, email=margaret.drake@fcc.gov, c=US Date: 2020.12.16 15:28:37 -05'00'	**Date** 12/16/2020	

Record of Approval

Date	Description	Author

Table of Contents

Enforcement Bureau

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 Enforcement Bureau Activity Tracking System (EBATS)
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Name, contact information, and other forms of PII may be collected and maintained in the system because of its investigatory and enforcement purposes.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? FCC/EB-5, Enforcement Bureau Activity Tracking System, 75 Fed. Reg. 77872 (Dec. 14, 2010)
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 47 U.S.C. 301, 303, 309(e), 312, 315, 318, 362, 386, 501, 502, 503, 507, and 510.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No.

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)]

☐ 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)]

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

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 Enforcement Bureau (EB) is the primary FCC unit responsible for enforcing the provisions of the Communications Act, the Commission's rules, orders, and various licensing terms and conditions. The only system within the EB Boundary is EBATS, which EB uses to track its activity and manage its documents related to its enforcement mission.

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

[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.

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.

EBATS does not collect PII directly from the public; however, information provided by and pertaining to members of the public may be retained in the system. For example, members of the public may report an alleged violation of the Commission's rules using the FCC's informal complaint intake portal, the Consumer Help Center (CHC). These consumer complaint data migrate into EBATS for investigation and possible enforcement action. EB staff may also enter data and upload evidence that has been created or obtained in connection with EB's investigatory and enforcement activities. In the course of EB investigations, information may be collected from law enforcement sources, directly from individuals, or from third parties.

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

The information collected is no greater than what is required to support EB investigations of alleged rule violations and the referral of any potential violations that are revealed throughout the course of the investigation. EB does not request information that exceeds the buden of proof required to legally support a finding of a rule violation or beyond the issues identified during the investigation.

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

If EB relies upon information and documents that contain PII, both EB staff and managers evaluate and validate the accuracy and completeness of these data. If necessary, EB will verify these data against other sources and public records.

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?

EBATS receives informal consumer complaint data from the FCC's Consumer & Governmental Affair Bureau's intake system, CHC, as well as the FCC's Public Service

[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.

Interference/Enterprise Service Interference (PSIX/ESIX) systems. The connections are currently not reflected in CSAM. EBATS does not share data with other systems.

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 some information may be shared through a manual process with other law enforcement organizations to support ongoing investigations. No API exists to share data from EBATS.

C. How long will the PII be retained and how will it be disposed of?
EBATS is subject to records schedule DAA-0173-2014-0002.

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)[5], https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

[5] NIST published revision 5 of SP No. 800-53 in September 2020. OMB Circular A-130 instructs federal agencies to "meet the requirements of, and be in compliance with, NIST standards and guidelines within one year of their respective publication dates," for legacy systems. OMB Circular A-130, App. I, at I-16.

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.

No.

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 system within the EB Boundary is restricted to authorized FCC system owners and end users who are assigned to the Enforcement Bureau. All system owners and end users must adhere to the FCC Rules of Behavior and ensure that access to any PII stored in the EB Boundary is appropriately limited. Access to the information stored within the EB Boundary 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 EB Boundary when necessary and only after access has been authorized by the system owner. Some authorized FCC contractors have access to the system 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 EB Boundary 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 – information in the system in this Boundary is exempt from disclosure.