UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT (PIA) FOR THE CONSUMER AND GOVERNMENT AFFAIRS BUREAU (CGB) BOUNDARY

July 2023
Annual Review Date

OFFICE OF GENERAL COUNSEL

Washington DC, 20554

Next Review Cycle: July 2024

Record of Approval

Document Approval	
Drafter Name: Farod Preston	**Bureau/Office: OMD/IR**
SAOP Approval	
Printed Name: Elliot S. Tarloff	**Senior Agency Official for Privacy**
X ELLIOT TARLOFF Digitally signed by ELLIOT TARLOFF Date: 2023.07.31 13:04:52 -04'00' **Signature & Date**	

Record of Approval

Date	Description	Author
5/27/2023	Validation of information - System Owner	Suzy Rosen Singleton
5/27/2023	Validation of completeness - IT Compliance Lead	Liem Nguyen

Revision History

Date	Description	Name
7/3/2023	Original Document Created	ISSO - Farod Preston Privacy Team - Elliot Tarloff & Katherine Morehead
7/7/2023	Incorporation of Paperwork Reduction Act and Privacy Act Statements	ISSO - Farod Preston
7/31/2023	Clerical edits	Senior Agency Official for Privacy (SAOP) – Elliot S. Tarloff

CGB Boundary

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).

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM: Video Programmers and Programming Distributors Registry (VPPD)
NAME OF BUREAU: Consumer and Government Affairs Bureau (CGB)
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE): Business contact and location information
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? FCC/CGB-1 Informal Complaints, Inquiries, and Requests for Dispute Assistance FCC-2 Business Contacts and Certifications
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 47 CFR Part 79
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, this system shares PII with CORES

The VPPD system was built and is hosted on ServiceNow and, in a future review cycle, will be incorporated into the ServiceNow Boundary Privacy Impact Assessment.

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)

☒ The FCC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service or PaaS)

The VPPD system was built, and is hosted, within the ServiceNow platform.

☐ 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)

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.

Under the Closed Captioning Responsibilities Order (2016), Video Programming Distributors (VPDs) are required to register their contact information in a database designated to receive such filings via FCC web form. Video Programmers are also required to register their contact information for the receipt and handling of written closed captioning complaints via FCC web form.

[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.

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.

The PII that is collected by and maintained on VPPD primarily comes directly from individuals. The Privacy Act Statement can be found here: Paperwork Reduction Act and Privacy Act Statements

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

Under the Closed Captioning Responsibilities Order, VPDs are required to register their contact information in a database designated to receive such filings via FCC web form. Video Programmers are also required to register their contact information for the receipt and handling of written closed captioning complaints via FCC web form. The webform does not allow for the submission of PII outside of the required fields.

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

It is the responsibility of each entity to ensure the completeness, accuracy, and currency of data at the time they are submitted to the FCC. Information that is used by the FCC as part of its enforcement and other activities will be reviewed for accuracy and timeliness as required by the particular activity and the laws and authorities, if any, applicable at the time the agency compiles the records (e.g., Communications Act, personnel laws, administrative or court evidentiary rules and procedures).

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?

VPPD will collect and maintain PII in the form of business contact information. Both Video Programming Distributors (VPD)s and Video Programmers are required to register

[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.

contact information. VPPD is integrated with CORES and will process FRNs as User IDs. There are no external connections for the VPPD system.

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")?

No. The VPPD system allows for both Video Programming Distributors (VPD)s and Video Programmers to register contact information, and for Video Programmers to provide certifications of compliance electronically per the FCC's Closed Captioning Responsibilities Order (2016).

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

Information in the systems within this boundary is retained and destroyed in accordance with applicable FCC policies and procedures, as well as with the FCC records disposition schedule or General Records Schedules approved by the National Archives and Records Administration (NARA).

1.5 Data Security and Privacy

A. What are the system's ratings for confidentiality, integrity, and availability?

Confidentiality	☐ High	☒ Moderate	☐ Low
Integrity	☐ High	☒ Moderate	☐ Low
Availability	☐ High	☒ 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. 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 systems/applications housed within the ServiceNow platform do 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?

FCC Staff: Access to VPPD is restricted to the VPPD system owner and end users. The VPPD system owner and end users must adhere to the FCC Rules of Behavior. Access to the information stored within VPPD 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.

Contractors: FCC may have contractor support within program areas, and these contractors will have access to the information in VPPD as required to perform their duties.

B. Does this system leverage Enterprise Access Controls?

Yes, the system leverages Enterprise Access Controls.