UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT FOR THE PERSONNEL CASE ADJUDICATIONS TRACKING SYSTEM (PCATS) BOUNDARY

September 25, 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** 9/25/2020	

Record of Approval

Date	Description	Author

Table of Contents

PCATS

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 Personnel Case Adjudications Tracking System (PCATS)
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) The Personnel Case Adjudications Tracking System (PCATS) is a personnel security and suitability tracking tool. The FCC Security Operations Center (SOC) uses PCATS to conduct employee intake, process employees for preliminary adjudication, input information from formal investigations conducted by the Defense Counterintelligence and Security Agency at the U.S. Department of Defense (DOD), conduct a final adjudication with badging, and generate correspondence to employees sharing the final results of their adjudication and on-boarding next steps. Because of its national and personnel security purpose, PCATS stores PII elements including medical, biometric, financial, legal, employment, photographic, educational, and contact information about FCC employees, contractors, applicants for employment, as well as the personal and professional contacts named in an applicant's SF-86 form. PCATS also contains other forms of PII about the applicant, such as place of birth or selective service number.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? FCC/OMD-16, Personnel Security Files, 83 Fed. Reg. 10721 (Mar. 12, 2018).
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The information in this system is collected, maintained, and disseminated pursuant to 5 U.S.C. §§ 73, 1302, 2951, 3301, 3304, 3328, 9101; Executive Order Nos. 10450, as amended, 10865, 12968, 13526; Pub. L. 104-134 (April 26, 1996); 5 CFR parts 2, 5, 731, 732, 736, and 1400; 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. SOC staff manually enters information from PCATS to an online portal managed by OPM.

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 FCC SOC collects PII as necessary to conduct and comply with requirements regarding background investigations and security clearances that determine an individual's eligibility and suitability for work at the FCC. This collection is consistent with the FCC's statutory obligation to maintain current personnel adjudications for employees, contractors, and temporary hires.

[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.

FCC SOC staff and contractors upload data that has been created or obtained in connection with the SOC's national and personnel security activities. Some information comes from personnel questionnaire forms completed by candidates for employment with the FCC, and is manually entered into PCATS by SOC staff, who periodically update the system to reflect the status of background, clearance, and security investigations. For example, individuals may complete SF-85 Questionnaire for Non-Sensitive Positions, SF-85P Questionnaire for Public Trust Positions, SF-86 Questionnaire for National Security Positions, OF-306 Declaration for Federal Employment, and/or A-600 FCC Security Operations Center Contract Personnel Record. The SF-86 Questionnaire requests PII about personal and professional contacts. All of these forms include Privacy Act Notices. Other information that is manually entered into PCATS by SOC staff comes from OPM's e-QIP system used for background investigations of all federal employees and contractors. Members of the public do not enter information, including PII, directly into PCATS.

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

The information collected is that which is required for the completion of background investigations, and the resolution of any issues 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.

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 SOC staff and verified against information collected from other records sources. Social Security Numbers are

[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.

also used to confirm identities of individuals pursuant to Public Law 104-134 (April 26, 1996). Reinvestigations of FCC staff and contractors are conducted every six or ten years depending on level of security clearance. The system also has built in audit logs to allow system administrators to monitor disclosures and determine who had access during a particular time.

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")?

There are no direct interfaces or interconnections in the system. Members of the SOC do export text files on a routine basis, which are then manually uploaded to an OPM site. The information that is uploaded relates to investigation status and adjudication results.

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

The data is retained throughout an employee's or contractor's tenure at FCC. Records retention policy requires that clearance records are maintained for five years after an employee leaves the agency, and all other records are maintained for three years. Records will be deleted from the system.

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 PCATS. As a cloud system, PCATS is hosted on a FedRAMP system and leverages those security controls in addition to those implemented by the FCC. Following the risk-based policy established in the Federal Information Modernization Act (FISMA),[5] 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 PCATS is restricted to authorized SOC supervisors and staff, including contractors, to fulfill their job duties. All SOC contractors who have access to the PII stored in PCATS 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. Micropact, the vendor, as well as

[5] The Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002) was subsequently modified by the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014). As modified, FISMA is codified at 44 U.S.C. § 3551 et seq.

Chain Bridge Solutions, the system support contractor, also have access to certain administrative aspects of PCATS to ensure functionality, but do not have access to the PII stored in PCATS.

B. Does this system leverage Enterprise Access Controls?

Yes, the identification of authorized users of PCATS and the specification of access privileges is consistent with the requirements in associated security controls that are depicted within the PCATS System Security Plan (SSP). Any users requiring administrative privileges on the PCATS accounts must be approved by the System Owners.

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

N/A – this system is exempt from disclosure.