



UNITED STATES
FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT (PIA) FOR THE WIDEPOINT-INTELLIGENT TECHNOLOGY MANAGEMENT SYSTEM (ITMS) BOUNDARY


December 2023

OFFICE OF GENERAL COUNSEL

Washington DC, 20554

Next Review Cycle: December 2024

Record of Approval

Document Approval	
Drafter Name: Farod Preston	Bureau/Office: Office of the Managing Director (OMD), Information Resiliency (IR)
SAOP Approval	
Printed Name: Elliot S. Tarloff	Senior Agency Official for Privacy
	
Signature & Date	

Record of Approval

Date	Description	Author
11/30/2023	Validation of information – System Owner	Lynette Taper-Pope
12/05/2023	Validation of completeness – IT Compliance Lead	Shelton Rainey

Revision History

Date	Description	Name
11/03/2023	Original Document Created	Information System Security Officer (ISSO) – Farod Preston
11/29/2023	Clerical edits and revisions to Sections 1.2, 1.3A-B, and 1.4A	Privacy Advisor – Katherine Morehead; Senior Agency Official for Privacy (SAOP) – Elliot Tarloff
11/30/2023	Final clerical edits and revisions to Sections 1.2	SAOP
12/18/2023	Revision to Section 1.5C to clarify that controls are inherited from WidePoint the SaaS provider	SAOP

WidePoint-ITMS 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
<p>NAME OF THE SYSTEM WidePoint-Intelligent Technology Management System (ITMS).</p>
<p>NAME OF BUREAU Office of the Managing Director (OMD).</p>
<p>DOES THE SYSTEM CONTAIN PII? Yes.</p>
<p>PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) ITMS contains business contact and employment information.</p>
<p>IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? FCC/OMD-18 - FCC Wireless Communications Information</p>
<p>WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 5 U.S.C. 301, 44 U.S.C. 3101, and 47 U.S.C. 154(i).</p>
<p>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.</p>
<p>DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes, ITMS shares information with the FCC Internal Okta Tenant for authentication purposes and ServiceNow for request submissions. Prior to gaining access to ITMS, users must authenticate via Okta Single-Sing-On (SSO) which is integrated with ITMS. While ITMS has the capability to leverage ServiceNow regarding mobile device request, replacement, upgrade, order processing, approvals, etc., the system is not yet configured to do so. Currently, ServiceNow is being utilized only to facilitate mobile device related requests from FCC employees; the ITMS System Owner does not use ServiceNow to process requests, provide approvals and denials, etc. This feature of ITMS can be configured upon request to the vendor from the ITMS System Owner.</p>

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 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.

Note: ITMS is currently undergoing FedRAMP Project Management Office (PMO) review ahead of receiving their FedRAMP authorization.

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 ITMS will capture, store, and transmit PII associated with the procurement and lifecycle of wireless services and mobile devices for FCC staff and select contractors (based on business needs). This PII includes business contact information and employment information, which is necessary for the FCC for the procurement and full-lifecycle management/support of wireless services and mobile devices for FCC FTEs and select contractors (based on business needs).

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 Statement⁴ for each system that is included with the online or paper form the system(s) use(s) to collect the PII.**

Yes. The ITMS collects information directly from FCC users. The system owner is working with the Privacy Team to develop a Privacy Act Statement that will be made available through the ServiceNow portal at the point of collection.

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

The ITMS System Owner, and other privileged system users, will have access to PII. Additionally, after employee mobile device requests are submitted via ServiceNow, FCC Human Resources (HR) will participate in the processing of mobile device requests, replacements, upgrades, etc. The collection of PII will be limited to only the information needed for the procurement and full-lifecycle management/support of wireless services and mobile devices for FCC FTEs and select contractors (based on business needs).

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

The ITMS System Owner, and Lead System Administrator, participate in monthly status meetings with the vendor and participating telecommunications carriers that provide wireless service(s) to FCC. Additionally, the System Owner has confirmed that all mobile device requests will be processed by FCC HR, and that required PII will be reviewed for accuracy and completeness prior to being entered into the ITMS system by privileged users.

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?**

Users must authenticate to the ITMS via Okta single-sign-on (SSO). Initial mobile device requests and requests for mobile device replacement, upgrade, etc., will be submitted and stored with ServiceNow. FCC HR will participate in the processing of mobile device requests submitted to ServiceNow and the routing of tickets to the FCC ITMS Team. All

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.

requests must be approved by the ITMS System Owner via email correspondence prior to being fulfilled. Typical mobile device requests will include a requestor’s business contact information. There is no ISA in CSAM for ITMS. However, the internal connections to both Okta and ServiceNow are documented in CSAM.

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.

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	<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.**

No. No privacy controls are inherited from an entity other than WidePoint, the SaaS provider. There is no ISA or MOU in place regarding ITMS.

1.6 Access to the Information

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

FCC full time employee (FTE) staff and select FCC contractors based on business needs.

- B. Does this system leverage Enterprise Access Controls?**

Yes.