UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT (PIA) FOR THE OKTA SYSTEM BOUNDARY[1]

November 2023

OFFICE OF GENERAL COUNSEL

Washington DC, 20554

Next Review Cycle: November 2024

Record of Approval

Document Approval	
Drafter Name: Ram Subramanian	**Bureau/Office: OMD**
SAOP Approval	
Printed Name: Elliot S. Tarloff	**Senior Agency Official for Privacy**
X ELLIOT TARLOFF Digitally signed by ELLIOT TARLOFF Date: 2023.11.29 14:15:56 -05'00'	
Signature & Date	

Record of Approval

Date	Description	Author
10/22/2023	Validation of information – System Owner	Christopher Lathrop
11/24/2023	Validation of completeness – IT Compliance Lead	Shelton Rainey

Revision History

Date	Description	Name
8/10/2021	Original Document Created	ISSO – Ram Subramanian
10/26/2023	Clerical/formatting edits and revisions to Sections 1.2 & 1.2B, 1.3A-C, 1.4A-B, 1.5A, C.	Privacy Advisor – Katherine Morehead Senior Agency Official for Privacy (SAOP) – Elliot S. Tarloff
11/7/2023	Clerical/formatting edits and revisions to Sections 1.2, 1.3C-D, 1.4A	SAOP
11/14/2023	Revisions to Section 1.3D and 1.4A	SAOP
11/16/2023	Clerical edits and revisions to Sections 1.2 & 1.4A	SAOP

OKTA System 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 Okta
NAME OF BUREAU OMD
DOES THE SYSTEM CONTAIN PII? Yes. Okta collects and maintains PII, and information can be retrieved from Okta based on an individual's name or other unique identifier.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Okta collects contact, login, and network activity information to authenticate and authorize users to various FCC systems.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? The FCC is in the process of developing and publishing a System of Records Notice that covers the Okta information system.
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 5 U.S.C. chapters 53, 55, 61, 63, and 65; Executive Order 9397, as amended (Nov. 20, 2008); Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (Pub. L. 104-193); 10 U.S.C. 1408; 42 U.S.C. 659; 47 USC 154(i).
DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT? Yes
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Okta incorporates information, including PII, from the FCC's Active Directory and from FCC User Registration. Additionally, Okta shares PII with every application that integrates Okta to assist with Single Sign On (SSO). Okta also shares information with the FCC's instance of Splunk, a separate information system for monitoring and analyzing network activity.

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.

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.

It is necessary for Okta to collect certain PII elements to perform its authorization and authentication functions.

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.

Okta collects PII from internal users and external users indirectly to allow for the authentication and authorization of users to other FCC applications.

Internal – User data are collected as part of the onboarding process into Active Directory, which in turn provides the PII to Okta.

External – FCC User Registration collects the data from external users and sends the data to Okta.

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

The FCC collects only the PII from individuals that is necessary to authenticate and authorize them to other FCC systems and applications.

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

It is the responsibility of individuals who provide information to ensure that the PII is accurate, complete, and up to date. For internal users, the accuracy, completeness, and timeliness of the PII, which is collected indirectly from Active Directory, is also covered by the Enterprise Support Infrastructure (CSAM ID 19) SSP PII Processing and Transparency (PT) control family. For external users, the accuracy, completeness, and timeliness of the PII, which is collected from FCC User Registration, is ensured by permitting users to update their information. The accuracy of the PII collected from User Registration for external users is also covered in the CORES2 FO (CSAM ID 81) SSP PII Processing and Transparency (PT) control family.

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.

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?

Okta collects PII from internal users and external users indirectly to allow for the authentication and authorization of users to other FCC applications.

Internal – User data are collected as part of the onboarding process into Active Directory, which in turn provides the PII to Okta.

External – FCC User Registration collects the data from external users and sends the data to Okta.

Okta enables single sign on (SSO) to other FCC applications. Therefore, the PII that Okta receives from AD and User Registration is shared with the various other FCC applications that are integrated with Okta for SSO. Okta also shares information with the FCC's instance of Splunk, separate information system for monitoring and analyzing network activity. Okta's connections to these other applications are documented in CSAM within Okta's SSP.

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. Okta collects and transmits data via API, but only from/to other FCC systems and applications.

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.

Yes, Okta inherits privacy controls from the FedRAMP-authorized vendor.

1.6 Access to the Information

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

Authorized FCC employees and contractors will have access to the PII in Okta.

B. Does this system leverage Enterprise Access Controls?

Yes