

1 System Overview

1.1 Describe the project/system and its purpose.


The FTC utilizes the Okta Customer Identity and Authentication Management (Okta CIAM or Okta) identity cloud platform to secure and validate external user identities. Okta has implemented the following features to support the registration of users for custom applications built into the ServiceNow platform.

Single Sign On (SSO) – SSO is a technology that combines different application login screens into one. With SSO, external users must first complete the Okta registration process; once registered, users only need to enter their login credentials (username, password) one time on a login page to access the ServiceNow applications.

Security Markup Language (SAML) – Okta utilizes SAML to integrate with the FTC SSO. SAML is an XML-based standard for exchanging authentication and authorization data between security domains. Okta exchanges information with the ServiceNow SAML plugin, which supports SSO-based authentication.

Multi-Factor Authentication (MFA)/ Okta Verify – MFA, also known as two-step verification, requires users to enter more than one set of credentials to authenticate their account. Okta Verify is an MFA factor and authenticator application developed by Okta that is used to confirm the user's identity when they sign into their Okta account. After the external user installs Okta Verify on their primary device, they can then verify their identity by approving a push notification or by entering a one-time code. Okta is used to verify identity only and act as a gateway to the FTC ServiceNow applications.

These features were chosen to provide a high level of identity management security to ensure that the users accessing the system are thoroughly authenticated each time they enter the system.

External User Registration – When requesting access to the ServiceNow applications system, an external user receives an email prompting them to register an account using a hyperlink provided within the email. Clicking on the hyperlink takes the user to the Okta customer registration web page. The user must fill in the following fields to complete the registration: first name, last name, business email, phone number, and company name. Upon successful registration, the user is presented with a  email on we. The

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The Federal Trade Commission Act, 15 U.S.C. §§ 41-58, the Commission Rules of Practice, and other statutes and regulations enforced by the agency authorizes the FTC to collect the information that is sent, received, and maintained by the Okta platform. In addition, collection of this information for purposes of managing and securing individuals' system access is authorized under the Federal Information Security Modernization Act, 44 U.S.C. §§ 3551 et seq.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)¹ may be collected or maintained in the system/project. Check all that apply.

<i>PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.</i>		
<input checked="" type="checkbox"/> Full Name	<input type="checkbox"/> Biometric Identifiers (e.g., fingerprint, voiceprint)	<input checked="" type="checkbox"/> User ID
<input type="checkbox"/> Date of Birth	<input type="checkbox"/> Audio Recordings	<input type="checkbox"/> Internet Cookie Containing PII
<input type="checkbox"/> Home Address	<input type="checkbox"/> Photographic Identifiers (e.g., image, x-ray, video)	<input type="checkbox"/> Employment Status, History, or Information
<input checked="" type="checkbox"/> Phone Number(s)	<input type="checkbox"/> Certificates (e.g., birth, death, marriage, etc.)	<input type="checkbox"/> Employee Identification Number (EIN)
<input type="checkbox"/> Place of Birth	<input type="checkbox"/> Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	<input type="checkbox"/> Salary
<input type="checkbox"/> Age	<input type="checkbox"/> Vehicle Identifiers (e.g., license plates)	<input type="checkbox"/> Military Status/Records/ ID Number
<input type="checkbox"/> Race/ethnicity	<input type="checkbox"/> Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	<input checked="" type="checkbox"/> IP/MAC Address
<input type="checkbox"/> Alias	<input checked="" type="checkbox"/> Geolocation Information	<input type="checkbox"/> Investigation Report or Database
<input type="checkbox"/> Sex	<input type="checkbox"/> Passport Number	<input type="checkbox"/> Driver's License/State ID Number (or foreign country equivalent)
<input checked="" type="checkbox"/> Email Address		<input checked="" type="checkbox"/> Other (<i>Please Specify</i>): Login and Log-out Date Time, Security questions for password reset/ PIN/Password/ Company Name_____
<input type="checkbox"/> Work Address		
<input type="checkbox"/> Taxpayer ID		
<input type="checkbox"/> Credit Card Number		
<input type="checkbox"/> Facsimile Number		
<input type="checkbox"/> Medical Information		
<input type="checkbox"/> Education Records		
<input type="checkbox"/> Social Security Number		
<input type="checkbox"/> Mother's Maiden Name		

¹ Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

Not applicable. The system does not collect any additional non-PII data.

2.3 What is the purpose for collection of the information listed above?

The information listed above is collected by Okta CIAM to validate user identity before granting users access to the ServiceNow application. The PII collected is used to create the registration email message generated by ServiceNow. The registration email is sent to the email address provided by the user.

Adaptive Multi-Factor Authentication (AMFA) for ServiceNow (AMFA) is a security solution that provides multi-factor authentication for ServiceNow users. It is designed to protect sensitive data and prevent unauthorized access to the system. The solution is based on the Okta CIAM platform and provides a secure and user-friendly authentication experience. It is designed to protect sensitive data and prevent unauthorized access to the system. The solution is based on the Okta CIAM platform and provides a secure and user-friendly authentication experience.

Source of Data

Type of Data Provided & How It Is

least privilege, code changes and maintenance are split between multiple teams. In all cases, administrative access is based on the concept of least privilege; users are limited to the minimum set of privileges required to perform their required job functions.

3.3 If you answered “yes” to 3.2, describe the privacy incident response plan maintained by the contractor’s organization or third-party service provider.

FTC contractors with access rights to the Okta CIAM application are subject to the same rules and policies as FTC staff, including adherence to the FTC Breach Notification Response Plan. Okta CIAM is also be subject to the FTC Incident Response plan, which includes measures to prevent, detect, contain, eradicate and recover from breaches that would include personal identity information (PII).

Okta is a Federal Risk and Authorization Management Program (FedRAMP) authorized system providing Software as a Service to the public cloud. Okta’s Incident Response procedures have been evaluated by a Third-Party Assessment Organization (3PAO), and Okta’s assigned controls meet FedRAMP compliance standards. The Okta Incident Response Team (IRT) is responsible for developing the facts relating to an incident and determining the appropriate response. If the

account with Okta CIAM to ensure that the information they have provided is accurate and up to date. See Section 4.3. and 4.4.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Yes. Okta CIAM can currently be accessed by FTC staff and FTC contractors. Contractors and Okta administrative users must sign confidentiality and nondisclosure agreements, and, in some cases, are required to undergo additional security clearance procedures.

Okta operates under a shared security responsibility model. Okta is responsible for the security of the cloud platform and underlying infrastructure, while the FTC is responsible for the security in the cloud, such as granting correct permissions, disabling accounts for former employees, enforcing multi-factor authentication, properly configuring and monitoring authentication policies, reviewing system logs, and monitoring Okta tenants for attacks. All Okta data is encrypted both at rest and in transit. Additionally, Okta uses organization-level encryption to protect sensitive data, such as authentication credentials and certificates.

User PII stored within Okta is accessible by a limited number of people based on

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

<i>Risk</i>	<i>Mitigation Strategy</i>
Misuse of data by authorized users	Prior to receiving access to the FTC's network, all users must agree to the FTC Rules of Behavior, which includes consenting to monitoring and restrictions on data usage.
Unauthorized system access	All FTC users must have an FTC account and government issued PIV card to access Okta CIAM. The FTC utilizes a combination of technical and operational controls to reduce risk in Okta CIAM, such as encryption, passwords, audit logs, firewalls, malware identification, and data loss prevention policies. As a FedRAMP-approved cloud service provider, Okta CIAM undergoes regular reviews of its security controls. External users will be required to authenticate using two-factor authentication: username/password and passcode delivered to user (voice or token authenticator app on their smartphone).
Data leakage	Non-FTC ServiceNow system administrators are not allowed to review, audit, transmit, or store FTC Okta CIAM registration data, which minimizes privacy risks from the vendor source.
Unwanted eavesdropping	Users interact with Okta CIAM over the TLS protocol (https), an authenticated protected channel.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

All Okta CIAM users are required by administrative security policy to select either Okta Verify or Voice Call Authent A A,n)-12d (k)2 (o)4 (e)4 (pa)4 ()T0.002 Tc -0.002ftabi

To the extent, if any, that the FTC collects and maintains agency records about individuals for identification and access and security purposes, such records would be covered by FTC VII-3 (computer user identification and access records). See <https://www.ftc.gov/site-information/privacy-policy/privacy-act-systems>.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The administrative and technical controls described in section 5.2 of this document provide assurance that the collection, use, and maintenance of the information will be conducted as described in this PIA. This PIA aligns with the FTC's existing privacy policies and procedures and is subject to periodic review by the Office of the Chief Privacy Officer (OCPO), in consultation with relevant program staff and other relevant agency officials.