PRIVACY IMPACT ASSESSMENT

State Enterprise – Identity as a Service (SE-IDaaS) PIA

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) Date of completion of this PIA: January 2023
(b) Name of system: State Enterprise Identity as a Service
(c) System acronym: SE-IDaaS
(d) Bureau: IRM (IRM/FO/ITI/SI)
(e) iMatrix Asset ID Number: 290662
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable): N/A

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

State Enterprise Identity as a Service (SE-IDaaS) is an identity and access management system that provides secure access to web-based applications for Department of State users. The system provides integrated Department of State (Department) systems the ability to leverage existing public key infrastructure (PKI) based authentication services

using a Personal Identity Verification (PIV) card or other Department-approved PKI certificates.

The core business needs for this system are:

1. Single Sign-On (SSO)
2. Multi-Factor Authentication (MFA)

The system provides Department users remote access to Department resources, i.e., applications, via the cloud – securely authenticating their identity through Okta.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The State Enterprise Identity as a Service (SE-IDaaS) stores the first name, last name, and Department of State e-mail address, which is the equivalent to User Principal Name (UPN) imported from Active Directory for all enterprise users. Enterprise users include direct, hire employees, Personal Service Contractors (PSC), When Actually Employed (WAE), interns, fellows, domestic/overseas contractors, locally employed staff (LES), detailees, and other government agencies (tenants). This is the minimal data required to establish user accounts. All data stored within the enterprise system is used to facilitate authentication to connected applications as well as provisioning, deprovisioning, and user registration.

Non-enterprise user information collected is their first name, last name, and Non-Department e-mail address. Non-enterprise users include FSI faculty, university researchers, members of a household (non-LES), retirees (non-WAE), non-governmental organizations (NGOs), and other government agencies (non-tenants).

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- Federal Information Security Modernization Act of 2014 (44 U.S.C. § 3551 et. seq.)
- Departmental Regulations (5 U.S.C. § 301)
- Organization of Department of State (22 U.S.C. § 2651a)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)?

☒Yes, provide:

- SORN Name and Number:
  Network User Account Records, State-56

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  December 12, 2017

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)):

- Disposition Authority Number:
  DAA-GRS-2013-0006-0004 (GRS 3.2, item 031)

- Length of time the information is retained in the system:
  Temporary. Six years after the user account is terminated.

- Type of information retained in the system:
  User identification and authorization records associated with systems which are highly sensitive and potentially vulnerable

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☐No ☒N/A

- If yes, under what authorization?

(d) How is the PII collected?

Enterprise user attributes are imported into the State Enterprise Identity as a Service (SE-IDaaS) from the Department's Active Directory. Non-Enterprise users will have their information provided by a government sponsoring official or be sourced from integrated endpoint applications (for example Salesforce, Safety and Accountability For Everyone (SAFE), and Foreign Affairs Network (FAN) mail).

(e) Where is the information housed?

☐ Department-owned equipment
☒ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.

The State Enterprise Identity as a Service (SE-IDaaS) data is stored within the Okta Cloud Service Provider's (CSP) cloud tenant and secured according to FedRAMP requirements for FISMA Moderate systems (example: data encryption at rest).

Okta is the software vendor that provides the Okta Identity as a Service (Okta IDaaS). Our system, State Enterprise IDaaS (SE-IDaaS) is the Department's implementation of the Okta cloud application.

(f) What process is used to determine if the PII is accurate?

Enterprise user information is imported into SE-IDaaS directly from Active Directory (AD). This ensures the accuracy of the information as the information in AD is entered by individual users themselves.

For non-enterprise users, it is the responsibility of each specific user to ensure that their information is accurate. The information within SE-IDaaS can be modified in the user profile by the user themself or by an administrator who may go in and correct any user profile information that is inaccurate.

(g) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Enterprise user information is synced from Active Directory on a scheduled basis. Any updates to users' information in Active Directory will therefore be reflected in SE-IDaaS.

Non-Enterprise user information can be changed by the user themselves or a designated administrator within the specific system for which they have been given access by navigating to the user's profile and correcting any user profile information.

(h) Does the system use information from commercial sources? Is the information publicly available?

Commercial sources are not used, and the information is not publicly available.

(i) How was the minimization of PII in the system considered?

SE-IDaaS collects only the minimum PII required to register, authenticate, and provision user accounts.

5. Use of information

(a) What is/are the intended use(s) for the PII?

All information stored within the State Enterprise Identity as a Service (SE-IDaaS) is used for end user account creation, provisioning, and authentication.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the information is used for authentication into SE-IDaaS and its integrated endpoint applications.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the PII?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

(d) If the system will use test data, will it include real PII?

☐Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal:
SE-IDaaS shares enterprise users' PII with any enterprise Department of State system in need of services offered by SE-IDaaS. SE-IDaaS does not share the PII of non-enterprise users.

External:
No PII will be shared outside the Department of State.

(b) What information will be shared?

Internal:
The information shared will be the minimum information required by SE-IDaaS for enterprise users:

1. First Name
2. Last Name
3. Department of State e-mail

The data collected/shared is the equivalent to the UPN imported from Active Directory (AD) for enterprise users.

External:
N/A

(c) What is the purpose for sharing the information?

Internal:
The purpose of sharing this information is to allow for authentication and Single Sign-On (SSO).

External:
N/A

(d) The information to be shared is transmitted or disclosed by what methods?

Internal:
The State Enterprise Identity as a Service (SE-IDaaS) end user attribute information is transmitted electronically via HTTPS/TLS1.2 (or higher, e.g., TLS 1.3) compliant encryption to the connecting systems.

External:
N/A

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal:
The Department's mission critical applications in use (exceeding 150+) that connect to SE-IDaaS, to facilitate user remote access capabilities, must be pre-registered to allow SSO and Multi-Factor Authentication (MFA).

Direct connection with connecting applications ensures that the data in SE-IDaaS is only shared with systems that have an approved business need for the information. All data shared is necessary to provide user access to subscribing applications for the purpose of authentication.

All data is encrypted using the encryption transport layer security (TLS) protocol over secure http (https) and TLS encryption standards exceed secure socket layer (SSL) since it is the later more current encryption versions in use.

External:
N/A

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

SE-IDaaS does not provide notice to enterprise users directly. Rather they are provided notice via the Network Access Request Form (DS-7667), before being provided an Active Directory account. The information from Active Directory is fed directly to SE-IDaaS.

SE-IDaaS also does not provide notice to non-enterprise users. Non-Enterprise users are provided a user information collection notification via their local system access request form.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?
☐Yes ☒No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?
There are no opportunities for enterprise users or non-enterprise users to decline to provide the information or to consent to particular uses of the information in SE-IDaaS as the system is not the original collector of the information.

(c) What procedures allow record subjects to gain access to their information?

Both enterprise and non-enterprise users are able to gain access to their information; however, from different sources. Enterprise users must make changes to their Active Directory profiles while non-enterprise users can change data within SE-IDaaS or within the end point application. Non-enterprise users log into the SE-IDaaS online. Then, the user clicks their name in the top right corner and a drop-down appears. The user then clicks on “Settings” and then “Edit”. From there, the user can edit and save their personal information.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Enterprise users must make corrections to information via their Active Directory profiles; these changes will be synchronized with SE-IDaaS.

Non-Enterprise Users can change their information in SE-IDaaS (Okta in the cloud/off-prem) by selecting the edit button on their profile.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

Enterprise users are notified every 60 days via email when they are required to update or review their information via Active Directory profiles; changes will be synchronized with SE-IDaaS.

Non-Enterprise users are notified by email when they are required to update or review their profile and are permitted to make changes in SE-IDaaS by selecting the edit button in their profile.

8. Security Controls

(a) How is all of the information in the system secured?

The SE-IDaaS encrypts sensitive user data in compliance with government regulations and policies. The SE-IDaaS encrypts data at rest and in transit, protecting sensitive information from being acquired by unauthorized viewers. Both data and encryption keys are protected. No one, including database administrators have unencrypted access to secured data and keys. Key management is handled as part of the infrastructure and, when at rest, encryption keys are stored separate from data. Encryption is incorporated at several different places within the application stack.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Role	Description
Enterprise End Users	Department of State employees and contractors with Active Directory credentials that will use SE-IDaaS to authenticate into their Department applications. These users have access to their basic user profile and their own information.
Non-Enterprise End Users	External users that do NOT have an Active Directory account that will use SE-IDaaS to authenticate into the Department applications. These users have access to their basic user profile and their own information.
Okta Platform Administrators	Privileged accounts that are responsible for the application configuration of SE-IDaaS. Okta Platform Administrators includes Super Admin, Org Admin, Group Admin, Application Admin, Read-Only Admin, Mobile Admin, Help Desk Admin, API Access Management Admin. SE-IDaaS Platform Administrators are cleared Department FTEs or contractors. Administrators do not have access to State Enterprise Identity as a Service (SE-IDaaS) databases and will only have access to the SE-IDaaS front-end privileged sites with no access to PII.
Department of State Administrators	Privileged accounts on the SE-IDaaS Okta Active Directory Agent Servers Only. These system administrators have no rights or access to the backend of Okta IDaaS core service. These users have access to the SE-IDaaS Okta Active Directory Agent Server logs that log user authentication and access information which contains user data. No PII access is permitted by these administrators.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

Non-Admin users can only access their own user data. Administrative direct access to the SE-IDaaS user data is restricted to cleared Department of State direct hire and contractor employees. The system and database administrators are the only users with direct access to the database for the purpose of performing maintenance. Database Administrators are Cloud Service Provider (CSP) personnel. Department of State Administrators do not have access to State Enterprise Identity as a Service (SE-IDaaS) databases and will only have access to the front-end Okta portal.

(d) How is access to data in the system determined for each role identified above?

Role	Description
Enterprise End Users	Non-Admin users can only access their own user data. FTEs and Contractors that have user accounts for access to the network and e-mail (Active Directory accounts); when granted permission to work remotely, are given access through SE-IDaaS to access Department resources. Enterprise End Users are provided access by the system owner. Enterprise End Users are imported from active directory.
Non-Enterprise End Users	Non-Admin users can only access their own user data. External users that do NOT have an Active Directory account, are granted access by bureau system owners to application(s) and will use SE-IDaaS to authenticate into the Department's application(s). These users have access to their basic user profile and their own information.
Okta Platform Administrators	SE-IDaaS Platform Administrators are cleared DOS FTEs or Contractors. Privileged access is granted by the System Owner (SO) and Information System Security Officer (ISSO) approval, following the principles of least privilege. Administrative Users are required to authenticate into dedicated workstations using their PIV card before accessing SE-IDaaS privileged sites. Requests to access privileged sites outside dedicated workstations will be rejected and logged by SE-IDaaS.
Department of State Administrators	Privileged accounts on the SE-IDaaS Okta Active Directory Agent Servers ONLY. These system administrators have no rights or access to the backend of Okta IDaaS core service. These users have access to the SE-IDaaS Okta Active Directory Agent Server logs that log user authentication and access

	information which contains user data. Access is granted by the system owner.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

The SE-IDaaS monitors all user interactivity with the system and logs it to its event viewer. Okta has a built-in event viewer and provides admins with access to several types of reports to discover and troubleshoot security and access anomalies.
Data includes information such as application usage and access, deprovisioning details, and the exposure of suspicious activity. SE-IDaaS end users can only access their own accounts.

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

Each enterprise role that has access to any PII, must complete the following annual training requirements through the Department's Foreign Service Institute (FSI):

- PA318 - Protecting Personally Identifiable Information
- PS800 - Cybersecurity Awareness