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) Name of system: State Enterprise Identity as a Service

(b) Bureau: Information Resource Management

(c) System acronym: SE-IDaaS

(d) iMatrix Asset ID Number: 290662

(e) Reason for performing PIA:

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

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

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

The Authority to Operate (ATO) package is under development, expected June 2019.

(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 systems the ability to leverage existing public key infrastructure (PKI) based authentication services using a Personal Identity Verification (PIV) card or other approved Department of State approved PKI certificates.

The core business needs for this system are as follows:

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

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

SE-IDaaS users fall into two types:

1. **Enterprise Users**
   - Direct hire employees
   - Personal Services Contractors (PSC)
   - When Actually Employed (WAE)
   - Interns and Fellows
   - Domestic Contractors
   - Locally-Employed Staff (LES)
   - Overseas Contractors
   - Detailee to DOS
   - Other Government Agencies (OGAs) (Tenant)
2. **Non-Enterprise Users**
   - Other Government Agencies (OGAs) (non-Tenant)
   - FSI Faculty
   - University Researchers
   - Member of Household (non-LES)
   - Retirees (non-WAE)
   - Non-Governmental Organization (NGO)

Enterprise Users: 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. 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 Users: User information collected is First Name, Last Name, and E-mail Address.

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

The State Enterprise Identity as a Service (SE-IDaaS) collects user data required to authenticate and authorize end users into target applications.

The relevant legal authorities and/or agreements include:

OMB Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements (M-19-02 § 3)	October 2018

Federal Information Security Modernization Act of 2014 (44 U.S.C. § 3551 et. seq.)	March 2015

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

☒Yes, provide:

- SORN Name and Number: State-56 (Network User Account Records)
- 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.
Click here to enter text.

(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 Division 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:

- Schedule number (e.g., (XX-587-XX-XXX)): DAA-GRS-2013-0006-0004 (GRS 3.2, item 031)
- Length of time the information is retained in the system: 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) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☒No

- If yes, under what authorization?

(c) How is the information collected?

Enterprise user attributes will be imported into State Enterprise Identity as a Service (SE-IDaaS) from the department's Active Directory. Non-Enterprise users will have their information populated via a government sponsoring official, or be sourced from integrated endpoint applications.

(d) 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). See FedRAMP package F1512167750.

(e) What process is used to determine if the information is accurate?

Enterprise user attributes will be imported and synced into State Enterprise Identity as a Service (SE-IDaaS) from Active Directory. Enterprise Users' information in SE-IDaaS is verified by Active Directory. For non-enterprise users, it is up to the discretion of that particular user to ensure that their information is accurate. This information can be modified in their user profile by the user themselves or by an administrator who may go in and correct any user profile information that is inaccurate.

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

Enterprise user attributes will be 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 attributes can be changed by the end user, a designated administrator, or integrated endpoint applications depending on attribute. This information can be modified in their user profile by the user themselves or by an administrator who may go in and correct any user profile information that is inaccurate.

(g) 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.

(h) Is notice provided to the individual prior to the collection of his or her information?

Enterprise users are not provided notice, because they do not interact directly with SE-IDaaS during information collection. Their information is sourced from Active Directory. Non-Enterprise Users are not provided notice, because they do not interact directly with SE-IDaaS during information collection. Their information will be imported from endpoint applications that provide appropriate notice.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, how do individuals grant consent?

- If no, why are individuals not allowed to provide consent?

There are no special provisions for 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.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The State Enterprise Identity as a Service (SE-IDaaS) collects only the minimum number of PII required to register, authenticate, and provision user accounts.

5. Use of information

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

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 information 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 information stored in it? ☐Yes ☒No

If yes:

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

(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

6. Sharing of Information

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

SE-IDaaS is the enterprise-wide solution for access management across the Department's applications. SE-IDaaS administrative user information will be selectively shared with a broad range of endpoint applications, owned by various bureaus, on an as needed basis in order to provide the end users the ability to access the endpoint applications appropriately.

(b) What information will be shared?

The information shared will be the minimum attributes required by the State Enterprise Identity as a Service (SE-IDaaS):

1. First Name
2. Last Name
3. Email (UPN for Enterprise Users)

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

Sharing this information will allow for authentication and single sign-on.

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

The State Enterprise Identity as a Service (SE-IDaaS) end user attribute information is transmitted electronically via HTTPS/TLS1.2 compliant encryption to the connecting system application.

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

The connecting applications must be pre-registered to allow Single Sign On (SSO) and Multi-Factor Authentication (MFA).

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

SE-IDaaS is the enterprise-wide solution for access management across the Department's applications. SE-IDaaS administrative user information will be selectively shared with a broad range of endpoint applications on an as needed basis in order to provide the end users the ability to access the endpoint applications appropriately. 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.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

After the information is received in SE-IDaaS all users can view their own information at any time after submission. Only Non-Enterprise Users can update their information in SE-IDaaS. Enterprise Users must update their information in Active Directory which SE-IDaaS will update on the next scheduled import.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Non-Enterprise Users can change their personal information in SE-IDaaS by selecting the edit button on their profile. Enterprise Users update their information in Active Directory which will update SE-IDaaS on the next scheduled import.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

It is the responsibility of each of the source systems to disclose its procedures for users to correct their information.

8. Security Controls

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

Information stored in the State Enterprise Identity as a Service (SE-IDaaS) is secured based on the baseline required controls for a FedRAMP Moderate system as defined by the FedRAMP PMO. Okta has a moderate FedRAMP certification with a Provisional Authority to Operate (ATO) and a subset of SE-IDaaS's security controls are inherited from this ATO. Information is stored in accordance with the FedRAMP Cloud Service Provider (CSP).

The IDaaS encrypts sensitive user data in compliance with Government regulations and policies. The 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) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

SE-IDaaS Platform Administrators

SE-IDaaS Platform Administrators are cleared DOS FTEs or Contractors. Privileged access is granted by assigning administrator roles after 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. 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.

Department of State Administrators
Department of State Administrators refers to the system administrators on the SE-IDaaS Active Directory (AD) Agent Servers ONLY. These servers do not store any PII and can only be accessed from Dedicated Administrative Workstations by users cleared by IRM/ENM, SE-IDaaS SO, and SE-IDaaS ISSO who have authenticated to AD using their PIV Card. These administrator accounts do not have access to the SE-IDaaS front-end privileged sites or the Okta SaaS back-end.

Okta System Administrators
Administrative direct access to the State Enterprise Identity as a Service (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 encrypted database for the purpose of performing maintenance. Database Administrators are Cloud Service Provider (CSP) personnel. CSP Administrators do not have access to the SE-IDaaS front-end privileged sites or the SE-IDaaS AD Agent Servers.

End Users
Non-Admin users can only access their own user data.

(c) What monitoring, recording, and auditing safeguards 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.

(d) Explain the privacy training provided to authorized users of the system.
Annual privacy training is provided by the Department of State via the FSI online course, PA459 Protecting Personally Identifiable information. The entire Department workforce

is also required to complete the Department's Cybersecurity Awareness course, PS800, which includes a module on privacy.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.
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.

All channels are configured to use strong authentication through smart cards (e.g. PIV) for Enterprise Users and strong passwords with Multi-Factor Authentication (MFA) for Non-Enterprise Users.

(f) How were the security measures above influenced by the type of information collected?
SE-IDaaS has been classified as a moderate level system based on an assessment following FIPS 199 guidelines. The assessment determined the confidentiality, availability, and integrity requirements of the system to all be at a moderate level. The controls mentioned above meet the baseline requirements for a moderate system outlined in FIPS 199 and NIST 800-53.

Due to the nature and content of DOS business operations, system and security measures such as user authentication are in place to safeguard against unauthorized access or compromise to the system.

9. Data Access

(a) Who has access to data in the system?

Category	Description
Enterprise End Users	Department of State employees and contractors with active directory credentials that will use SE-IDaaS to authenticate into their DOS 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 DOS applications. These users have access to their basic user profile and their own information.
SE-IDaaS Platform Administrators	Privileged accounts that are responsible for the Application side configuration of SE-IDaaS. This includes the following types of SE-IDaaS Platform Administrators: Super Admin, Org Admin, Group Admin, Application Admin, Read-Only Admin, Mobile Admin, Help Desk Admin, API Access Management Admin. These users have elevated privileges and can access user data based on the table below.
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, and which contains user data.
Okta System Administrators	Vendor privileged accounts for the Okta Core Service. These accounts are held by Okta IDaaS personnel only. Okta IDaaS deploys the principles of least privilege and segregation of duties, and secures these account. These users do not have access to any PII stored in SE-IDaaS.

(b) How is access to data in the system determined?

Criteria for Access:

- End Users need access to Single Sign-On (SSO) to their endpoint applications.
- Administrators need access to perform administrative duties relating to their role. E.G. user, group, and integration management, accessing reporting, troubleshooting, etc.

All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties. Only users performing system administrative functions have access to aggregate user data for their endpoint application to be used for the purpose of providing operations & maintenance support.

Access to collected data is role-based on a need-to-know basis (see table above). The End-User only has access to their own profile and their own applications that they can access. The SE-IDaaS platform Administrators have elevated privileges depending on the type of Admin role they have and based solely on the principles of separation of duties and least privilege.

SE-IDaaS management has assigned administrative roles for role types based on existing permissions in place for the target on-premises and cloud applications.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

No. All users do not have access to all data in the system. The only users with access to other users' data are administrative users. Non-privileged users may only see data about themselves.

Application Administrators - access to all administrative features of the system depending on the scope of their administration. Permissions for Administrator roles adhere to the principle of least privilege and separation of duties so that within SE-IDaaS admins only have access to the data they require to do their job. For example, Salesforce Administrators do not have access to ServiceNow data and are not able to view the same data as Super Administrators.

Non-enterprise Users and Enterprise Users - access content that they created or content that was shared with them.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

SE-IDaaS prevents users who have access to the system from misusing data by:

- Auditing user activity based on usage of the system, tying user activity in the system to their identity.
- Controlling access over what content each user can access via roles and groups.
- Employing the principles of least privilege and separation of duties to ensure users are able to access only the information and resources that are necessary for its legitimate purpose.
- Security awareness and training policy and procedures required by the department which educate employees on policies and procedures when utilizing the IDaaS.

Access control is implemented via the secure network; authentication to the system is granted via Active Directory individual and group role membership. In addition, security tools are in place to proactively monitor subject system(s). Controls to prevent the misuse of data include mandatory cyber security training for all Department employees and contractors, privacy training, and the Department's Rules of Behavior for Protecting Personally Identifiable Information (PII).