Affects Members Of the Public? Mark if Applicable w/ an X

Department of Energy

Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: ***https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file***

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	8/4/2022
Departmental Element & Site	Office of Chief Information Officer (OCIO) – IM-64
Name of Information System or IT Project	Saviynt Identity Governance Administration (IGA) - MyIdentity
Exhibit Project UID	019-000001955
New PIA [X] **Update** [ ]	This is a new PIA

	Name, Title	Contact Information Phone, Email
System Owner	Aaron Wisner Information Technology Specialist, IM-62	(301) 903- 5247 Aaron.Wisner@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Brooke Dickson Director of Privacy Management and Compliance Office of the Chief Information Officer, IM-42	(202) 287-5786 Brooke.Dickson@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Olaleye Oluwabiyi (CONTR), ISSO	(443) 657-0833 Olaleye.Oluwabiyi@hq.doe.gov
Person Completing this Document	Olaleye Oluwabiyi (CONTR), ISSO	(443) 657-0833 Olaleye.Oluwabiyi@hq.doe.gov
Purpose of Information System or IT Project	Saviynt Identity Governance and Administration (IGA) solution also known as MyIdentity is used for managing accounts, access, and entitlements for EITS identities. MyIdentity collects data through its connectivity with OneID Global Address List (GAL), OneID Attribute Exchange Service (AES), DOEInfo, and doe.local Active Directory to establish the user's identity from authoritative sources. Connectivity is also established with Azure AD (O365), Azure AD, Microsoft Azure Government (MAG), DAYS (ServiceNow), and AWS to gain visibility into a user's access and entitlements in key target systems. MyIdentity is integrated with DAYS to implement deep ticketing and Service Catalog functionalities and replaces the current PDF System Authorization Access Request (SAAR) process with automated account provisioning. MyIdentity will provide other governance features including the ability to create access policies, certify the use of accounts and entitlements, and generate reports.	
Type of Information Collected or Maintained by the System:	☐ SSN Social Security number ☐ Medical & Health Information e.g. blood test results ☐ Financial Information e.g. credit card number ☐ Clearance Information e.g. "Q"	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address – Official/personal email, office location, primary/mobile phone number. (The following attributes are amongst those collected by the system considered to be some variation of PII: Citizenship, First Name, Middle Name, Last Name, Suffix Name, Display Name, Manager, Manager DUID, Sponsor DUID, Employee Type, Employee Category, OneID Person Type, OneID Status, Email Address, Personal Email, DOE Affiliation Level1, DOE Affiliation Level2, Org Unit Name, Org First Tier Code, Org Unit ID Title, Org First Tier Title, Department Number, Employee Organization Code, Organization Title, Personnel Status Code. Personnel Status Description, Mobile Phone, Primary Phone, Office Address 1, Office Address 2, Office Address 3, Office Address 4, Office Address City, Office Address State, Office Address Country, Office Address Zip, Office Room, Office Building, Employee Category Description, Company Name, Title, DOE Sponsor Role Flag, DOEInfo Primary Email, DOEInfo Secondary Email, DOEInfo Email3). ☐ Other
Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1, *Department of Energy Privacy Program*, defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.*	YES This is a new system and automates a process that uses PII to establish user identity from authoritative sources.
If "Yes," what method was used to verify the system did not contain PII? (e.g., system scan)	Manual Verification

Threshold Questions

MODULE I – PRIVACY NEEDS ASSESSMENT

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES
2. Is the information in identifiable form?	YES
3. Is the information about individual Members of the Public?	NO
4. Is the information about DOE or contractor employees?	YES ☒ Federal Employees ☒ Contractor Employees

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

MODULE II – PII SYSTEMS & PROJECTS	
1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	Electronic Government Act (Pub. L. 104–347, sec. 203); Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, Aug. 27, 2004; Federal Property and Administrative Act of 1949, as amended; DOE Order 206.2 Identity, Credential, and Access Management, as amended; Department of Energy Authority (42 USC Section 7101 et sequential). Technology Management Reform Act of 1996 (Pub. L. 104-106, sec. 5113).
2. CONSENT **What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**	User whose PII data is processed by the system does not have direct access to input PII data into the system where opportunity to consent or decline may be given. PII data is ingested from DOEInfo, OneID, DAYS and Azure Active Directory, and Active Directory. The authoritative User attributes are defined from DOEinfo and OneID.
3. CONTRACTS **Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?**	Contractors are involved with the design, development, and maintenance of the system. Saviynt Security Manager Identity Governance and Administration (IGA) is a FedRAMP authorized Software-as-a-Service (SaaS) cloud offering. DOE does not maintain, administer, nor have visibility into the Cloud Service Provider's underlying infrastructure hosting the provided cloud service. The individuals providing this type of information are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a. Yes. Contract clauses require the contractors to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of the DOE. Rules of Behavior are signed.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed Saviynt IGA (MyIdentity) as a low risk system for confidentiality, integrity, and availability according to the criteria set forth in Federal Information Processing Standard (FIPS) 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. MyIdentity uses information already available through OneID, DOEInfo, DAYS etc. PII attributes processed by the system are considered non sensitive in nature neither can they be aggregated to create new sensitive PII data. PII data processed by the system are limited to Official/ Personal Email, Office Location, Primary / Mobile Phone Number. (Refer to Module 1 comprehensive list). MyIdentity is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls: • Strict access control enforcement based on need-to-know • Administrative and Technical controls • Annual Privacy training While MyIdentity is not the authoritative source for the privacy data processed within its system environment and thus, impact to privacy is considered low. The focus of MyIdentity is to establish the identity of DOE Federal and Contractor systems' users through its connectivity, which does not require or encourage collection of sensitive PII and is not driven by analysis of PII.
5. SORNs **How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?** **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**	The data can be retrieved by user DOE Unique ID (DUID), which is a OneID system generated identifier. Additionally, other application specific unique identifiers might be used by to correlate users including the GUID (DOEinfo) or various forms of system IDs. All unique ids are treated as strings.

MODULE II – PII SYSTEMS & PROJECTS	
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	Data can be retrieved by user DOE Unique ID (DUID), which is a OneID system generated identifier. OPM GOVT-1 is the applicable SORN that covers this system.
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	NO
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	OneID and DOEInfo are used to establish the user's identity from authoritative sources. Active Directory (doe.local), Azure AD (O365), Azure AD (MAG), DAYS (ServiceNow), and AWS are used to gain visibility into a user's access and entitlements in key target systems.
9. Will the information system derive new or meta data about an individual from the information collected?	The system does not and will not derive new meta data considered to be PII about an individual from the information collected.
10. Are the data elements described in detail and documented?	Yes, the data elements are described in detail and documented in the IGA product configuration, Identity Repository, a MySQL user Schema.
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	The core MyIdentity services are: **Identity Management**: MyIdentity aggregates, correlates, and synchronizes authoritative identity data from key sources. MyIdentity also facilitates the reconciliation of identity data where different sources might have incomplete or inaccurate data. This establishes a complete identity record for users and reduces silos and inefficiencies in identity management. With this data MyIdentity can facilitate the onboarding of new contractors and federal employees and automate the full scope lifecycle management of these identities. MyIdentity contains several features including rules, jobs, and analytics reports which support strong identity governance. **Access Management:** MyIdentity collects data on the access privileges, and permissions which accounts are granted. Additionally, MyIdentity correlates these entitlements with individual user identities, providing deep visibility into the type of access a user has. This data is used to support additional reporting and analytics features. Furthermore, this data can used for access control policies.
12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	Not Applicable
13. With what other agencies or entities will an individual's information be shared?	None
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	MyIdentity will provide reports and analytics on identity management and access management. These reports are built within the Saviynt platform.
15. What will be the use of these reports?	Report will be used by IT administrators for the purpose of auditing identities and access and for compliance with DOE access management policies and best practices.
16. Who will have access to these reports?	MyIdentity applies strict access control procedures as described in Module I item 4 and Module II item 25-27.

MODULE II – PII SYSTEMS & PROJECTS	
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No. The system does not track the physical identity or location of individuals, nor does it monitor their personal behavior.
18. What kinds of information are collected as a function of the monitoring of individuals?	Not Applicable
19. Are controls implemented to prevent unauthorized monitoring of individuals?	No
DATA MANAGEMENT & MAINTENANCE	
20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.	Daily pulls from authoritative systems to maintain congruency and data accuracy. No human/manual interaction. Data retrieval is automatic synchronization between systems to maintain records integrity.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	The system is hosted and operated within the FedRAMP approved Saviynt SSM SaaS Cloud environment.
Records Management	

MODULE II – PII SYSTEMS & PROJECTS

22. Identify the record(s).	The Records Management office (IM-41) has recommended following DAA-GRS-2013-0006-0003 Schedule GRS 3.2 item 030 as applicable to Saviynt IGA (MyIdentity) records. System access records. These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as: •user profiles •log-in files •password files •audit trail files and extracts •system usage files •cost-back files used to assess charges for system use Exclusion 1. Excludes records relating to electronic signatures. Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement. Systems not requiring special accountability for access: These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users. DOE Business Use: Records would be destroyed one year after system access is terminated.

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. □ Unscheduled x Scheduled *(cite NARA authority(ies) below)* GRS 3.2, item 030 DAA-GRS-2013-0006-0003
24. Records Contact	Maria Levesque, 202-586-9527, Maria.Levesque@hq.doe.gov Christie Flora, 301-903-2560, Christie.Flora@hq.doe.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Technical and administrative controls are in place to prevent the misuse of data by individuals with access. These access controls are part of the Saviynt IGA (MyIdentity) and FedRAMP Saviynt Security Manager System Security Plan (SSP). All system team members (federal and contractor) are required to annually complete the Department of Energy Headquarters Annual Cyber Security Refresher Briefing and the Annual Privacy Training as a requirement for access to the system. Administrative controls include separation of duties, so individuals only have access to appropriate personal information, and use of system audit logs to monitor access and user activity in the system. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. The technical controls include restricted access with access/functional privileges to Saviynt IGA (MyIdentity) commensurate with the user's job responsibilities.
26. Who will have access to PII data?	Strictly approved administrators will have access to PII data within MyIdentity**.**
27. How is access to PII data determined?	Role-based job functions determine a Federal or Contractor employee access to the PII within MyIdentity.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	MyIdentity will write data to select systems including OneID, DAYS, Active Directory. No system has direct access to MyIdentity data.

MODULE II – PII SYSTEMS & PROJECTS	
29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	There will be interface agreement developed between Saviynt IGA (MyIdentity) and DOEInfo.
30. Who is responsible for ensuring the authorized use of personal information?	DOE Identity Access Federal Sponsor and MyIdentity System Owner
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**Aaron Wisner** (Print Name) AARON WISNER Digitally signed by AARON WISNER Date: 2022.08.31 14:08:22 -04'00' (Signature)	
Local Privacy Act Officer	**Brooke Dickson** (Print Name) Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2022.08.25 16:03:01 -04'00' (Signature)	
Ken Hunt **Chief Privacy Officer**	**Ken Hunt** (Print Name) William K. Hunt Digitally signed by William K. Hunt Date: 2022.08.24 15:56:31 -04'00' (Signature)	