Affects Members Of the Public? □

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	8/25/2023	
Departmental Element & Site	Office of the Chief Information Officer; DOE Headquarters.	
Name of Information System or IT Project	DOE At Your Service (DAYS)	
Exhibit Project UID	019-000001955	
New PIA □ **Update** ☒	Periodic update to the 4/21/2021 DAYS PNA/PIA required for yearly system assessment. Periodic update with no material changes to the system.	
	Name, Title	**Contact Information Phone, Email**
System Owner	Timothy S. Lydick Project Manager	19901 Germantown Road Germantown, MD 20874 301-903-7759 Timothy.Lydick@hq.doe.gov
Local Privacy Act Officer	Brooke Dickson Director of Privacy Management and Compliance Office of the Chief Information Officer, IM-42	1000 Independence Avenue, S.W. Washington DC 20585 202-287-5786 Brooke.Dickson@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Manda Shu-Nyamboli Information System Security Officer (ISSO) Security and Compliance Office, (IM-63)"	19901 Germantown Road Germantown, MD 20874 301-903-0102 Manda.shu-nyamboli@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Jedediah Blanks Software Developer	19901 Germantown Road Germantown, MD 20874 409-789-8554 Jedediah.blanks@hq.doe.gov
Purpose of Information System or IT Project	DAYS is the primary management information system used to support EITS. DAYS is based on the cloud ServiceNow IT service management system (SaaS model). The DAYS System contains multiple ServiceNow application instances within the ServiceNow SaaS. In addition, the DAYS environment includes four (4) ServiceNow Management, Instrumentation, and Discovery (MID) Servers hosted on Windows servers within the DOE cloud subsystem. DAYS automates IT Service Management (ITSM) functions through Information Technology Infrastructure Library (ITIL) processes and customized applications for the DOE Office of the Chief Information Officer (OCIO). The DAYS system integrates service delivery and service support functions for EITS as EITS delivers a wide range of products and services to customers throughout DOE headquarters and field sites nationwide. It supports internal EITS operations and maintenance functions and serves as a direct customer conduit for requests and reporting of incidents. Secondarily, DAYS provides employees and other systems with current IT Service delivery status and pertinent information. DAYS supports the use of DOE standard personal computers using Internet Explorer, Chrome and other JavaScript enabled web browsers as clients. DAYS contains employment PII including contact information, company, badge serial number, employee type, DOE employee ID, user GUIDs (globally unique identifiers) for Management Information System (MIS – the system used to onboard contractors and confirm their sponsorship), and certain security questions and answers. Employment PII is used for standard employment functions including to enable individuals to obtain technical support and needed equipment as well as to ascribe an asset, project, or incident to the individual. DAYS contains citizenship information which is used to verify eligibility for elevated or privileged access permissions. Citizenship data are only accessible by administrators and personnel who run the elevated access permission process.	
Type of Information Collected or Maintained by the System:	□ SSN □ Medical & Health Information □ Financial Information □ Clearance Information	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Biometric Information ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☒ Other – This system stores e-mail address, U.S. citizenship information, company, badge serial number, employee type, DOE employee ID, user GUIDs for Management Information System (MIS – the system used to onboard contractors and confirm their sponsorship), and certain security questions and answers.
Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1 Chg 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.*	The system contains PII.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Not applicable
Threshold Questions	
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

MODULE I – PRIVACY NEEDS ASSESSMENT

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. seq. Federal Property and Administrative Services Act of 1949, Section 202(b), 40 U.S.C. 483(b)
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)?**	Information is a requisite of employment and system access. PII use is limited to specified authorized purposes. DAYS is only accessible from within the DOE network. All systems on the network display a warning banner as required by DOE O 205.1C Chg 1, paragraph 4.c (11), which directs that SDM Risk Management Implementation Plans "Must require DOE and NNSA, NSS and Federal unclassified systems to display a system use notification (e.g. Warning Banner) at login and require users to electronically acknowledge the warning (such as clicking on 'OK' or 'I agree' button to proceed)."
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. Privacy Act clauses are included in their contracts.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DAYS poses a moderate privacy risk to individuals. Should PII in the system be compromised, it could cause personal and professional harm to individuals in light of the employment data in the system. Such a breach could affect the trust between employees and their employer(s) as well as between individuals and the government. The only potentially highly sensitive PII in DAYS includes citizenship information which is used to verify eligibility for elevated or privileged access permissions. Citizenship data are only accessible by administrators and personnel who run the elevated access permission process. DAYS observes a number of protocols in observance of the Fair Information Practice Principles (FIPPs) to mitigate privacy risk. DAYS collects and maintains only PII needed for authorized business purposes in contemplation of data minimization and purpose specification. DAYS utilizes GUIDs instead of SSNs to further data minimization and security. In addition, DAYS implements a series of technical and administrative controls to promote data integrity and security. These access controls are part of the DAYS 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 as a necessary requirement for access to the system. Access is limited to approved federal and contractor employees controlled by the system administrator. Administrative controls include separation of duties so individuals only have access to limited data for authorized business purposes. System audit logs are generated to monitor access and user activity in the system and to ensure that only authorized functions are performed. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. Technical controls include restricted access via unique user-id and password with access/functional privileges to DAYS commensurate with the user's job responsibilities. System passwords are stored using 128 bit encryption.

MODULE II – PII SYSTEMS & PROJECTS

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.**	Information can be retrieved by Name, Location, Extension, and Asset Tag Number.
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*.**	OPM/GOV-1, 71 FR 35341 DOE-23 Property Accountability System, 74 FR 1023 DOE-43 Personnel Security Files, 74 FR 1044
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	MyIdentity, which is an internal connection, is the source of PII that resides in DAYS. No additional PII is requested or provided by other systems.
9. Will the information system derive new or meta data about an individual from the information collected?	No.
10. Are the data elements described in detail and documented?	The data elements are contained in the database schema with field attributes contained in the MOU/MOA agreements for OneID, EERE, and Sunflower. Detailed descriptions are not maintained in DAYS as it is not the source system for these data elements.

MODULE II – PII SYSTEMS & PROJECTS

DATA USE	
11. How will the PII be used?	PII is used in the day-to-day maintenance and administration of DOE's IT infrastructure and user support. Citizenship data are used to verify eligibility for elevated or privileged access permissions.
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?**	N/A
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?	Ad hoc reports may be produced that reference an account holders' ticket history, records of their asset configuration, organizational affiliation, location, or account status relevant to DAYS or systems that receive data from DAYS.
15. What will be the use of these reports?	Ad hoc reports are generated to assess and log DOE IT Infrastructure projects, incidents and maintenance, and asset and configuration management.
16. Who will have access to these reports?	Authorized access will be limited to Help Desk, system administration, project management, and infrastructure engineering personnel with a need to know. In addition, DAYS system developers and administrative personnel will have access to the system for development and maintenance.
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	The system does not provided the capability to monitor individuals but does include work location.
18. What kinds of information are collected as a function of the monitoring of individuals?	Individuals are not monitored. Assets, projects, and incidents are monitored in this system, not individuals.

MODULE II – PII SYSTEMS & PROJECTS

19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes, the system is only accessible from within the DOE network. Access is limited to approved federal and contractor employees controlled by the system administrator. System passwords are stored using 128 bit encryption.
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.	PII is provided by MyIdentity. The account request process matches the email address provided by the user in their application to the email address on file to ensure accuracy. If the application address is different or no email address is listed by the pull from MyIdentity, the user record in DAYS is updated. The DAYS process preserves these updates and ensures that they do not get overwritten by outdated information from MyIdentity. DAYS does not collect or store information from sources outside of DOE.
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 DAYS system is a SaaS solution and can be accessed on DOE networks. The system provides a single repository containing all system information and the rules, controls, and procedures that govern access to the system are applied consistently.
RECORDS MANAGEMENT	
22. Identify the record(s).	Records within DAYS held in the form of tickets entered via the Service Desk. The primary record types in DAYS are: ASSET: information concerning hardware and software items allocated to and used by a customer CHANGE: records requests to modify or update an asset, system or process INCIDENT: records data concerning an occurrence related to the customer's ability to work or request for information related to it PROJECT: records activities associated with project tasks REQUEST: request from customer for additional or changed assets

MODULE II – PII SYSTEMS & PROJECTS

23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Disposition of records: These records are temporary records. National Archives and Records Administration Records Schedule Number: DAA-0434-2018-0001 Master File/Database DAYS and similar information technology service solutions may include, but may not be limited to, the employee/requester full name, contact phone number, business email, office of assignment, office location, request ticket number, request date and time. Disposition Instruction: TEMPORARY. Cut off in year the system is terminated, defunded or decommissioned. Destroy 3 year(s) after cutoff, but longer retention is authorized for business use. Input • GRS 5.2 item 020 recommended, but IM-60 to review and verify applicability for use retention and disposition use. Output • GRS 5.2 item 020 recommended, but IM-60 to review and verify applicability for use retention and disposition use. Documentation • GRS 3.1 item 051 recommended, but IM-60 to review and verify applicability for use retention and disposition use. Note: DAYS contains records and info that are media specific to electronic records in the service solution master file/database and may also be stored electronically on hard disks managed by a MYSQL database server or other electronic media. The records and information are/will be reportedly retained in the system for the life of the system versus migration elsewhere externally.
24. Records Contact	Troy Manigault, 301-903-9926, troy.manigault@hq.doe.gov

ACCESS, SAFEGUARDS & SECURITY

MODULE II – PII SYSTEMS & PROJECTS

25. What controls are in place to protect the data from unauthorized access, modification or use?	DAYS implements a series of technical and administrative controls to protect data from unauthorized access, modification, or use. These access controls are part of the DAYS 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 as a necessary requirement for access to the system. Access is limited to approved federal and contractor employees controlled by the system administrator. Administrative controls include separation of duties so individuals only have access to limited data for authorized business purposes. System audit logs are generated to monitor access and user activity in the system and to ensure that only authorized functions are performed. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. Technical controls include restricted access via unique user-id and password with access/functional privileges to DAYS commensurate with the user's job responsibilities. System passwords are stored using 128 bit encryption.
26. Who will have access to PII data?	Authorized access are limited to Help desk, System Administration, Project Management, and infrastructure engineering personnel, on a need to know basis. In addition, DAYS system developers and administrative personnel have access to the system for system development and maintenance.
27. How is access to PII data determined?	Access to data is determined by evaluation of personnel job roles and responsibilities and organization. Based on the evaluation, the user is assigned specific permissions according to job function that are applied using system access control lists.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes. MyIdentity allows a Java Database Connectivity (JDBC) connection from DAYS to gather user information. Sunflower and DAYS exchange information via a JDBC connection containing IT asset information. BigFix allows a JDBC connection from DAYS to gather IT asset information. EBR provides a flat file to DAYS with SGL codes for billing. EBR receives flat files from DAYS with Reports for billing data. DAYS also shares information with DOE Active Directory.

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?	DAYS has only internal connections. IM-60 does not employ ISAs for internal connections. Additional information is available in the DAYS System Security Plan (SSP) and Assessment & Authorization (A&A) Package.
30. Who is responsible for ensuring the authorized use of personal information?	The DAYS Authorizing Official as identified in the System Security Plan. Data from interfaces is covered under MOAs that include documented system security restrictions.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**Timothy Lydick** **(Print Name)** Timothy S. Lydick Digitally signed by Timothy S. Lydick Date: 2023.09.26 08:39:46 -04'00' **(Signature)**	
Local Privacy Act Officer	**Brooke Dickson** **(Print Name)** Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2023.09.22 15:23:30 -04'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	**Ken Hunt** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2023.09.21 12:21:52 -04'00' **(Signature)**	