Affects Members Of the Public? ☐

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT		
Date	4/21/2021	
Departmental Element & Site	U.S. Department of Energy (DOE) Headquarters (HQ) Office of the Chief Information Officer (OCIO) IM-63	
Name of Information System or IT Project	DOE At Your Service (DAYS)	
Exhibit Project UID	000001141 IM-60 RightPath	
New PIA ☐ **Update** X	Updated in light of personnel changes.	
	Name, Title	**Contact Information Phone, Email**
System Owner	Timothy S. Lydick Project Manager	301-903-7759 Timothy.Lydick@hq.doe.gov
Local Privacy Act Officer	Brooke Dickson-Knowles Privacy Management and Compliance IM-42	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) IM-62	301-903-0102 Manda.shu-nyamboli@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Mitchell Chin Software Developer	904-652-3979 Mitchell.chin@hq.doe.gov
Purpose of Information System or IT Project	The Department of Energy (DOE) uses a self-service portal called DOE At-Your-Service (DAYS) to enable Energy Information Technology Services (EITS) customers to order EITS services, report incidents, and check the status of service tickets for such services as, but not limited to, software installations and hardware repair and replacements. EITS uses DAYS data to monitor service requests, workloads, resource rates, request resolution time lines, and to manage associated metrics and statistics for corrective actions, forecasting, troubleshooting and related IT reporting. The DOE IT Service Management (ITSM) system functions through Information Technology Infrastructure Library (ITIL) processes and customized applications for the DOE Office of the Chief Information Officer (OCIO). The IT Service Management system is a suite of highly integrated out-of-the-box (OOB) and customized applications which automate the DOE's ITSM processes for the OCIO. The system primarily supports ITSM personnel in performing their duties to manage service requests, incidents, change management and problems. Secondarily, the system provides employees and other systems with current IT Service delivery status and pertinent information.	
Type of Information Collected or Maintained by the System:	☐ SSN ☐ Medical & Health Information ☐ Financial Information ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Other – This system stores e-mail address and U.S. citizenship information, company, badge serial number, employee type, DOE employee ID, user GUID's for MIS, and certain security questions and answers.
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.*	The system contains PII.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

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

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 State Code (U.S.C.), Section 7101 et. Seq.
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)?**	DAYS is only accessible from within the DOE network. All systems on the network display a warning banner as required by DOE 0 205.1C, 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 DAYS and are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a. Contract language states that data covered by the Privacy Act may be disclosed to contractors. Any information that is obtained or viewed shall be on a need-to-know basis. Assigned contractors are required to safeguard all information they obtain in accordance with the provisions of the Privacy Act and requirements of DOE. The contractors shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DAYS contains limited PII necessary for the administration, maintenance, and use of the system including employment and contact information. The unauthorized disclosure of PII is expected to have a moderately adverse effect on organizational operations, organizational assets, or individuals. Considering the low-to-moderate sensitivity of the PII contained in the system, a compromise of this information could cause harm to the trust between employees and employers and between individuals and the Federal Government. Because DAYS contains employment information, a compromise of this information could also cause professional harm or inconvenience to individuals. The compromise of citizenship information could result in additional professional or personal harm. Technical and administrative controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of DAYS from being compromised. Citizenship information is only viewable by system administrators and is not routinely retrieved. Please see the "ACCESS, SAFEGUARDS & SECURITY" section for additional information relating to system data protection.
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.**	Service requests and other related tasks can be retrieved by an identifier such as an associated customer's name, location, extension, and asset tag number. The use of these identifiers is to facilitate the services mentioned within the purpose section of this PIA and are not used to retrieve any additional PII.
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 • DOE-5 Personnel Records of Former Contractor Employees • DOE-2 Supervisory Maintained Personnel Records • DOE-11 Emergency Locator Records • DOE-28 General Training Records Additional information regarding DOEInfo, the primary data source system for DAYS, may be found within its own PIA.

MODULE II – PII SYSTEMS & PROJECTS	
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?	PII necessary to the maintenance and use of DAYS is obtained primarily from DOEInfo as well as BigFix and Sunflower. No additional information is requested in order to use DAYS beyond service and asset information. Note that citizenship information is carried over from DOEInfo but is not routinely retrieved or used in DAYS; only system administrators have the ability to view this information.
9. Will the information system derive new or meta data about an individual from the information collected?	DAYS does not derive new data or create previously unavailable data about an individual through aggregation from the information collected.
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 DOEInfo, BigFix, and Sunflower. Detailed descriptions are not maintained in DAYS as it is not the source system for these data elements.
DATA USE	
11. How will the PII be used?	DAYS is an asset management and Help Desk tool; accordingly, PII will only be used when necessary to facilitate the day-to-day maintenance and administration of DOE's IT Infrastructure and user support. Citizenship information is used exclusively in connection with on-boarding requests for foreign nationals to help facilitate the process by which they may obtain equipment and access according to DOE policies and procedures.
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

MODULE II – PII SYSTEMS & PROJECTS	
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 holder's 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 used for the maintenance and security of the system. More specifically, these reports are generated to assess and log DOE IT Infrastructure projects and incidents and for asset and configuration management.
16. Who will have access to these reports?	Only authorized DOE Federal and contractor personnel have access to the reports in the system. Authorized access is limited to Help Desk, system administrators, 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?	DAYS is not designed to monitor individuals. DAYS does contain employees' work locations in relation to service requests and installations.
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A.
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	

MODULE II – PII SYSTEMS & PROJECTS

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.	DAYS does not verify the accuracy or completeness of the DOE federal and contractor data in the system. The data in the system is provided by DOEInfo, BigFix, and Sunflower. Please reference the existing PIAs for those systems for additional information. Our account request process does attempt to match the email address provided by the user in their application to the email address that we have on file for them. If the application address is different or no email address is listed by the pull from DOEInfo, the user record in DAYS is updated. Our process preserves these updates, and ensures that they do not get overwritten by outdated information from DOEInfo. 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 Software-as-a-Service (SaaS) cloud solution which can be accessed on any DOE network. 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, regardless of the access site.
RECORDS MANAGEMENT	
22. Identify the record(s).	Records within DAYS held in the form of tickets entered via the Service Desk. Record types include: • ACTION ITEM: records tasks requested and assigned to a DAYS user • 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 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 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?	Technical and administrative controls are in place to prevent the misuse of data by individuals with access. 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 DOE Headquarters Annual Cyber Security Refresher Briefing as a necessary requirement for access to the system. Administrative controls include separation of duties so individuals only have access to appropriate PII as well as the use of system audit logs to ensure the security and integrity of the system. Rules of behavior and consequences for violating the rules are displayed to the user at each log-on. Technical controls include restricted access via unique user ID and password with access/functional privileges to DAYS commensurate with the user's job responsibilities.
26. Who will have access to PII data?	Authorized DOE Federal and contractor personnel will have access to data in the system. 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 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 permissions that are applied using system access control lists.

MODULE II – PII SYSTEMS & PROJECTS	
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Yes. DOElnfo allows a 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. EITS Business Reporting (EBR) provides a flat file to DAYS with Standard General Ledger (SGL) codes for billing. EBR receives flat files from DAYS with Reports for billing data. DAYS also shares information with DOE Active Directory for log-on purposes.
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 are MOAs/ISAs between the DOElnfo, Sunflower, BigFix and DAYS System Owners. Additional information is available in the DAYS SSP and AA 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)** _____ **(Signature)**	_____
Local Privacy Act Officer	**Brooke Dickson** **(Print Name)** Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2021.05.03 18:09:13 -04'00' _____ **(Signature)**	_____
Ken Hunt **Chief Privacy Officer**	**Ken Hunt** **(Print Name)** WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2021.05.03 16:50:02 -04'00' _____ **(Signature)**	_____