Affects Members Of the Public?

Department of Energy

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	04/22/2024
Departmental Element & Site	HC
Name of Information System or IT Project	Workday Government Cloud
Exhibit Project UID	
New PIA [X] **Update** [ ]	

	Name, Title	Contact Information Phone, Email
System Owner	Letitia Lawson Program Manager	240-848-0013 Letitia.lawson@hq.doe.gov
Local Privacy Act Officer	Brooke Dickson Privacy Management and Compliance Officer / DOE IM-42	202-287-5786 Brooke.dickson@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Lamont Void Information System Security Officer	253-495-1596 Lamont.void@hq.doe.gov
Person Completing this Document	Greg Siegel Workday Project Program Manager	Gregory.siegel@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Purpose of Information System or IT Project	DOE is implementing the Workday SaaS solution in 4 phases: (1) Core HCM (2) Learning (3) Performance Management (4) Time and Attendance This initial PIA covers the first phase and will be updated as each subsequent phase is implemented. Workday will become the official Human Resources system of record for DOE, replacing CHRIS and other ancillary HR systems. The system will officially track the DOE employee lifecycle and will document notifications of personnel actions, an employee's learning history, performance management, and timekeeping. During the initial conversion process historical information is used to build individual employee profiles by migrating data from DOE's legacy HR System "CHRIS". Workday HCM allows for the processing of personnel transactions related to: hiring and onboarding, termination, retirement and calculation of retirement benefits, promotion, awards and compensation, employment status, pay and leave calculation, benefits enrollment and administration, which includes the assignment of beneficiaries and dependents and the calculation of benefits eligibility, organization assignments, and time and attendance administration including the calculation of leave eligibility. This information is also used for strategic workforce reporting. For beneficiaries and dependents of DOE employees, information is collected to properly administer benefits provided by the DOE. For emergency contacts, this information is collected to contact an individual on a DOE employee's behalf in case of an emergency. Workday provides a feature whereby Workday Customers can download and analyze activity performed by users in their Workday Government Cloud tenant. Workday provides an add-on for Splunk to enable aggregation of the user activity logging to an organization's security information and event management (SIEM) or security operations center (SOC). The system implements a number of processes and controls to protect data and mitigate privacy risk, further discussed in Module II.
Type of Information Collected or Maintained by the System:	Name; SSN; contact information (including home and work address); home and work telephone numbers; mobile telephone numbers; work email address; marital status; ethnicity; citizenship information; military service information; date of birth; gender; disability information; employee identification information; education, licenses and certification information; probation period and employment duration information; job or position title; business title; job type or code; business site; supervisory, work schedule and status (full-time or part-time, regular or temporary); compensation and related information (including pay type and information regarding raises and salary adjustments); payroll information; allowance, bonus, leave of

MODULE I – PRIVACY NEEDS ASSESSMENT

	absence information; employment history; work experience information; accomplishment information; training and development information; award information.
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.*	PII exists.
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?	Only DOE 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?**	5 USC §§ 4115, 4117, and 4118 and Executive Order (EO) 11248. EO 11248 assigns additional responsibilities to OPM for planning and promoting the development, improvement, coordination, and evaluation of training in accordance with 5 USC Chapter 41 and policy set forth in the Executive Order. Additional authorities for sharing, leveraging, and acquiring shared services are contained in the Economy Act, 31 USC § 1535 and Federal Acquisition Regulation 17.5 and the Revolving Fund, 5 USC § 1304(e). 5 USC § 301 - Departmental regulations. 5 CFR Part 293 – Personnel Records 5 CFR Part 294 – Availability of Official Information 5 CFR Part 297 – Privacy Procedures for Personnel Records 5 CFR Part 831 – Retirement 5 CFR Part 841 – Federal Employees Retirement System 5 CFR Part 850 – Electronic Retirement Processing P.L. 106-65, "National Defense Authorization Act [Section 3212(d)], enacted October 1999; 42 USC § 7101 et. Seq. The Cybersecurity Information Sharing Act of 2015 (“CISA”) requires the Director of National Intelligence and the Departments of DHS, Defense, and Justice to develop procedures to share cybersecurity threat information with private entities, nonfederal government agencies, state, tribal, and local governments, the public, and entities. under threats.

MODULE II – PII SYSTEMS & PROJECTS	
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)?**	Individuals have two opportunities to decline to provide information: 1) All visitors to the portal will see the following system use / warning banner which states that logging in is equivalent to providing consent. An individual may choose not to log into the system. **WARNING**WARNING**WARNING**WARNING** This is a Department of Energy (DOE) computer system. DOE computer systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DOE computer systems to appropriate authorities. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF INFORMATION. 2) DOE will decide which PII is loaded into their Workday Government Cloud tenant. The data uploaded will depend on the features that DOE chooses to use and the populations that they choose to upload into the system.
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 in this design, development and maintenance of the system and the appropriate clauses were included in their contracts.

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The system has a FIPS moderate categorization. The compromise of PII contained in the system would have a serious impact to individuals' privacy in light of the sensitive PII contained in the system including SSN, citizenship data, disability information, and financial information. Should this information be compromised, it could cause significant harm to individuals including professional harm, social harm including embarrassment, financial harm, and it could damage the trust between individuals and their employer. The system observes the Fair Information Practice Principles (FIPPs) in order to protect individuals' information privacy. The system contains only the PII necessary for specified, authorized business purposes in furtherance of data minimization and purpose specification. PII is not used for unauthorized purposes in furtherance of use limitation. Data quality and security are protected via a number of technical and administrative controls. Access to PII for Workday Customer Support and Development Operations is subject to a number of criteria: 1. Their Customer Support role 2. Completion of mandatory role-specific security and privacy training 3. Use of a specific set of secure technology including end-point equipment, access via a Virtual Clean room (i.e., secure computers or virtual desktops) and use of multi-factor authentication. 4. Approval of access by management in either Customer Support or Operations management.
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.**	PII may be retrieved by employee data points including employee ID.

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*.**	OPM GOVT-1, General Personnel Records, Nov 30, 2015, 80 FR 74815 OPM/GOVT-2 Employee Performance File Systems Records, November 30, 2015, 80 FR 74815 OPM/GOVT-3 Records of Adverse Actions, Performance based Reduction in Grade and Removal Actions, and Termination of Probationers, Nov 30, 2025, 80 FR 74815 OPM/GOVT-5 Recruiting, Examining and Placement Records, Dec 1, 2021, 86 FR 68291 OPM/GOVT-7 Applicant, Sex, National Origin and Disability Status Records, Nov 30, 2015, 80 FR 74185 OPM/GOVT-9, File on position classification appeals, job grading appeals, and retained grade or pay appeals, and fair labor standard act (FLSA) claims and complaints, Nov 30, 2015, 80 FR 74815 DOE-2, DOE-Personnel Supervisor Maintained Personnel Records, Jan 9, 2009, 74 FR 999 DOE-13, Payroll and Leave Records, Jan 9, 2009, 74 FR 1012
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	

MODULE II – PII SYSTEMS & PROJECTS	
8. What are the sources of information about individuals in the information system or project?	Any data that is populated into the authorization boundary will either be added by the Workday customer directly into their Workday Government Cloud tenant or populated into their Workday Government Cloud tenant using integrations or other data flows that have been configured by the Workday customer or by a party engaged by the Workday customer. For the initial migration, data is transferred from the legacy system, CHRIS. Data that is typically required for human capital includes data on employees, beneficiaries and dependents.
9. Will the information system derive new or meta data about an individual from the information collected?	Workday will be used as DOE's primary system for processing HR transactions for employees and will derive new or meta data about an individual for authorized HR purposes including the calculation of benefits eligibility and various administrative employee functions.
10. Are the data elements described in detail and documented?	Data elements are described as part of the FEDRAMP authorization for the Workday Government Cloud and within the DOE Moderate ATO authorization.
DATA USE	
11. How will the PII be used?	Workday HCM allows for the processing of personnel transactions related to: hiring and onboarding, termination, retirement and calculation of retirement benefits, promotion, awards and compensation, employment status, performance rating, pay and leave calculation, benefits enrollment and administration, which includes the assignment of beneficiaries and dependents and the calculation of benefits eligibility, organization assignments, and time and attendance administration including the calculation of leave eligibility. This information is also used for strategic workforce reporting. For beneficiaries and dependents of DOE employees, information is collected to properly administer benefits provided by the DOE. For emergency contacts, this information is collected to contact an individual on a DOE employee's behalf in case of an emergency.

MODULE II – PII SYSTEMS & PROJECTS	
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?**	Derivative data will be used for administrative HR purposes including the calculation of benefits eligibility, employment decisions, and other HR transactions.
13. With what other agencies or entities will an individual's information be shared?	Defense Finance Accounting Service (DFAS) - This is DOE's payroll provider. Office of Personnel Management (OPM) - For regulatory reporting purposes.
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	There are extensive reports with employment, HR and personal information, and dependent information produced in Workday.
15. What will be the use of these reports?	These reports will be used by HR professionals to monitor all the HR transactions processed in Workday and for regulatory reporting purposes.
16. Who will have access to these reports?	All HR professionals accessing Workday will have access to these reports but they will only be able to see information about employee populations based on user role and permissions.
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Workday will have a record of employees' work location and home address. The system will not provide the capability to monitor individuals.
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. All baseline security controls have been implemented and tested as appropriate to the FIPS categorization by the Workday CSP and by DOE in accordance with the Senior DOE Management Program Cybersecurity Plan (PCSP) and DOE directives.

MODULE II – PII SYSTEMS & PROJECTS	
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.	Individuals and HR professionals may view and correct PII to maintain accuracy and currency. Workday uses non-destructive updates, which means data is never overwritten unless specifically purged, and is maintained for the lifetime of the Workday Customers Workday Government Cloud tenant. However, Workday provides its Customers with features to allow the Customer to purge personal data records in line with the Customer's own retention requirements. DOE is currently reviewing data purging options within Workday. When the data purging solution is implemented, the following record retention periods will be in effect for the following data: • Payroll records. • Time and attendance. • Office Personnel Folder (OPF). Until a solution is developed, the data will be retained indefinitely. This PIA will be updated once a final decision has been rendered by 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 system is a SAAS and will be operated in the FEDRAMP authorized Amazon Web Services (AWS) U.S. East and U.S. West regions.
RECORDS MANAGEMENT	
22. Identify the record(s).	GRS 2.2 Notifications of personnel actions. (FEDERAL ONLY) Copies of Standard Form 50, documenting all individual personnel actions such as hiring, promotions, transfers, and separation. Includes chronological files, fact sheets, general correspondence, and forms about pending personnel actions maintained by agency Human Resources offices. Exclusion: SF-50s filed in the OPF. Items 040 and 041 of this schedule cover these records.

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Scheduled: DAA-GRS- 2017-0007- 0006
24. Records Contact	Carmen Norris, Carmen.Norris@hq.doe.gov, 240-805-8998
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	IM has implemented and tested all baseline security controls appropriate to its FIPS MODERATE categorization in accordance with the Senior DOE Management PCSP and DOE Directives. Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The technical controls include restricted access based on user responsibility and job function. Those with elevated access to perform functions on employee records besides themselves, have to complete a user request form and be granted special access. Additionally, unique username/password, PIV Card via SSO is also in place to ensure unauthorized access.
26. Who will have access to PII data?	HR Professionals System Administrators DOE Employees and Supervisors DOE prioritizes security at every level of organization. Access to the information maintained in WGC is limited to authorized users, which consists of DOE employees and contract workers who access the information on a need-to-know basis. Access to the information is restricted to that which is required in the performance of the user's duties.
27. How is access to PII data determined?	User access to data is restricted by the level of security provided to the specific user role and specific employee populations. Workday has the capability to segment access to data.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	Workday serves as a primary source of data to other existing systems such as DFAS (Payroll Provider), DOE Info (Data/Reporting Platform) and OPM systems for HR processing and regulatory reporting.

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?	No ISA exists at this time.
30. Who is responsible for ensuring the authorized use of personal information?	The information system owner is responsible for ensuring the authorized use of personal information.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**Letitia Lawson** **(Print Name)** Letitia L. Lawson Digitally signed by Letitia L. Lawson Date: 2024.04.30 16:56:43 -04'00' **(Signature)**	
Local Privacy Act Officer	**Brooke Dickson** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2024.04.26 11:49:27 -04'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	**(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2024.04.26 11:49:42 -04'00' **(Signature)**	