Affects Members Of the Public?	

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:
http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf
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	May 31, 2023
Departmental Element & Site	Office of the Chief Financial Officer, Headquarters
Name of Information System or IT Project	Corporate Human Resources Information System (CHRIS)
Exhibit Project UID	019-000000122
New PIA ☐ **Update** ☒	This is an annual update for the PIA. An updated PIA for this system will be submitted to the Chief Privacy Officer for review within twelve (12) months. This PIA was updated with the additions of NNSA, FEHB, eOPF and TSP.

	Name, Title	Contact Information Phone, Email
System Owner	Erika L. Johnson Office of Corporate Information Systems, CF-40, Germantown, U.S. Department of Energy	(240) 562-1861 erika.johnson@hq.doe.gov
Local Privacy Act Officer	Ana Manchester Office of Corporate Information Systems, CF-40, Germantown, U.S. Department of Energy	301-903-9360Ana.manchester@hq.doe.gov
Cyber Security Expert reviewing this document (e.g., ISSM, CSSM, ISSO, etc.)	Lee M. Canda Office of Corporate Information Systems, CF-40 Germantown, U.S. Department of Energy	(301) 903-2077 Lee.Canda@hq.doe.gov
Person Completing this Document	Erika L. Johnson Office of Corporate Information Systems, CF-40, Germantown, U.S. Department of Energy	(240) 562-1861 erika.johnson@hq.doe.gov

PRIVACY PROGRAM

MODULE I – PRIVACY NEEDS ASSESSMENT	
Purpose of Information System or IT Project	The CHRIS system is a major application supporting HR Management throughout all of the DOE. This system addresses the entire Federal enterprise with functionality designed specifically to meet government requirements including support for the following: • Personnel Actions Request (PAR) processing - supports the Standard Form (SF)-52 and SF-50 that officially documents an employee's Federal service history to include, but not limited to employee appointments, reinstatements, transfers, promotions, separations, etc. • Workflow – electronic approvals for HQ and Recruit personnel actions. • Position Management – personnel data in CHRIS is managed by position rather than employee. In driving the system by position, data is attached to positions to move employees in and out of those positions. Data specific to each position is used as the basis for organizational planning, recruitment, and career planning. Salary Administration maintains up-to-date DOE pay plans and associated pay tables to support locality pay, pay adjustments, allowances, differentials, premium pay, and the National Nuclear Security Administration's (NNSA) pay banding structure. • Performance Management documents performance ratings and supports tracking monetary and non-monetary awards (time-off), and quality step increases. Benefits Administration supports processing benefits elections for Federal Employee Helathcare Benefit (FEHB), Thrift Savings Plan (TSP) and electronic Official Personnel Folders (eOPF). Employee and Notification of Personnel Actions (SF-50) files are transferred weekly from the CHRIS/PeopleSoft database to the eOPF servers owned by OPM and physically located in Denver, CO. These files ensure that employee data, as well as all SF- 50 actions, are kept up to date in each employee's eOPF. They are transferred weekly via a secure Virtual Private Network (VPN). This is in direct support of the e-Government Act of 2002 (Public Law 107-347). • Labor Management and Employee Relations Tracking. • Standards of Conduct - identifies occupational series required to file financial disclosure forms. • Telework/Remote Work tracking for position designations and employee telework agreement type.
Type of Information Collected or	☒ Social Security Number (SSN) ☐ Medical & Health Information ☒ Financial Information (Salary, Cash Award Amounts) ☐ Clearance Information ☐ Biometric Information

MODULE I – PRIVACY NEEDS ASSESSMENT

Maintained by the System:	☐ Mother's Maiden Name ☒ Date of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☐ 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.*	N/A	
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. CHRIS does not continue to collect information on employees or contractors after separation from DOE.	
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.

PRIVACY
P R O G R A M

MODULE I – PRIVACY NEEDS ASSESSMENT

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

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.
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)?**	The information in the CHRIS system is required for individuals to be employed by DOE. This information is necessary in order for DOE to properly pay and administer benefits to employees, and track performance.

PRIVACY
PROGRAM

MODULE II – PII SYSTEMS & PROJECTS	
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 and development of the system and will be involved with the maintenance of the system. Personal information may be disclosed to contractors in performance of their contract. Individuals provided this information are subject to the same limitation 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. Contractors are required to safeguard all information they may obtain in accordance with the provisions of the Privacy Act and the requirements of DOE. The contractor shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling by assigned personnel.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed CHRIS as a moderate-risk systems according to the criteria set forth in Federal Information Processing Standard 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. CHRIS 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 • Technical controls • Administrative controls • System reviews The unauthorized disclosure of information is expected to have adverse effect on organizational operations, organizational assets, or individuals. DOE recognizes there are risks involved with all Information Technology systems and the steps that are later described in this document have been taken to limit access and secure the CHRIS.

PRIVACY
PROGRAM

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.**	Data may be retrieved by name, employee id, social security number, or organization.
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*.**	The system operates under the following Privacy Act systems of records: • OPM – Govt-1 General Personnel Records • DOE – 2 DOE-Personnel Supervisor Maintained Personnel Records • DOE - 3 Employee Concerns Program Records • DOE – 28 General Training Records
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	The current Systems of Records Notices do not require amendment or revision.
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	The information is provided by the employee.
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?	Yes, data elements are described in the CHRIS Users Manuals.
DATA USE	
11. How will the PII be used?	The CHRIS system is a major application supporting HR Management throughout all of the DOE. PII data maintained is required by OPM for identification, payroll and reporting purposes.

PRIVACY PROGRAM

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?**	N/A
13. With what other agencies or entities will an individual's information be shared?	OPM. Employee and Notification of Personnel Actions (SF 50) files are transferred weekly from the CHRIS/PeopleSoft database to the eOPF servers owned by OPM and physically located in Denver, CO. These files ensure that employee data, as well as all SF 50 actions, are kept up to date in each employee's eOPF. They are transferred weekly via a secure Virtual Private Network (VPN). This is in direct support of the e-Government Act of 2002 (Public Law 107-347).
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	The system allows authorized DOE Human Resources (HR) staff to produce reports on individuals or groups of individuals. The following reports may be produced by authorized HR staff: • Alpha List of Active Employees • Awards Report • Bargaining Unit Employees • Organization (Profile) Report The reports listed above contain no personal information other than employee name. Birth date and SSN were removed from all HR reports in 2015. Users can generate reports via Query Manager; these reports could potentially contain birth date and SSN since N_DOE_EMPLOYEES includes both. The details of these reports are defined in the CHRIS User's Manual.
15. What will be the use of these reports?	These reports will be used only to perform required Human Resource functions and activities.
16. Who will have access to these reports?	System Administrators, HR Project Administrators, HR users, and Personnel Offices.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	For limited use of security purposes system audit logs are maintained to record system activity and user activity.
18. What kinds of information are collected as a function of the monitoring of individuals?	For security purposes system audit logs are maintained to record system activity and user activity. This activity includes invalid logon attempts and access and modification to data in the system.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	CHRIS has established policies and procedures for controlling and monitoring access to the system. These are defined in the Security Plan and are compliant with privacy controls in NIST 800-53, rev 4.

PRIVACY
P R O G R A M

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.	Data in the CHRIS system concerning DOE federal employees goes through workflow approval processes to ensure accuracy, completeness, and appropriate management approvals.
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 maintained in Microsoft Azure Cloud located in Virginia; however, DOE employees from across the Department who are responsible for the management and operation of the system may access the system via the DOE Network or Virtual Private Network (VPN) connection.
Records Management	
22. Identify the record(s).	Records relating to employee hiring, management and personnel actions, compensation and benefits, separation, and training.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	The records in CHRIS have not yet been scheduled electronically but would fall under: Employee Acquisition Records: GRS 2.1, items 010, 020, 030, 040, 050, 110, and 111 Employee Management Records: GRS 2.2, items 020, 030, 040, 050, 060, 070, 072, 100, and 110 Employee Compensation and Benefits Records: GRS 2.4, items 010, 020, 070, 090, 140, and 141 Employee Separation Records: GRS 2.5, items 010, 011, 020, 040, 050, and 051 Employee Training Records: GRS 2.6, items 010, 020, and 030
24. Records Contact	Sean Kennedy, Records Manager sean.kennedy@hq.doe.gov (240) 315-6772
ACCESS, SAFEGUARDS & SECURITY	

PRIVACY PROGRAM

MODULE II – PII SYSTEMS & PROJECTS	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Through CF's Assessment and Accreditation program and annual assessment processes, all baseline security controls have been implemented and tested as appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. The system was certified and accredited with full Authority to Operate and found to have mitigated risk to an acceptable level. 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. These access controls are defined in the system security plan. All system team members (Federal and contractor) are required to take the DOE standard cyber security certification course as a necessary prerequisite for the system access. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. Administrative controls include non-disclosure agreements, separation of duties so individuals only have access to appropriate pieces of personal information, and use of system audit logs to monitor access and user activity in the system.
26. Who will have access to PII data?	System Administrators, HR Project Administrators, HR users, and Personnel Offices.
27. How is access to PII data determined?	Authorized DOE HR staff is provided access based on role and responsibility in order to perform required HR functions and activities. System Administrators and help desk staff have access to all data in the system in order to maintain the system and assist users with issues and problems.

PRIVACY PROGRAM

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, the CHRIS system interfaces with OPM and the following DOE systems: Internal to DOE • ESS – provides CHRIS system Thrift Savings Plan data, education, competency, emergency contact, disability, and ethnic origin information. • DOEInfo –provides CHRIS system email, home address, LWOP (Leave Without Pay) data and receives Thrift Savings Plan data, education, competency, emergency contact, disability, and ethnic origin information from CHRIS. • ePerformance – Receives basic employee data from CHRIS to populate the employee table in ePerformance and to validate the employee status and organization relationship. Receive Reports To data from ePerformance. • DPP – Provides data needed for Payroll to DPP. External to DOE • OPM – receives EHRI and Benefit information from CHRIS system • Learning Nucleus – provides training course completion data to CHRIS.
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?	Yes, for external systems only.
30. Who is responsible for ensuring the authorized use of personal information?	The System Owner, the Chief Financial Officer, and the Director for Corporate Business Systems.
END OF MODULE II	

SIGNATURE PAGE

PRIVACY P R O G R A M

	Signature	Date
System Owner	_____ ____ **Erika L. Johnson**_____ (Print Name) _____ (Signature)	_____
Local Privacy Act Officer	_____ **Ana Manchester**_____ (Print Name) _____ (Signature)	_____
Chief Privacy Officer	_____ **W. Ken Hunt**_____ (Print Name) _____ (Signature)	_____

PRIVACY
PROGRAM