Affects Members Of the Public? ☐

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	August 10, 2021
Departmental Element & Site	Office of Environment, Health, Safety and Security Office of Resource Management Office of Information Management DOE Germantown Computer Center (CA007) Germantown, MD
Name of Information System or IT Project	AU Reporting Databases and Systems (RDS)
Exhibit Project UID	019-10-01-22-02-3015-00
New PIA ☐ **Update** X	This is an update to the RDS PIA dated November 15, 2015. RDS has since become a cloud-based system managed by EITS.

	Name, Title	Contact Information Phone, Email
System Owner	Helen Heupel System Owner	301-903-9031 Helen.Heupel@hq.doe.gov
Local Privacy Act Officer	Raymond Holmer, Director AU Authorizing Official (AO) Director, Office of Information Management (AU-72)	301-903-7325 Raymond.Holmer@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Shawn Pastor Contractor to the DOE Edgewater Federal Solutions	202-735-7320 Shawn.Pastor@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Krystal Harne AU Cyber Security Point of Contact AU-72	301-903-8283 Krystal.Harne@hq.doe.gov
Purpose of Information System or IT Project	The Department of Energy's (DOE) Office of Environment, Health, and Security Office of Information Management (EHSS) uses Reporting Databases and Systems (RDS) to support its mission to provide reporting services technology that securely allows users to submit and perform reporting duties in accordance with DOE Order 231.1B Admin Chg 1, Environment, Safety and Health Reporting. The RDS enclave is a collection of applications that fall under a FIPS 199 security category of MODERATE. All information in RDS is unclassified. The applications are hosted by the DOE OCIO within the AWS Cloud and operated by the Energy IT Services (EITS) Data Center and System Services (DC&SS) team. RDS contains the following applications which support various EHSS business processes and operational needs: <u>Operational Incident Reporting and Tracking:</u> **Computerized Accident/Incident Reporting System (CAIRS)** is used to collect and analyze DOE and DOE contractor reports of injuries, illnesses, and other accidents that occur during DOE operations in accordance with DOE Order 231.1B Admin Chg 1, Environment, Safety and Health Reporting. CAIRS contains sensitive personally identifiable information (PII) and personal health information (PHI) which is used to satisfy the recording and reporting requirements of 29 CFR 1904, RECORDING AND REPORTING OCCUPATIONAL INJURIES AND ILLNESSES. **Occurrence Reporting and Processing System (ORPS)** provides a way to prepare, submit, update, and sign occurrence reports as required by DOE Order 232.2, Occurrence Reporting and Processing of Operations Information, which promotes awareness of events that could adversely affect the health and safety of the public or the workers, the environment, DOE missions, or the credibility of the Department. ORPS is used to identify corrective actions that will prevent recurrence. **The Health and Safety Issue Tracker (HSIT)** allows DOE employees and contractors to raise concerns relating to the environment, safety, health, or management of DOE operations without fear of reprisal. Administrative PII is used to manage concerns submitted by employees regarding health or safety. **Response Line (RL)** is an application that is managed by the Office of Worker Safety and Health Policy, AU-11. It provides responses to questions for DOE and DOE contractor personnel regarding worker safety and health requirements and guidance.	

MODULE I – PRIVACY NEEDS ASSESSMENT

Lessons Learned (LL) is a database used to prevent the recurrence of significant adverse safety events/trends by facilitating the sharing of performance information, lessons learned, and good practices across the DOE complex.

Fire Protection (FP) allows sites to report site fire protection information pertaining to the DOE complex in accordance with DOE Order 440.1B Chg 1, Worker Protection Program for DOE (Including the National Nuclear Safety Administration) Federal Employees, DOE Order 420.1C, Facility Safety, DOE Order 436.1 Departmental Sustainability, DOE Order 151.1C, Comprehensive Emergency Management System, DOE Order 231.1B Admin Chg 1, Environment, Safety and Health Reporting, and DOE Order 360.1C, Federal Employee Training.

Health and Safety:

Safety Basis Information System (SBIS) supports the Nuclear Safety Management Rule (10 CFR 830) requirements for DOE contractors and operators. Authorized users will use the application to update or review Safety Basis information for Nuclear Facilities.

Radiological Source Registry and Tracking (RSRT) is a DOE database that supports Department of Energy DOE Order 231.1B Admin Chg 1, Environment, Safety and Health Reporting, which identifies the requirements for centralized inventory and transaction reporting for radioactive sealed sources.

Financial Management:

The Electronic Fund Administration System (EFAS) is used by internal HQ DOE Budget Analysts, Procurement Analysts, and Budget Management staff to perform financial procurement functions in support of HQ DOE operational and administrative activities.

Document Repository and Secure Document Transfer:

Secure Electronics Records Transfer (SERT) provides DOE, the Department of Labor (DOL) and the National Institute for Occupational Safety and Health (NIOSH) a secure, efficient means to transfer medical and work-related documents in support of the Energy Employees Occupational Illness Compensation Program Act (EEOICPA). The intent of SERT is to establish a secure method to transmit electronic records between three different government agencies. The use of SERT enables DOE to automate and better manage a pre-existing process in a more secure and efficient manner. SERT also serves as a repository for documents containing PII and PHI relevant to an EEOICPA claimant's application. PII will be used for claim management.

MODULE I – PRIVACY NEEDS ASSESSMENT

DOL administers the EEOICPA program. To apply for the program, a claimant must sign a release form authorizing DOL to request their information from DOE. DOE and DOL have entered into a Memorandum of Understanding (MOU) and part of that MOU stipulates that DOL will not request information from DOE unless the claimant has signed the release. If the claimant does not consent to DOE sharing their information, they have the option not to sign the release when applying to the program.

Application	PII?	Sensitivity	Type
Computerized Accident/Incident Reporting System (CAIRS)	Yes	Sensitive	Name, Email, Phone number, Address, Social Security Number, date of birth, medical information
Secure Electronic Records Transfer (SERT)	Yes	Sensitive	Name, Email, Phone number, Social Security Number, Address, Date of birth, medical information
Occurrence Reporting and Processing System (ORPS)	Yes	Non-sensitive	Name, Email, Phone number, address
Electronic Fund Administration System (EFAS)	Yes	Non-sensitive	Name, phone number, address, email
DOE Operating Experience Program (OPEXShare)	Yes	Non-sensitive	Name, phone number, email
Worker Safety & Health Policy Clarification Portal (PC Portal)	Yes	Non-sensitive	Name, phone number, email
Radiological Source Registry and Tracking (RSRT)	Yes	Non-sensitive	Name, phone number, address, email

MODULE I – PRIVACY NEEDS ASSESSMENT

Safety Basis Information System (SBIS)	Yes	Non-sensitive	Name, phone number, email
MicroStrategy Dashboards	No	N/A MicroStrategy provides Dashboards for CAIRS and ORPS and does not generate or maintain its own separate PII.	N/A
Health and Safety Issue Tracker (HSIT)	Yes	Non-sensitive	Name, email
Fire Protection (FP)	Yes	Non-sensitive	Name, phone number, address, email
Lessons Learned (LL)	Yes	Non-sensitive	Name, phone number, address, email

PII in RDS is protected by a number of controls. The information types and system inventory within the authorization boundary of RDS meet mission and support impact requirements as defined by Section 5, NIST SP 800-60 Rev 1. RDS has been assigned an overall security categorization of Moderate during the FIPS 199 categorization process. Additionally, some information processed by RDS is Sensitive But Unclassified (SBU)/OUO etc. RDS has its own Active Directory that is separate from the DOE HQ LAN Active Directory. RDS operations personnel implement access control groups within the RDS Active Directory to control access for each application and each user in furtherance of the security and integrity of the system. The RDS system undergoes a yearly assessment of its Authorization Boundary and its applications from a security controls perspective as well as an Authority to Operate (ATO) from the Authorizing Official (AO) every three years.

Type of Information Collected or

☒ SSN Social Security number

MODULE I – PRIVACY NEEDS ASSESSMENT

Maintained by the System:	☒ Medical & Health Information ☒ Financial Information ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☒ DoB, Place of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☐ Other – Please Specify

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.*	Some applications in the RDS enclave contain sensitive PII. Some RDS applications contain non-sensitive PII (username, email, and phone number) for administrative purposes.
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?	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ 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?**	• 42 U.S.C. 7101–7385, Department of Energy Organization Act • 42 U.S.C. 5801–5911, Energy Reorganization Act of 1974 (ERA), 42 U.S.C. 5801–5911 • 42 U.S.C. 2011, Atomic Energy Act of 1954, as amended, (AEA) 42 U.S.C. 2011 • Title 10 CFR part 820 • 29 U.S.C 651 et seq., Occupational Safety and Health Act • 29 CFR 1904, Recording and Reporting Occupational Injuries and Illnesses • 29 CFR 1960, Basic Program Elements for Federal Employee Occupational Safety and Health Programs and Related Matters • 10 CFR 851, Worker Safety and Health. Specifically, 10 CFR 851.26 Record Keeping and Reporting ensures that the work-related injuries and illnesses of its workers and subcontractor workers are recorded and reported accurately and consistent with DOE Order 231.1B Admin Chg 1, Environment, Safety and Health Reporting.
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)?**	Only two applications in RDS, CAIRS and SERT, contain sensitive PII. CAIRS cases are entered as a final summary of workplace related incidents reported by employees at each site. There are case managers in each site who are notified of work-related injury and then access the CAIRS database for reporting purposes as dictated by DOE Orders. There is no direct consent from affected employee to get their information entered into CAIRS. Additionally, the PII regarding each case's target subject is provided by the subject's employer. The employer is required by law to provide this information for OSHA reporting purposes. Target subjects do not have the opportunity to consent to this use. Information is not used for other than required or authorized use. Information contained in SERT is provided by the target individual or their survivors who claim benefits under the EEOICPA. To apply for the program, a claimant must sign a release form authorizing DOL to request their information from DOE. DOL will not request information from DOE unless the claimant has signed the release. If the claimant does not consent to DOE sharing their information, they have the option not to sign the release when they apply to the program. In addition to information provided by the claimant, PII is collected in SERT that does not allow for the specific consent of the individual. This includes records from other Federal agencies (DOL and NIOSH) and records from DOE field sites (both Federal and contractor information).

<table>
<tr><td></td><td></td></tr>
<tr><td>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?</td><td>DOE EHSS contractors are involved in the design, development, and maintenance of RDS with oversight and approval from the System & Data Owners, Cyber Team, and Authorizing Official. Contractors serve as system administrators and programmers to maintain and upgrade various RDS applications. Privacy Act clauses were included in these contracts.</td></tr>
<tr><td>4. IMPACT ANALYSIS:

How does this project or information system impact privacy?</td><td>Certain applications in the RDS enclave are designed to contain sensitive PII/PHI. CAIRS and SERT contain sensitive medical information. Should individuals' sensitive PII be compromised, it could cause serious professional, reputational, and social harm and could result in significant embarrassment. A breach of sensitive PII could damage the trust between individuals and the Federal Government.

EHSS business processes and system controls are in place to protect individuals from the risk of harm and embarrassment. For example, access to and use of PHI in the CAIRS application is limited to employees specifically tasked to collect and analyze injury and illness data respecting DOE employees. EHSS is aware that compromise of PHI/PII maintained in CAIRS may impact an individual's privacy by exposing information about reported injuries or illnesses. Emerging technologies tested on CAIRS information are limited to aggregate data in a separate database so as not to risk compromise of PII in CAIRS.

RDS has an Allowlist methodology that provides user access based on an approval process and an IP FW acceptance once access is approved. The system applications within the system use various controls such as two factor authentication and PIV badges to authenticate users' access to the system. In addition, SSL certificates ensure that communications between servers and web browsers is secure, allowing the secure transmission of PHI and other PII data to support the EEOICPA program.

No information not discussed in this PIA is being collected or disseminated by this system.</td></tr>
<tr><td>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</td><td>When a user files a claim, a unique identifier is created for the user. Claim records are deleted after 60 days.

<table>
<tr><th>Application</th><th>How PII is retrieved</th><th>Why is PII retrieved</th></tr>
<tr><td>Computerized Accident/Incident</td><td>• RDS System Admins can retrieve name, email, Phone number, or</td><td>Each CAIRS case requires administrative PII for</td></tr>
</table>
</td></tr>
</table>

retrieve information on the individual.		Reporting System (CAIRS)	address from user profile in the database. • RDS System admins and authorized application admin users with special permissions can retrieve name, email, phone number, address, SSN, or DoB through reporting screens within the application.	contact and reporting purposes.	
		Secure Electronic Records Transfer (SERT)	• RDS System Admins and authenticated users can retrieve name and DoB when looking up claims in the system.	SERT claims require PII retrieval to track down EEOICPA documents per request type.	
		Occurrence Reporting and Processing System (ORPS)	• RDS System Admins and approved Help Desk Team members can retrieve name, e-mail, phone number, or address for registered users using the appropriate user management screens. • RDS System Admins and authenticated users can retrieve name, e-mail, phone number, or address from ORPS reports.	PII is retrieved for contact purposes.	
		Electronic Fund Administration System (EFAS)	• Authenticated users can retrieve name, phone number from authorized forms within the application. • RDS System Admins and approved Help Desk Team members can retrieve name, phone number, address, email for registered users using the appropriate user management screens.	PII is retrieved for contact purposes.	
		DOE Operating Experience Program (OPEXShare)	• RDS System Admins, authorized application admins, and Help Desk Team members can access name, email, and phone number of registered and approved users using the user administration screens and user reports.	PII is retrieved for contact purposes.	

		Worker Safety & Health Policy Clarification Portal (PC Portal)	• RDS System Admins and authorized application admins can access name, email, and phone of the submitter of new questions so they can be contacted for more information, as necessary • RDS System Admins and authorized application admin users can also view the email addresses of other authorized admins in the application to manage notifications for workflows	PII is retrieved for contact purposes.	
		Radiological Source Registry and Tracking (RSRT)	• Only RDS System admins can retrieve Name, phone number, address, email for registered users from the database • RDS System admins and Help Desk Team Members can view Name, Phone Number, and Email for registered users using approved user management screens	PII is retrieved for contact purposes	
		Safety Basis Information System (SBIS)	• Only RDS System admins can retrieve Name, phone number, email for registered users from the database • RDS System admins and Help Desk Team Members can view Name, Phone Number, and Email for registered users using approved user management screens	PII is retrieved for contact purposes	
		Health and Safety Issue Tracker (HSIT)	• Only RDS System admins can retrieve Name, phone number, email for registered users from the database	PII is retrieved for contact purposes	
		Fire Protection (FP)	• Only RDS System admins can retrieve Name, phone number, address. email for registered users from the database • RDS System admins and Help Desk Team	PII is retrieved for contact purposes	

			Members can view Name, Phone Number, and Email for registered users using approved user management screens		
		Lessons Learned (LL)	• RDS System admins and Help Desk Team Members can retrieve Name, phone number, and email for registered users from the approved user management screens • Authenticated admin users can retrieve Name, Phone Number, and Email address for all approved users from admin screens and reports within the application	PII is retrieved for contact purposes	
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*.**	PII retrieval within RDS applications is restricted to administrative use retrieval and does not therefore require SORN coverage. Only two applications, CAIRS and SERT, contain sensitive PII. While retrieval in those applications in actual practice is administrative, the records in those applications are covered by the following SORNS: • DOE-10 *Energy Employees Occupational Illness Compensation Program Act Files*, 74 FR 1008, January 9, 2009 • DOE-38 *Occupational and Industrial Accident Records*, 74 FR 1039, January 9, 2009				
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?	Most PII in RDS applications is provided by the individuals to whom that PII pertains. Additional sources of PII include employing and other Federal agencies including DOL and NIOSH. Employing agencies are required by law to provide this information for OSHA reporting purposes.				
9. Will the information system derive new or meta data	No. Neither RDS nor the applications that reside within it derive new or meta data about individuals.				

about an individual from the information collected?	
10. Are the data elements described in detail and documented?	Data elements are described in the RDS System Security Plan (SSP).
DATA USE	
11. How will the PII be used?	PII use is based on the business process supported by the application. Please see the "Purpose" section in Module I as well as the table in the response to Question #5 for details on PII use.
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?	Information in SERT will be shared with the Department of Labor (DOL) and the National Institute for Occupational Safety and Health (NIOSH).
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	Access logs containing user name are created by each application for security purposes. In SERT, reports containing name and SSN (for identification and security purposes) are generated which list the cases that have not been completed, the cases previously completed, and the timeliness of the completed requests.
15. What will be the use of these reports?	Log reports are generated to maintain the security and integrity of the system. In addition, SERT case reports will provide claim status information for EEOICPA claim processing and management. Managerial reports will provide program information about claim completion, timeliness, and quantity.
16. Who will have access to these reports?	Certain authorized users are granted access to specific reports within RDS applications based on their roles and responsibilities. Please see the response to Question #26 for more information on roles.
MONITORING	

17. Will this information system provide the capability to identify, locate, and monitor individuals?	RDS provides no capability to identify, locate, or monitor individuals beyond the capability intrinsic to basic contact information (e.g., address). Neither RDS nor the applications within it are used 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?	Various controls are implemented to prevent the unauthorized use (including unauthorized monitoring) of PII. RDS operations personnel implement access control groups within the RDS Active Directory to control access for each application and each user in furtherance of the security and integrity of the system. The RDS system undergoes a yearly assessment of its Authorization Boundary and its applications from a security controls perspective as well as an Authority to Operate (ATO) from the Authorizing Official (AO) every three years. Role-based access controls ensure that only the data that should be accessible to that individual will appear on the screen. The System Owner has implemented and tested all baseline security controls appropriate to FIPS categorization of MODERATE in accordance with the DOE EITS PCSP, Attachment 3 – NIST SP 800-53, Revision 4 and DOE Directives. Paper records are maintained in locked cabinets and desks. Electronic records are controlled through established DOE computer center procedures (personnel screening and physical security), and they are password protected. Access is limited to those whose official duties require access to records.
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.	RDS and applications will undergo a yearly security assessment at which time user records will be analyzed for accuracy and validity. CAIRS performs several validation checks on input data before it may be submitted into production. Many values are selected from a predetermined list with no deviations allowed. There are designated data reviewers to check for classification coding correctness. Case numbers are rolled up to an aggregate report for each organization that is checked for correctness quarterly. Data is input and kept current as cases are discovered. Data must be marked current by the end of each quarterly reporting period as per DOE Order. Note that case data prior to 1983 may not be as accurate, as the system was manually populated with aggregated data prior to 1983. SERT users at individual sites upload relevant records of individuals and are responsible for the accuracy of the information uploaded. Claims processors

	review the information provided and request additional information or clarification, as needed. The system contains field edits and consistency checks to prevent invalid data entry.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	RDS is hosted by the DOE OCIO within the AWS Cloud and managed by the Energy IT Services (EITS) DCCS team. All users must acknowledge and agree to the system rules of behavior to ensure consistent use. RDS is a web-based design with a database backend. The system uses a series of access control elements to classify users and control business flow. Designated data input users may only input data for the organizations for which they are approved. Users who do not have input access for an organization cannot view PII associated with data records for that organization. Data collected is specified by DOE Orders and Manuals. Input users complete a standard form that the system presents to them.
RECORDS MANAGEMENT	
22. Identify the record(s).	Each RDS application complies with the records schedule applicable to the types of records maintained by the application. Computerized Accident/Incident Reporting System (CAIRS), CAIRS can produce the Occupational Safety and Health Administration (OSHA) 100, 101, 102 and 200 forms. CAIRS can also reproduce the original DOE 5484.3 form which is an individual accident/incident report that contains subject persons PII. These records have a retention period of 75 years, after which they will be deleted from the database The National Archives and Records Administration (NARA) approved the Energy Employees Occupational Illness Compensation Program Act (EEOICPA) Schedule on February 7, 2014. The Request for Records Disposition Authority records scheduled items includes; 1. The Health Compensation Program Claims Response Files has a retention period of 75 years. 2. The Health Compensation Program Working File has a retention period of 3 years. 3. The Health Compensation Program Control Files has a retention period of 15 years. 4. The Health Compensation Programs Administrative Files has a retention period of 3 years
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	• DAA-GRS-2017-0010-0001 should be preceded with "DOE 2.7 item 010" to help better identify the schedule and retention • DAA-GRS-2016-0015-0012 – should list ADM 1.31 (in part) or N1-434-92-4, item 26 (in part) for Workers Compensation until superseded • DAA-GRS-2016-0015-0013 – should list ADM 1.31 (in part) or N1-434-92-4, item 26 (in part) for Workers Compensation until superseded.

	• The ADM Schedule 1, Item 34. Occupational Injury and Illness Files (N1-434-98-4 item 34) should be updated to DOE 2.7, item 100 (DAA-GRS-2017-0010- 0002) • DAA-0434-2013-0001-0001Health Compensation Program Claims Response Files • DAA-0434-2013-0001-0002 Health Compensation Program Working Files • DAA-0434-2013-0001-0003 Health Compensation Program Control Files • DAA-0434-2013-0001-0004 Health Compensation Programs Administrative Files
24. Records Contact	Baldev Dhillon, Baldev.Dhillon@hq.doe.gov, 301-903-0990
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification, or use?	PII in RDS is protected by a number of controls. RDS operations personnel implement access control groups within the RDS Active Directory to control access for each application and each user in furtherance of the security and integrity of the system. The RDS system undergoes a yearly assessment of its Authorization Boundary and its applications from a security controls perspective as well as an Authority to Operate (ATO) from the Authorizing Official (AO) every three years. Role-based access controls ensure that only the data that should be accessible to that individual will appear on the screen. The System Owner has implemented and tested all baseline security controls appropriate to FIPS categorization of MODERATE in accordance with the DOE EITS PCSP, Attachment 3 – NIST SP 800-53, Revision 4 and DOE Directives. Paper records are maintained in locked cabinets and desks. Electronic records are controlled through established DOE computer center procedures (personnel screening and physical security), and they are password protected. Access is limited to those whose official duties require access to records.
26. Who will have access to PII data?	Each application within RDS contains role-based controls which restrict access to PII to administrators (e.g., User Accounts Administrators, System Approvers, Database Administrators, System Super Users) and users authorized to access PII for a business purpose (e.g., case officers processing and managing cases in claim-based applications including CAIRS and SERT).
27. How is access to PII data determined?	User profiles are established and roles are defined to restrict access exclusively to information needed for role function. Roles determine which users see which data. Criteria, procedures, controls, and responsibilities are documented.

	RDS operations personnel implement access control groups within the RDS Active Directory to control access for each application and each user in furtherance of the security and integrity of the system. The RDS system undergoes a yearly assessment of its Authorization Boundary and its applications from a security controls perspective as well as an Authority to Operate (ATO) from the Authorizing Official (AO) every three years.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No.
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?	N/A
30. Who is responsible for ensuring the authorized use of personal information?	The Data Owners of each system are responsible for ensuring the authorized use of personal information.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	(Signature)	
Local Privacy Act Officer	(Signature)	
Ken Hunt **Chief Privacy Officer**	William K. Hunt Digitally signed by William K. Hunt Date: 2022.03.29 12:02:27 -04'00' (Signature)	