Department of Energy

Privacy Impact Assessment (PIA)

Affects Members Of the Public? ☒

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	November 21, 2022
Departmental Element & Site	Office of Environment, Health, Safety and Security Office of Resource Management (EHSS-70) Office of Information Management (EHSS-72) DOE Headquarters, Germantown, MD DC&SS Room CA-007
Name of Information System or IT Project	AU System Hosting Environment (ASHE), and the hosted applications: Electronic Department of Energy (DOE) Integrated Security System (eDISS+) Unclassified Safeguards and Security Information Management System (U-SSIMS)
Exhibit Project UID	019-10-01-22-01-1013-00-403-134
New PIA ☐ **Update** ☒	This update is to reflect that ASHE hosts U-SSIMS and eDISS.

	Name, Title	**Contact Information Phone, Email**
System Owner	Michelle Ho, System Owner Office of Information Management (EHSS-72)	301-903-0521 Michelle.Ho@hq.doe.gov
Local Privacy Act Officer	Raymond Holmer Director, Office of Information Management (EHSS-72)	301-903-7325 Raymond.Holmer@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Krystal Harne EHSS Information Systems Security Officer (ISSO) Office of Information Management (EHSS-72)	301-903-8283 Krystal.Harne@hq.doe.gov
Person Completing this Document	Leif Dahl, CISSP, CISM ASHE, eDISS+, U-SSIMS ISSO	301-903-8688 Leif.Dahl@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Purpose of Information System or IT Project	The AU System Hosting Environment (ASHE) currently provides system hosting services to eDISS+ and U-SSIMS. eDISS+ is a major application that supports unclassified DOE security clearance processing and stores personnel security clearance information for complex-wide use. It also provides security clearance processing and adjudication status and is used by the DOE Protective Force to access active clearance information and visit authorization information needed for local site visitor access control, including classified visits to DOE facilities, and access to weapons data. eDISS+ contains PII types specified in the next section. U-SSIMS is an unclassified version of SSIMS which allows data entry and query of the two unclassified data tables from classified SSIMS production, DOE F 470.2, *Facility Data and Approval Record (FDAR)* and DOE F 470.1, *Contract Security Classification Specification (CSCS)* in an unclassified environment while maintaining the complete database in the classified SSIMS production environment. U-SSIMS contains no PII; U-SSIMS contains only contract and facility information.
Type of Information Collected or Maintained by the System:	**All of the below responses are for eDISS+** ☒ 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 ☐ Other – Please Specify
Has there been any attempt to verify PII does not exist on the system?	eDISS+ contains PII. U-SSIMS contains no PII.

MODULE I – PRIVACY NEEDS ASSESSMENT

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.*	
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	**eDISS+:** Not applicable **U-SSIMS:** Not applicable
Threshold Questions	
1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	**eDISS+:** Yes **U-SSIMS:** No
2. Is the information in identifiable form?	**eDISS+:** Yes **U-SSIMS:** No
3. Is the information about individual Members of the Public?	**eDISS+:** Yes **U-SSIMS:** No
4. Is the information about DOE or contractor employees?	**eDISS+:** ☒ Federal Employees ☒ Contractor Employees **U-SSIMS:** No

END OF PRIVACY NEEDS ASSESSMENT

The remainder of this PIA refers exclusively to eDISS+

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated**	The Department of Energy Organization Act, 42 U.S.C. 7101–7385, the Energy Reorganization Act of 1974 (ERA), 42 U.S.C. 5801–5911, and the Atomic Energy Act of 1954, as amended, (AEA) 42 U.S.C. 2011, require DOE to protect the public safety and health, as well as the safety and health

MODULE II – PII SYSTEMS & PROJECTS	
collection, use, and/or retention of personal information?	of workers at DOE facilities, in conducting its activities, and grant DOE broad authority to achieve this goal. Authority for maintenance of the system is given by 42 U.S.C. 7101 et seq. and 50 U.S.C 2401 et seq. The Privacy Act of 1974, Public Law 93-579 as amended, allows an agency to maintain information about an individual that is relevant and necessary to the purpose of the agency as required by statute or by Executive Order of the President.
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 may decline to provide information (either through the form collecting the information or through a Disclosure Authorization that applicants must sign during the investigation process), however, failure to provide necessary information can delay the clearance process or prevent granting of the clearance altogether.
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?**	Yes. Privacy Act contract clauses have been included in contracts associated with contractor firms supporting eDISS+.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The unauthorized disclosure of information contained in the system is expected to have a serious adverse effect on individuals' privacy. The system contains highly sensitive PII. Should sensitive PII in the system be compromised, it would result in significant privacy harm to individuals potentially including financial harm, professional harm, embarrassment, harm to personal relationships, and it would damage the trust between individuals and the Federal Government. The system observes a number of protections to protect privacy and via the Fair Information Practice Principles (FIPPs). The connection between the end user's browser and the server employs Transport Layer Security (TLS) encryption. Authorized users of the system are the subject of a favorably adjudicated background investigation and receive extensive training on the use and protection of PII. The system maintains the minimum PII necessary for its business purpose to mitigate privacy harm. In addition, use of the PII in is limited to clearly defined business purposes. Security controls have been implemented and processes are in place to ensure that access is restricted

MODULE II – PII SYSTEMS & PROJECTS

	according to role and that controls are operating effectively to mitigate the risk of data compromise. Please see question 25 for more details on controls.
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 for an individual can be retrieved by name, social security number, or DOE 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*.**	DOE-43, Personnel Security Clearance Files, 74 FR 1044 DOE-45, Weapons Data Access Control System (WDACS), 74 FR 1047 DOE-51, Employee and Visitor Access Control Records, 74 FR 1053
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?	Personal information is submitted by the end user during the completion of the Questionnaire for National Security Positions (SF 86) via the Office of Personnel Management (OPM) Electronic Questionnaires for Investigations Processing (e-QIP) application. Additional information is submitted during the investigation and adjudication processes by Investigative and Personnel Security staff.
9. Will the information system derive new or meta data about an individual from the information collected?	No

MODULE II – PII SYSTEMS & PROJECTS

10. Are the data elements described in detail and documented?	Yes, data elements are described in the Personnel Security Database (PSDB) data dictionary.
DATA USE	
11. How will the PII be used?	The data are used to determine the level of an employee's access to sensitive or classified data. Clearance request data are used to determine if an applicant is suitable for such access. The data are also used to process and track classified visits and access approvals to DOE facilities (CVCS) and to track visits and access approvals for the DOE and UK nuclear weapons complexes (WDACS and US-UK Visits).
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?**	Not applicable
13. With what other agencies or entities will an individual's information be shared?	Clearance data is shared with the following agencies/entities: a. ***OPM*** to provide data for their ***Clearance Verification System (CVS)*** which serves as a national database for clearance reciprocity information b. Intelligence community within DOE for the ***Scattered Castles*** information system c. ***DOEInfo*** system to provide clearance data for employees in the DOE Management Information System (MIS) d. ***Kansas City Plant (KCP)*** within DOE to verify clearance level for local visits e. ***NNSA*** for local clearance tracking and case management via the ***Clearance Action Tracking System Stabilization Enhancement (CATS SE)*** in Albuquerque, NM. f. ***NNSA*** to provide clearance data for the ***Weapons Data Access Control System (WDACS)*** application. This system tracks visits at domestic DOE weapons sites that require SIGMA access for all visitors. g. ***NNSA*** to provide clearance data for the ***US-UK Visits*** application. This system tracks visits between NNSA and United Kingdom stakeholders, that are held domestically or in the UK and have attendees from both locations. These visits require clearance verification and tracking of SIGMA level access for all visitors.

MODULE II – PII SYSTEMS & PROJECTS

	h. *NNSA* for clearance verification and tracking for specific individuals using the ***Sandia Total Access Request Tool (START)*** at the ***Sandia Field Office (SFO)***. START is used to manage requests for physical access to SNL that may or may not require a clearance. i. *NNSA* for bi-directional communication between eDISS+ and the ***OneID*** system hosted by ***LLNL at the NNSA/AC*** (Albuquerque Complex). j. ***Nevada National Security Site (NNSS)*** to allow the ***ForgeRock*** System access to synchronize data (clearance level and status) between eDISS+ and ForgeRock for all employees and contractors conducting business at the NNSS. k. ***Idaho National Laboratory (INL)*** to share clearance data electronically between the INL Identity Management System ***(IMS)*** and eDISS+ to allow department and agency customers to access clearance information for IMS identities.
REPORTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	The following eDISS+ applications produce reports: Web-based Central Personnel Clearance Index (WebCPCI), CVCS, PSDB Admin, and WDACS. WebCPCI produces reports associated with clearance and adjudication information. The Classified Visitor Control System (CVCS) generates reports such as visit summaries, daily visit reports, and cancelled visit reports. The Personnel Security Database (PSDB) Admin application produces reports associated with access to the PSDB. The Weapons Data Access Control System (WDACS) generates reports associated with visits and access to weapons data. The US-UK Visits application generates reports associated with visits and access to weapons data.
15. What will be the use of these reports?	The reports are used to maintain the security and integrity of DOE sites.
16. Who will have access to these reports?	Users of eDISS+ applications have access to the above reports based on assigned roles within each application. System users are personnel security, Protective Force officers and badge office staffs that have access to a limited portion of PII in the performance of their daily job duties. For a list of roles and permissions associated with those roles see Section 4.5 Account Management in the eDISS+ Security Plan Addendum to the ASHE System Security Plan (SSP).
MONITORING	
17. Will this information system provide the capability to	The system does not provide monitoring capabilities beyond tracking site access.

MODULE II – PII SYSTEMS & PROJECTS

identify, locate, and monitor individuals?	
18. What kinds of information are collected as a function of the monitoring of individuals?	Not applicable
19. Are controls implemented to prevent unauthorized monitoring of individuals?	A series of physical, technical, and administrative controls are implemented to prevent the unauthorized use of the system.
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.	Clearance records are assigned an effective date. Clearance requests are certified by the applicant for a given date, which is then stored in the Personnel Security Database (PSDB). Validation routines in the e-DISS+ software applications ensure that data is complete and non-contradictory. Investigation results are subject to a rigorous adjudication process before a clearance is granted or denied. Employees are given the chance to address questions that arise from the investigation.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Consistency is maintained by policies documented in DOE Orders. All users and administrators of the system must sign End User and Privileged User Rules of Behavior which provide detailed guidance on appropriate usage of the system.
RECORDS MANAGEMENT	
22. Identify the record(s).	**IAW DOE ADM RECORDS SCHEDULE 18, September 2010, Rev 2:** **11.3 Incident of Security Concern Inquiry/Investigation Files.** Destroy 5 years after cutoff. **21. Security Clearance/Access Authorization Administrative Subject Files.** a. Destroy 10 years after cutoff, b. Destroy 5 years after cutoff. c. Destroy 10 years after cutoff. d. Destroy when related records are destroyed or when no longer needed for reference. e. Cut off at the end of the fiscal year. Destroy 2 years after cutoff.

MODULE II – PII SYSTEMS & PROJECTS

	f. Cut off at the end of the fiscal year. Destroy 3 years after cutoff. **21.3 Pre-Employment Background Investigation.** a. Destroy 2 years after cutoff or date of background investigation. b. Destroy 5 years after cutoff or date of pre-employment background investigation. **22. Security Clearance/Access Authorization Case Records.** a. & b. Destroy not later than 10 years after date the individual's authorization is terminated or upon notification of death of the individual, whichever is sooner. c. & d. Destroy when no longer needed. **23. Security Clearance/Access Authorization Status Files.** Destroy 75 years after cutoff. **24. Security Violations Files.** Copies of "Report of Security Incident/Infraction," or similar forms or reports that are placed in Personnel Security files are handled in accordance with item 22, above. Other documentation relating to infractions or violations is handled in accordance with items 11.1 and 11.3.
23. Identify the specific disposition authority (ies) that correspond to the record(s) noted in no. 22.	**(N1-434-98-21, Item 11.3)** **(N1-434-98-21, Item 21)** **(N1-434-98-21, Item 21.3)** **(N1-434-03-01, item 22)** **(N1-434-98-21)** **(GRS 18, item 24)**
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?	The System Owner has implemented and tested all baseline security controls appropriate to its FIPS 199 security categorization of Moderate in accordance with the DOE EITS ***Program Cyber Security Plan (PCSP)***, February 2020, NIST SP 800-53 rev. 4 and applicable DOE Orders and Directives. ASHE (and its only hosted system at the time, eDISS+) was assessed and authorized on October 17, 2019. A supplemental ATO was issued on September 25, 2020, authorizing inclusion of U-SSIMS within ASHE. An ATO extension was issued on June 8, 2021, to authorize operation of ASHE (including eDISS+ and U-SSIMS) through May 31, 2022, to allow EHSS to determine the best environment to move ASHE to following closure

MODULE II – PII SYSTEMS & PROJECTS

	of the GTN DC&SS. The Information Security Categorization of eDISS+ and the associated connection hardware was recently upgraded to High (based on FIPS 199 and NIST SP 800-60 Vol. I & II). However, a full A&A has not been performed on eDISS+ at the High level due to the impending migration to a new environment. Comprehensive security measures are in place, including firewalls, restricted user roles, data encryption, and audit logs. A complete discussion of controls in place to provide data protection is available in the ASHE System Security Plan (SSP) and e-DISS+ Security Plan Addendum (SPA).
26. Who will have access to PII data?	Restricted access to data pertaining to their site or organization is granted to users and their managers based on roles within each application. System users are personnel security, Protective Force officers and badge office staffs that have access to a limited portion of PII in the performance of daily job duties. The Data Owner and limited designated system administrators have access to all databases.
27. How is access to PII data determined?	Access to PII is determined by specific job functions. Procedures, controls, and responsibilities for assigning system access are documented in the eDISS+ SPA.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	The Weapons Data Access Control System (WDACS) has indirect, electronic access to the clearance data for individuals in eDISS+. This application, used by NA-122.12, is housed within the eDISS+ system. Only a small subset of clearance data is shared with WDACS, in order to verify the proper clearance level for individual, before allowing access to visits that require the additional Sigma access. A data feed consisting of clearance data is provided to DOE IN-20 for the Scattered Castles database, as well as OPM for the CVS system on a daily basis. A data feed consisting of clearance data is provided to DOE MA for the DOEInfo database on a daily basis. eDISS+ receives investigative information from OPM via the eDelivery process. A web service architecture provides investigative information received from OPM via eDelivery to the NNSA CATS SE system on a daily basis. Other data feeds provide clearance data for access control and various other services. Refer to the responses to question 13 above and question 29 below for additional detail on Interconnection Security Agreements, Connection Agreements and Data Feeds.

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?	Currently, eDISS+ shares information with eleven systems, including the DOE Employee Data Repository (commonly referred to as DOE*Info*); the DCSA eDelivery System[1]; four ISAs with the NNSA: Clearance Action Tracking (CATS) (NA-IM-40), DIF Exchange, LLNL OneID via NNSA/AC, and the NNSA Sandia Field Office (SFO); NNSA's Kansas City Plant (KCP) ID Manager software application; the DOE Office of Intelligence and Counterintelligence (IN-20) Counter Intelligence Evaluation Division (CIED) Scattered Castles application; NNSS ForgeRock, INL IMS, and the DOE Office of the Chief Information Officer for DOENet WAN services via the EITS Networks Enclave to support eDISS+. The ISA with DOEInfo outlines the details of the provision of clearance information from eDISS+ to DOEInfo. There is a one-way connection between these two systems with no modification of eDISS+ data by DOEInfo. The MOU with DCSA Agency Delivery defines the nature of the nightly data feed of clearance information from DCSA. There is no direct connection between Scattered Castles or CVS or capability for DCSA to modify eDISS+ data. An ISA has been approved between NNSA (NA-IM-40) and AU for CATS and is referenced in the eDISS+ SPA. Compressed encrypted "DIF" packages received from DCSA via eDelivery are sent to CATS via encrypted SSL over HTTPS using DOENET. Dataflow is unidirectional from eDISS+ to CATS. A second ISA is in place with NNSA in the form of a Data Bridge between CATS and the eDISS+ PSDB. A description of the elements to be transferred is provided in the ISA. The purpose of this data feed is to allow the NNSA CATS to query, create, update, and delete data in the eDISS+ CPCI database transparently, and automatically. A third ISA with the NNSA SFO START tool is used to establish a secure communications link to provide a consumer web service to SNL from eDISS+, with a limited view of the PSDB, for clearance verification and information for specific individuals. A fourth ISA with NNSA for LLNL OneID is a bilateral agreement between eDISS+ and the OneID system hosted by LLNL at the NNSA/AC. This interconnection allows bi-directional communication between eDISS+ and OneID via APIs using web services architecture (Web Services Description Language - WSDL) and Extensible Markup Language (XML) over HTTPS. An interface has been approved between the NNSA ID Manager application at the Kansas City Plant and AU for a data feed to the Kansas City Plant and

[1] Technically, eDISS+ data is not shared with OPM via eDelivery. Investigation data is *received* from OPM and populated in case folders as appropriate.

MODULE II – PII SYSTEMS & PROJECTS

	is referenced in the eDISS+ SPA. An ISA has been approved to allow the NNSS ForgeRock System access to synchronize data (clearance level and status) between eDISS+ and ForgeRock for all employees and contractors conducting business at the NNSS. An ISA is in place with INL IMS to share clearance data electronically between the INL IMS and eDISS+ to allow department and agency customers to access clearance information for IMS identities. (This interface does not exist in the eDISS production environment). There is no direct connection between eDISS and DNI for the Continuous Evaluation enrollment interface.
30. Who is responsible for ensuring the authorized use of personal information?	The Director of the DOE Office of Departmental Personnel Security (EHSS-53) is responsible for assuring proper use of the data.

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	**Michelle Ho** Michelle Huyen Ho Digitally signed by Michelle Huyen Ho Date: 2023.01.03 08:58:08 -05'00' **(Signature)**	
Local Privacy Act Officer	**Raymond Holmer** RAYMOND HOLMER Digitally signed by RAYMOND HOLMER Date: 2023.01.03 15:01:45 -05'00' **(Signature)**	
Chief Privacy Officer	Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2022.12.29 16:22:07 -05'00' **(Signature)**	