Affects Members Of the Public?	NO

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	05/18/2020	
Departmental Element & Site	Department of Energy (DOE), Office of the Chief Information Officer (OCIO), Cybersecurity Compliance and Oversight Office, (IM-32)	
Name of Information System or IT Project	Cyber Security Assessment and Management (CSAM)	
Exhibit Project UID	N/A	
New PIA □ **Update** ☒	PIA is being updated in light of the change in system owner.	
	Name, Title	**Contact Information Phone, Email**
System Owner	Robert Coffman	(301) 903-2171 Robert.Coffman@hq.doe.gov
Local Privacy Act Officer	Brooke Dickson	(202) 287-5786 Brooke.Dickson@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Lawrence Orah	(202) 409-5584 Lawrence.Orah @hq.doe.gov
Person Completing this Document	Lawrence Orah, ISSO	202-409-5584 Lawrence.Orah @hq.doe.gov
Purpose of Information System or IT Project	CSAM provides DOE's information assurance and program officials with a secure web-based network capability to assess, document, manage, and report on the status of information technology (IT) for security authorization processes in the risk management framework in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). CSAM provides a Department-wide view of the status of information system security and documented processes, including security and privacy risk assessments, implementation of DOE privacy and IT security mandates, and information system compliance documentation. CSAM is a Government Off-the-Shelf (GOTS) application owned by the Department of Justice (DOJ) Cybersecurity Services Staff (CSS). CSAM is a Sensitive But Unclassified (SBU) system that has been implemented under FISMA. CSAM provides the following functions: • Process, store, and report DOE IT Security Program information; • Employ an enterprise-wide tool for leveraging National Institute of Standards and Technology (NIST) and Office of Management and Budget (0MB) guidance; • Support system inventory management; • Support FISMA reporting; • Provide security oversight and compliance; • Provide security authorization and accreditation; • Provide privacy oversight of compliance activities; • Manage the continuous monitoring process.	
Type of Information Collected or Maintained by the System:	□ SSN □ Medical & Health Information	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Financial Information ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address Used by CSAM to identify officials with responsibility for risk management functions, security authorizations, security or privacy risk assessments, audits, and compliance oversight. ☐ 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.*	N/A This system contains PII
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A
Threshold Questions	
1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES
2. Is the information in identifiable form?	YES
3. Is the information about individual Members of the Public?	NO

MODULE I – PRIVACY NEEDS ASSESSMENT

4. Is the information about DOE or contractor employees?	YES ☒ Federal Employees ☒ Contractor Employees

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. seq. Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. §§ 3551-3558
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 generally do not have the right to decline information or to consent to specific uses of information within CSAM. A DOE employee or contractor must provide basic information in order to create a user account and access CSAM to perform official duties. This information is voluntarily provided during the CSAM account creation process, and individuals who decline to provide requested information will not be provided access to CSAM. Other individuals involved in information system security functions may have their name, title, organization, and contact information captured and used within the system, or within related system artifacts, without their awareness or specific consent. The identification of officials responsible for risk management functions, security authorizations, security or privacy risk assessments, and compliance oversight is critical for DOE to ensure proper monitoring of security and privacy controls in accordance with Federal law, policy, and standards and is not voluntary.
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 were 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.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed CSAM as a moderate-risk system according to the criteria set forth in Federal Information Processing Standard (FIPS) 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. The unauthorized disclosure of information is expected to have a minimal adverse effect on organizational operations, organizational assets, or individuals. The PII contained in CSAM is low sensitivity and is not anticipated to cause significant harm in the event of a breach. 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 CSAM.
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.**	DOE staff can download information with proper permission via the web browser to Excel files and other common formats. For limited administrative purposes, information can be retrieved by individual name, role, and system name.
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*.**	No. Maintenance of information about an individual is not enough to trigger the SORN requirements of the Privacy Act, although it is enough to warrant a privacy impact assessment (PIA). To trigger the SORN requirements of the Privacy Act, information must actually be retrieved by a personal identifier in practice.
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?	DOE Active Directory and user inputs regarding system ownership are the sources of information about individuals that resides in CSAM. The use of that information about individuals is limited to administrative functions related to use and access of CSAM and contact information for ownership of systems contained on CSAM. No additional PII is provided by other systems or requested in order to use CSAM.
9. Will the information system derive new or meta data about an individual from the information collected?	CSAM does not derive new data or create previously unavailable data about an individual through aggregation from the information collected, nor is new data about individuals input into the system.
10. Are the data elements described in detail and documented?	The data elements are contained in the database schema with field attributes. Detailed descriptions are not maintained in CSAM as it is not the source system for these data elements.
DATA USE	
11. How will the PII be used?	CSAM supports DOE information assurance and privacy functions, documents assessments, and information about the configuration, vulnerabilities, weaknesses, and security posture of DOE information systems. Employee and contractor name, organization, title and official contact information are collected and used in CSAM to support the DOE information assurance programs to identify officials with responsibility for risk management functions, security authorizations, security or privacy risk assessments, and compliance oversight.
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?	System data may also be shared with the Office of Management and Budget during oversight activities such as those under 0MB Circular A-123.
REPORTS	

MODULE II – PII SYSTEMS & PROJECTS	
14. What kinds of reports are produced about individuals or contain an individual's data?	There are a number of canned reports in CSAM that contain data of that type. Ad-hoc reports may also be produced that reference an account holders name, role, phone #, location, department, etc. The emphasis of these reports will be about the systems as opposed to individuals. Information about individuals is for administrative purposes, i.e., identifying system owners and other responsible parties associated with a system.
15. What will be the use of these reports?	System Owners, ISSO's, Security Control Assessors and other stakeholders will use these reports in support of system-level assessment and authorization exercises.
16. Who will have access to these reports?	Approved DOE federal and contractor personnel will have access to data in the system. Authorized access will be limited to users with a valid need-to-know, and permissions will be restricted to their particular role within CSAM.
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	CSAM data input and changes can be tracked through database logging and auditing functions. Access and changes to CSAM data are captured in audit logs that are assigned to privileged individuals with appropriate system roles to monitor audit logs. Audit logs are designed to be checked on a routine basis and monitored by system administrators.
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.

MODULE II – PII SYSTEMS & PROJECTS

19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes, the system is only accessible from within the DOE network. Controls are in place to protect the confidentiality, integrity, and availability of the system, including meta data transferred to, ingested by, and stored in CSAM. Access is limited to approved federal and contractor employees controlled by the system administrator. System passwords are stored using 128 bit encryption. In addition, access control and account management policies and procedures regarding user roles and responsibilities are in place and are detailed in the DOE CSAM System Security Plan. These controls are publicly listed in the National Institutes of Standards (NIST) Special Publication (SP) 800-53 (Revision 4), Recommended Security Controls for Federal Information Systems and Organizations database, which represents security controls and associated assessment procedures and can be located here: https://nvd.nist.gov/800-53. Controls include but are not limited to the following: • (AC-2) Account Management • (AC-3) Asset Enforcement • (AC-4) Information Flow Enforcement • (AC-5) Separation of Duties • (AC-6) Least Privilege • (AC-7) Unsuccessful Login Attempts • (AC-8) System Use Notification • (AU-2) Audit and Events • (AU-6) Audit Monitoring, Analysis, and Reporting • (IA-5) Authenticator Management • (SC-7) Boundary Protection • (SC-8) Transmission Confidentiality and Integrity

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.	CSAM does not verify the accuracy or completeness of the DOE federal and contractor data in the system. Our account request process does attempt to match the email address provided by the user in their application to the email address that we have on file for them. If the application address is different or no email address is listed by the pull from Outlook, the user record in CSAM is updated. Our process preserves these updates, and ensures that they do not get overwritten by outdated information. CSAM does not collect or store information from sources outside of DOE.

MODULE II – PII SYSTEMS & PROJECTS

21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	CSAM can be accessed on any DOE network via VPN between DOE and DOJ. CSAM provides a single repository containing all system information. The rules, controls, and procedures that govern access to CSAM will be applied consistently, regardless of which site the system is accessed from.
RECORDS MANAGEMENT	
22. Identify the record(s).	Records within CSAM are stored in the CSAM database located in a Department of Justice (DOJ) data center. DOJ owns, manages, operates and maintains the CSAM operating system, databases, application and related hardware. The primary record types in CSAM are systems descriptions, system POC's, security control implementation details and security assessment results.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Scheduled under: • GRS 3.1, item 040 Information technology oversight and compliance records (DAA-GRS2013-0005-0010) • GRS 3.2, item 010 Systems and data security records (DAA-GRS2013-0006-0001).
24. Records Contact	Maria Levesque Supervisory Information Technology Specialist U.S. Department of Energy IM-41 Records Management Phone: 202-586-9527, 703-459-6322 maria.levesque@hq.doe.gov Shannon Hughes shannon.hughes@hq.doe.gov
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Technical and administrative controls are in place to prevent the misuse of data by individuals with access. These controls are detailed in the CSAM System Security Plan (SSP). All system team members (Federal and contractor) are required to annually complete the Department of Energy Headquarters Annual Cyber Security Refresher Briefing as a necessary requirement for access to the system. Administrative controls include separation of duties so individuals only have access to appropriate personal information, and use of system audit logs to monitor access and user activity in the system. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. The technical controls include restricted access via DOE PIV card and PIN. If a user does not have a PIV card, they will be issued a unique-id and password.
26. Who will have access to PII data?	DOE federal and contractor personnel will have access to data in the system. Authorized access will be limited to the CSAM Technical Point of Contact, System Owner, ISSO and on a need to know basis.
27. How is access to PII data determined?	Access to data is determined by evaluation of personnel job responsibilities and organization. Based on the evaluation, the user is assigned permissions that are applied using system access control lists.
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?	There is an ISA between the DOE Authorizing Official for CSAM and the counterpart at the DOJ.

MODULE II – PII SYSTEMS & PROJECTS

30. Who is responsible for ensuring the authorized use of personal information?	The CSAM System Owner, Technical Point of Contact and ISSO are responsible for ensuring the authorized use of personal information.

END OF MODULE II

SIGNATURE PAGE

	Signature
Robert Coffman ***System Owner***	Robert W. Coffman Digitally signed by Robert W. Coffman Date: 2020.06.02 12:01:10 -04'00' **(Signature)**
Brooke Dickson ***Local Privacy Act Officer***	**(Signature)**
Ken Hunt **Chief Privacy Officer**	William K. Hunt Digitally signed by William K. Hunt Date: 2020.07.06 15:28:45 -04'00' **(Signature)**