U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Cyber Security Assessment and Management System (CSAM)
Bureau/Office: Office of the Chief Information Officer
Date: November 2, 2017
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Cyber Security Assessment and Management (CSAM) system is the Department of the Interior's (DOI's) official repository of information systems, and provides the DOI information assurance and program officials with a web-based secure 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 DOI mandated IT security and privacy control standards and policies, and information system compliance documentation. The DOI CSAM instance is managed by the Compliance and Audit Management Branch within the Office of the Chief Information.

CSAM is a Department of Justice (DOJ) system that provides DOI users with access to the DOI instance of DOJ's CSAM application hosted within the DOJ's Data Center. The connection between DOJ and DOI is a site-to-site Virtual Private Network (VPN).

CSAM provides the following functions:

- Processes, stores and reports DOI IT Security Program information
- Uses an enterprise-wide tool for leveraging National Institute of Standards and Technology and Office of Management and Budget guidance
- Supports system inventory management
- Manages the Plan of Action and Milestones process
- Supports FISMA reporting
- Provides security oversight and compliance
- Provides security Authorization and Accreditation
- Provides privacy oversight of compliance activities
- Manages the Continuous Monitoring process

C. What is the legal authority?

Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. §§3551-3558

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

UII Code: 010-000002258

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☐ Yes: *List Privacy Act SORN Identifier(s)*
☒ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Other: *Specify the PII collected.*

CSAM does not collect, process or maintain sensitive personally identifiable information (PII) on individuals. Only official information on employees contractors and auditors, such as name, bureau, title, location, contractor organization and address, work email, and work phone number, are used in CSAM to identify officials with responsibility for risk management functions, security authorizations, security or privacy risk assessments, audits, and compliance oversight. Access to CSAM is restricted by roles within each bureau/office and is based on least privilege principles.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe*

Some records may come from contractors, auditors or other organization during the performance of audit or oversight functions.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☐ Face-to-Face
☐ Web site
☐ Fax
☐ Telephone Interview
☐ Information Shared Between Systems
☐ Other: *Describe*

D. What is the intended use of the PII collected?

CSAM supports DOI information assurance and privacy functions, documents assessments and information about the configuration, vulnerabilities, weaknesses and security posture of DOI information systems. Employee and contractor name, organization, title and official contact information are collected and used in CSAM to support the DOI information assurance programs to identify officials with responsibility for risk management functions, security authorizations, security or privacy risk assessments, and compliance oversight. These functions support DOI OCIO oversight responsibility, and promotes compliance and accountability in accordance with Federal law, policy and standards.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

DOI bureaus and offices use employee and contractor name, organization, title and official contact information to support information assurance functions and identify officials with responsibility for risk management functions, security authorizations, security or privacy risk assessments, and compliance oversight.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

Records are shared with the DOI Office of Inspector General. Authorized officials within information assurance programs in the DOI OCIO have access to all bureau/office records in CSAM to identify responsible officials and ensure compliance with responsibility for risk management functions.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Metrics and statistical data on IT systems are shared with the Office of Management and Budget, Department of Homeland Security, and Congress during quarterly and annual reports as required by

FISMA. System data may also be shared with the Office of Management and Budget during oversight activities such as those under OMB Circular A-123.

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☒ Contractor: *Describe the contractor and how the data will be used.*

Contractors supporting information assurance functions have limited access to CSAM to perform risk management functions, and are subject to all the same controls and requirements.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

System records may be shared with oversight organizations during audits or reviews of information assurance programs pursuant to Federal law and other requirements.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Individuals generally do not have the right to decline information or to consent to specific uses of information. A DOI employee or contractor must provide minimum required 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.

All 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 DOI to ensure proper monitoring of security and privacy controls in accordance with Federal law, policy and standards.

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided to individuals through the publication of this PIA.

☒ Other: *Describe each applicable format.*

All users are presented with a warning banner that informs them they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data is retrieved by the name of the bureau or office IT system or project. PII is not used to retrieve any records, though authorized CSAM users may run reports that include points of contacts for their accessible IT system records.

I. Will reports be produced on individuals?

☐ Yes: *What will be the use of these reports? Who will have access to them?*
☒ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

System records and artifacts are from DOI sources.

B. How will data be checked for completeness?

Form validation ensures the completeness of data upon account creation. There is no procedure to review data to ensure ongoing accuracy. Documents are updated on an ongoing basis or during the normal compliance artifact life cycle.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

CSAM is DOI's official repository of information systems, and provides the capability to assess, document, manage, and report on the status of information technology for the risk management framework. The purpose of the system is to help DOI maintain compliance with Federal laws and policies. System records are continuously monitored and updated as part of the security authorization process, though there is no standard procedure to review official contact data within artifacts to ensure ongoing accuracy.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Information Technology records are maintained under Departmental Records Schedule (DRS) 1 - Administrative Records, which was approved by the National Archives and Records Administration (NARA) (DAA-0048-2013-001) and may be viewed at: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-the-interior/rg-0048/daa-0048-2013-0001_sf115.pdf. DRS-1.4, Information Technology, covers records that document the Department's creation, management, and use of IT systems and applications, system design and implementation, change management, technological specifications, system security files, maintenance and monitoring records, system documentation, risk management, and all related forms and documents for managing electronic systems. Retention periods vary as records are maintained in accordance with the records schedule for each specific type of record.

Routine short-term IT records related to system maintenance and use that are not needed for extended retention have a temporary disposition. Records are cut off when superseded or obsolete, and destroyed no later than 3 years after cut-off, unless longer retention is required for administrative, legal, audit, or other operational purposes.

System Planning, Design and Documentation short-term records include system security plans, risk assessment and action plans, test files, control measures, and other IT system documentation have a temporary disposition. Records and are cut off when superseded or obsolete, and destroyed no later than 3 years after cut-off, unless longer retention is required for administrative, legal, audit, or other operational purposes.

Long-term Information Technology records related to the management, planning, and implementation of systems and applications, and related or supporting documents, which are typically created by the OCIO and other reporting program offices have a have a temporary disposition. Records are cut off as instructed in bureau records manual or at the end of the fiscal year, and destroyed no later than 7 years after cut-off, unless longer retention is required for administrative, legal, audit, or other operational purposes.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

The approved disposition methods include shredding or pulping for paper records, and purging, degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a minimal risk to individual privacy as the CSAM system does not collect or maintain sensitive PII. Only employee and contractor name, organization, title and official contact

information are used to identify officials responsible for security authorizations, assessments, and oversight of compliance procedures.

There is a risk of unauthorized access the CSAM system or unauthorized disclosure of system data from CSAM. The risk to privacy is deemed low due to the non-sensitive PII maintained in CSAM and the mitigating controls to prevent unauthorized access or disclosure. Access is limited to authorized users and user activity with the system is monitored. An unauthorized user would need to have DOI network access and a username and password in order gain access. DOI roles within CSAM are restricted to Departmental, bureau or office responsibilities, and are based on least privileges to perform official functions.

CSAM is rated as a FISMA moderate system based on its information types. Security artifacts generally require special handling and are controlled due to the sensitivity of system security information. Mitigating controls include DOI rules of behavior, annual security and privacy awareness training, role-based training, audit logs, encryption, firewalls, and continuous monitoring of security and privacy controls, to ensure the confidentiality, integrity and availability of DOI information and information systems.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

CSAM maintains information about all DOI IT systems and provides the DOI information assurance program officials with the capability to assess, document, manage, and report on the status of information technology (IT) for security authorization processes in the risk management framework.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

User access is based on least privileges and limited to the systems within their bureau or office.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are involved in supporting DOI systems and information assurance processes and are subject to the same requirements and standards as Federal employees. Some relevant controls are inherited from DOJ.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

CSAM data input and changes can be tracked through database logging and auditing functions. Access and changes to CSAM data is captured in audit logs that are assigned to privileged individuals with appropriate system roles to monitor the audit logs. Audit logs are designed to be checked on a routine basis and monitored by system administrators.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

- All access activity (e.g., unsuccessful login attempts, date/time of access, etc.)
- Changes to CSAM data

M. What controls will be used to prevent unauthorized monitoring?

Access to system is limited to authorized DOI personnel. Audit logs are only accessible to privileged users with the appropriate system roles to monitor the audit logs. Personnel must complete annual security and privacy awareness training, role-based training, and acknowledge DOI Rules of Behavior.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☐ Locked File Cabinets
☒ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Compliance and Audit Management Branch Chief serves as the Information System Owner and the official responsible for oversight and management of the CSAM security and privacy controls and the information processed and stored by the system. The Information System Owner and Information System Security Officer share responsibility for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within the system, in consultation with DOI Privacy Officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The CSAM Information System Owner is responsible for the daily operational oversight and management of CSAM program security and privacy controls, and for ensuring to the greatest possible extent that data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Information System Owner, Information System Security Officer, and authorized users are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and for working with the Departmental Privacy Officer to ensure appropriate remedial activities are taken to mitigate any impact to individuals.