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) Decommissioning
Bureau/Office: Office of the Chief Information Officer
Date: March 7, 2023
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 was the Department of the Interior's (DOI's) official government risk and compliance system. CSAM maintained the Department-wide repository of information systems and provided the DOI cybersecurity 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 provided 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. CSAM is a Department of Justice (DOJ) system that provided 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 was a site-to-site Virtual Private Network (VPN). The DOI CSAM instance was managed by the Cyber Governance Branch within the Cybersecurity Division (CSD), Office of the Chief Information Officer.

CSAM is being decommissioned in 2023 as it was replaced with a new government risk and compliance system, Xacta 360. DOI has developed a decommissioning plan to ensure privacy, security and records requirements are met.

- **Software Archive:** CSAM is hosted within the DOJ Data Center. Therefore, there is no on-premise software in DOI that requires to be archived.
- **Documentation Archive:** User documentation was migrated to Xacta 360 but had to be recreated for the new environment. System authorization and security documentation is archived in Xacta. The system cannot be re-initiated, as the contract has ended.
- **Hardware Disposition:** CSAM is hosted within the DOJ Data Center. Therefore, DOI has no hardware or equipment that require sanitization or disposal.
- **Data Archive:** CSD will manage the migration of all bureau/office system data to Xacta 360 prior to the decommissioning of CSAM.
- **Security:** System security and access rights to CSAM cannot be reconstituted within Xacta. However, security and associated rights managed by OCIO were duplicated in Xacta.
- **Decommission Risks:** There are no associated risks or challenges to decommissioning CSAM. All data and applications will be verified as migrated and approved by bureau/office Associate Chief Information Officers.

There is minimal risk to individual privacy as CSAM system does not collect or maintain sensitive PII and the mitigating controls in place to prevent unauthorized access or disclosure. 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. Access is limited to authorized users and user activity with the system is monitored. DOI roles within CSAM are restricted to Departmental, bureau or office responsibilities, and are based on least privileges to perform official functions.

Security artifacts in CSAM generally require special handling and are controlled due to the sensitivity of system security information. Mitigating controls include DOI Rules of Behavior, annual security, privacy, records management, Section 508, Paperwork Reduction Act, and Controlled Unclassified Information awareness training, role-based privacy and security training,

audit logs, encryption, and firewalls ensure the confidentiality, integrity and availability of DOI information and information systems.

DOI completed a privacy impact assessment (PIA) for Xacta to assess any privacy risks related to the use of the system. The Xacta 360 PIA may be viewed on the DOI PIA website at https://www.doi.gov/privacy/pia.

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: 010-000000323; Cyber Security Assessment and Management System Security and Privacy Plan

☐ 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