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: Xacta 360
Bureau/Office: Office of the Chief Information Officer
Date: April 29, 2022
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?

Xacta 360 is the Department of the Interior's (DOI's) official repository of information systems, which provides 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). Xacta 360 will provide 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 Department's instance is managed by the Cyber Risk Management Branch, Cybersecurity Division within the Office of the Chief Information Officer (OCIO). Xacta 360 is replacing the Cyber Security Assessment and Management (CSAM), a system managed by the Department of Justice (DOJ).

Xacta 360 was developed by Telos and is hosted in the Cybersecurity Division hosting environment on premise in the Albuquerque Data Center. Authorized users can only access the system when directly on a DOI managed network or the DOI Virtual Private Network.

Xacta 360 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 (NIST) and Office of Management and Budget (OMB) guidance
- Supports system inventory management
- Manages the Plan of Action and Milestones (POAM) process
- Supports FISMA reporting
- Provides security oversight and compliance
- Provides security Assessment and Authorization (A&A)
- 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 et seq.

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. A System Privacy Plan is being developed for the Xacta 360 system.

☐ 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.*

Xacta 360 does not collect, process or maintain sensitive personally identifiable information (PII) on individuals. Only official contact information on employees, contractors, and auditors is collected, such as name, bureau/office, title, work address, work email address, and work phone number. This information will be used to identify officials with responsibility for risk management functions, security authorizations, security or privacy risk assessments, audits, and compliance oversight. Only authorized users will have access to Xacta 360 based on least privilege.

DOI employees use their government issued Personal Identity Verification (PIV) card. A user is authenticated via their government issued PIV card by way of their PKI certificate/string. The user's PKI certificate/string must be associated with an account to grant access to Xacta 360. If there is no account associated with the PIV being used to access the site, the user will not be granted access. The PKI certificate/string must be captured by the Xacta administrators and associated with an account. Once this is completed, the user can utilize their PIV to authenticate to Xacta 360.

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*

Data from CSAM system will be migrated to Xacta 360. DOI personnel with authorized access can update their official contact information in Xacta 360. DOI IT systems, program performance audit or oversight records may be provided by organizations supporting the Department's A&A process. DOI employees and contractors access Xacta 360 by signing in with their AD credentials or DOI PIV card.

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

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

The Xacta Support Team will be utilizing two methods to facilitate the migration of CSAM system data into Xacta 360. The first method is importing data from the CSAM database provided by the DOJ into Xacta's database. This is a manual approach and will require tailoring of the received data to be acceptable to the Xacta 360 database schema. The second method is a manual approach which utilizes a combination of reports from CSAM and manual entry. The aforementioned reports will be utilized to import data into Xacta 360, such as equipment inventory, controls implementation, POAMs, etc. The manual entry component of this process

refers to system description information, control inheritance linkages, POAM milestones, etc. After the migration is completed, electronic records are uploaded, and information manually updated by authorized officials as needed.

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

The purpose of Xacta 360 is to support DOI's security and privacy functions and document assessments and information about the configuration, vulnerabilities, weaknesses, and security posture of DOI information systems. DOI employee name, bureau/office, title, and official contact information will be collected and used in Xacta 360 to identify the responsible officials for the systems. This information will identify DOI officials with responsibility for risk management functions, security authorizations, security or privacy risk assessments, and compliance oversight 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.*

Authorized officials within the CSD, OCIO have access to all bureau/office records in Xacta 360 to identify responsible officials and ensure compliance with responsibility for risk management functions.

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

Records are shared with the DOI Office of Inspector General for audit purposes. DOI bureaus and offices will use PII data to identify officials with responsibility for risk management functions, security authorizations, security or privacy risk assessments, and compliance oversight. Bureaus and offices may only see system records for their organization's systems.

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

Metrics and statistical data on IT systems are shared with OMB, Department of Homeland Security, and Congress during quarterly and annual reports as required by FISMA. System data may also be shared with OMB 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.*

Data is not shared with Telos or any of its external partners or systems. Telos will have access to the data only for technical support purposes. DOI contractors supporting security and privacy

offices have limited access to Xacta 360 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 security 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 Xacta 360 to perform official duties. This information is voluntarily provided during the Xacta 360 account creation process, and individuals who decline to provide requested information will not be provided access to Xacta 360.

All other individuals involved in information system security functions may have their name, title, organization, and contact information captured by the system, or entered by a user, and used within the system or within related system artifacts, without specific awareness or consent. However, these officials are aware of their roles in the risk management framework and the responsibility to be identified in or to sign security or privacy compliance documents. 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 privacy impact assessment (PIA).

☒ Other: *Describe each applicable format.*

A warning banner will be displayed that informs users 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.).

The name of the bureau or office IT system or project will be used to retrieve data in Xacta 360. Reports run in the tool may include official contact information for security and privacy roles assigned to a system. PII data will not be used to retrieve information in Xacta 360.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Xacta does not generate reports on individuals. System reports may contain responsible official's names, email address, work phone number, work address, and role. These records will be accessible to System ISSOs and may be distributed to System Owners and Authorizing Officials. However, Xacta 360 collects audit logs where individuals' names may be listed as associated with a system and the user activity. These audit records may only be accessed by Bureau Administrators.

☐ No

Section 3. Attributes of System Data

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

PII data is restricted to official contact information on DOI employees, contractors, and auditors. Information is maintained and updated by system users. In order to maintain the accuracy of the user information, Xacta system administrators review user accounts bi-weekly. Any anomalies are addressed and resolved by contacting the user, and modifying their user data, or by removing their access if no longer required. Under this process, outdated and inaccurate PII for users is identified and deleted. Only Xacta system administrators can create or modify user accounts. Activities of all users including system administrators are logged.

B. How will data be checked for completeness?

Data input 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).

Xacta 360 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). 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 Departmental policy.

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 Xacta 360 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 to the Xacta 360 system, unauthorized disclosure of system data from Xacta 360 or usage for unauthorized purposes. The risk to privacy is deemed low due to the non-sensitive PII maintained in Xacta 360 and the mitigating controls to prevent unauthorized access or disclosure or for unauthorized purposes. Access is limited to authorized users and user activity with the system is monitored. DOI roles within Xacta 360 are restricted to Departmental, bureau or office responsibilities, and are based on least privileges to perform official functions.

Telos has a Master Administrator role in Xacta 360 and has full control of all users, projects, and security settings. Bureau/office Administrators manage the users and projects in their respective bureau/office. The role of the Bureau Administrators will be migrated from CSAM. All user activity is tracked via the Xacta audit logs which are captured by DOI's Security Information and Event Management (SIEM) tool to collect and manage log data. Information collected includes logs from servers and databases, security components, including asset management tools, vulnerability data, and malware alerts, and infrastructure and other network equipment. These audit logs are only accessible by the SIEM officials and Bureau Administrators. Users may submit an account request via DOI's IT helpdesk. The individual requesting the account must provide the appropriate certificates indicating completion of the Xacta overview course which is required for all users, and role-specific Xacta training as necessary.

Bureaus/offices may only access their organization's system records. Auditors will only have access to the records in Xacta 360 for the duration of the audit. Access to the system will be removed after the audit is complete. The Xacta360 software disables inactive accounts after 45 days. In addition to that, the user of the account is notified 15 days prior to the account being disabled.

Xacta 360 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, privacy, records management, Controlled Unclassified Information (CUI), Section 508, and Paperwork Reduction Act 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. The system is reauthorized every three years based on the results of an independent assessment. Security controls are tested annually by an independent assessor. All DOI staff and contractors must complete annual security awareness and privacy training. In addition, DOI contractors are subject to background checks prior to obtaining access to DOI systems.

There is a risk that records in Xacta 360 may be maintained longer than necessary. Records are maintained and disposed of under a NARA approved records schedule. Information collected and stored within Xacta 360 is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

There is a risk that individuals may not receive adequate notice. Notice is provided through the publication of this PIA. There is also a warning banner informing individuals 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.

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*

Xacta 360 will provide a department-wide view of the status of information system security and privacy posture and the 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. This information will be included in any audits conducted on a system.

☐ 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. This system does not derive new data or create previously unavailable data about an individual through data aggregation.

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. The Xacta system implements security controls per NIST SP 800-53 to protect the system and information. Xacta resides on a server located in a secure, access-controlled room at the DOI

Albuquerque Data Center. Unauthorized individuals may not access the physical equipment on which the system resides. Electronic access to Xacta is available only through the DOI network. The Bureau Administrators can create accounts for users within their organizations. Role-based access is used to ensure only authorized users have access to system records through the use of their PIV cards.

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?*

☒ No

Privacy Act contract clauses were not included in the contract. Xacta is not a Privacy Act system. DOI will work with contracting officials to include the appropriate privacy clauses and terms and conditions.

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*

Access and changes to records in Xacta 360 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 routinely and monitored by system administrators. Privilege User activities are captured in the Splunk audit logs for Xacta as well as General Users activities. This includes file modification, user account creation and user access, etc.

☐ No

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

All access activity such as unsuccessful login attempts, and date/time of access, etc. are collected on users. Any changes to Xacta data are documented in the system and monitored by system administrators.

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

Access to system is limited to authorized DOI personnel. Audit logs are only accessible by the SIEM personnel and Bureau Administrators who are responsible for monitoring the audit logs. Personnel must complete annual security, and privacy, records management, and CUI awareness training, role-based privacy and security 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 Chief, Cyber Governance Branch serves as the Information System Owner and the official responsible for oversight and management of the Xacta 360 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, and addressing any privacy complaints, 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 Xacta 360 Information System Owner is responsible for the daily operational oversight and management of Xacta 360 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.