



U.S. Department of the Interior DECOMMISSIONING PRIVACY THRESHOLD ANALYSIS

Introduction

The Department Privacy Office ensures that system decommissioning activities comply with current federal privacy regulations and standards, effectively mitigating risks associated with Personally Identifiable Information (PII) and maintaining comprehensive documentation. The DI-4025 Decommissioning Privacy Threshold Analysis (DPTA) form aligns with federal privacy and security compliance requirements outlined in Section 208 of the E-Government Act of 2002, the Federal Information Security Modernization Act (FISMA), Office of Management and Budget (OMB) Circular A-130, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, and NIST SP 800-37 Rev. 2.

This DPTA ensures that the retirement or transition of federal systems, applications, or services is conducted securely, preventing unauthorized access or disclosure of PII, ensuring adherence to National Archives and Records Administration (NARA) records retention schedules, and maintaining compliance with data sanitization requirements described in NIST SP 800-88, Guidelines for Media Sanitization. The analysis documented by this DPTA provides essential evidence of due diligence in meeting federal cybersecurity, privacy, and data disposition mandates throughout the decommissioning lifecycle. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our [Privacy Office Support Request Page](#). For further guidance, consult the [DOI PTA Guide](#).

Section 1: System Information

System Information

System: Xacta 360
System Acronym: Xacta 360
Date submitted for review: May 19, 2026

System Manager

Name: Alex Bahramzadeh
Title: Senior Cybersecurity Specialist
Bureau: OCIO
Phone: Microsoft Teams
E-mail: alex_bahramzadeh@ios.doi.gov

Information Systems Security Officer

Name: Reginald Butler
Title: Cybersecurity Specialist
Bureau: OCIO
Phone: Microsoft Teams
E-mail: rbutler@ios.doi.gov

1. What was the purpose of the system?

Xacta 360 served as the Department of the Interior's (DOI's) official repository of information systems, providing cybersecurity and program officials with a secure, web-based 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 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. DOI adopted Xacta 360 to replace the Cyber Security Assessment and Management (CSAM) system managed by the Department of Justice. The DOI-managed instance of Xacta 360 was developed by Telos, hosted on-premises in the Cybersecurity Division hosting environment at the Albuquerque Data Center, and managed by the Cyber Risk Management Branch, Cybersecurity Division, Office of the Chief Information Officer (OCIO). Authorized users could access the system only while connected to a DOI managed network or through the DOI Virtual Private Network.

Xacta 360 supported the following functions:

- Processing, storing, and reporting DOI IT Security Program information
- Leveraging National Institute of Standards and Technology (NIST) and Office of Management and Budget (OMB) guidance through an enterprise-wide tool
- Managing system inventory
- Managing the Plan of Action and Milestones (POA&M) process
- Supporting FISMA reporting
- Enabling security oversight and compliance
- Supporting security Assessment and Authorization (A&A)
- Providing privacy oversight of compliance activities
- Supporting the continuous monitoring process

As part of a planned, policy driven lifecycle transition, the on-premise version of Xacta 360 was decommissioned to ensure legacy systems comply with federal security, privacy, and data disposition requirements. DOI transitioned to the cloud-hosted Xacta 360 Software-as-a-Service (SaaS) offering.

2. Why is the system being decommissioned?

This was part of a planned, policy-driven lifecycle closure to ensure all legacy systems meet federal security, privacy, and data disposition requirements. Xacta 360 was retired and replaced by Xacta 360 SaaS (i.e., Bison Governance, Risk and Compliance (GRC), covered by separate privacy compliance documentation).

3. What bureaus or offices were using this system?

The on-premise system was used by all bureaus and offices within DOI.

4. Was this system internally developed or a third-party service?

- ☐ Developed Internally
☒ Third-Party Service

5. Is this a cloud-based system?

- ☒ No
☐ Yes

6. List associated privacy compliance documentation, if applicable:

System of Record Notice(s): N/A – Xacta 360 did not create a Privacy Act system of records.

Privacy Impact Assessment PIA(s): Xacta 360 (Filename: Xacta 360 PIA_final_04292022)

Section 2: PII & Data Disposition

1. Did the system contain, process, transmit, store, archive, or manage PII, including login credentials, authentication information, account identifiers, or other individual-linked technical identifiers?

- ☐ No, Skip to Section 6.
☒ If yes, what type(s) of PII?

- | | | |
|--|--|---|
| ☒ Name (full, first or last) | ☐ Home telephone number | ☐ Employment or resume info |
| ☐ Aliases/nickname | ☐ Personal Email | ☐ Full or Truncated SSN |
| ☐ Driver's license | ☐ Mailing or home address | ☐ Physical characteristics |
| ☐ Citizenship | ☐ Religious preference | ☐ Biometrics/facial recognition |
| ☐ Legal Status | ☐ Mother's maiden name | ☐ Vehicle information |
| ☐ Sex | ☐ Marital status | ☐ Passport information |
| ☐ Race or ethnicity | ☐ Spouse Information | ☐ Travel information |
| ☐ Date of birth | ☐ Child or family information | ☐ Parent's name |
| ☐ Place of birth | ☐ Emergency contact info | ☐ Credit card number |
| ☐ Personal cell phone number | ☐ Financial information | ☐ Nationality |
| ☒ Username / user ID / acct ID | ☐ IP address / network ID | ☐ Device ID / online ID |
| ☐ Geolocation / GPS / location | ☐ Photos / video / audio | ☐ Health / medical information |
| ☐ Tribal or other ID number | ☐ Education information | ☐ Disability Information |
| ☐ Criminal / disciplinary info | ☐ Military records | ☒ Other: Describe below |

Only the official contact information of employees, contractors, and auditors was collected (i.e., name, bureau/office, title, work address, work email address, and work phone number). This information was used to identify officials with responsibility for risk management functions, security authorizations, security or privacy risk assessments, audits, and compliance oversight.

Page | 3 Records Management:

This document is maintained in accordance with applicable Department of the Interior and National Archives and Records Administration (NARA)–approved records schedules, including General Records Schedule (GRS) 4.2, as appropriate.

Note: For decommissioning purposes, treat usernames, account identifiers, credentials, access tokens, audit records tied to individual users, and similar authentication data as PII when linked to a specific individual.

2. Did the system contain workforce or public login credentials, authentication data, access tokens, certificates, or user-linked account records?

- | | |
|--|--|
| ☒ Yes – workforce only | ☐ Yes – members of the public |
| ☐ Yes – mixed workforce and public users | ☐ No |
| ☐ Derived analytics (e.g., engagement trends) | |

Authorized DOI employees and contractors accessed the on-premise Xacta 360 by signing in with their Active Directory (AD) credentials or DOI Personal Identity Verification (PIV) card. During decommissioning, active credentials were revoked and account records were exported for retention where required.

3. What was the source of the PII?

- | | |
|--|---|
| ☒ User-submitted (e.g., contact forms) | ☐ Publicly visible profile data |
| ☐ Automatically collected (e.g., cookies, trackers) | ☒ Other: <i>Specify below</i> |
| ☐ Derived analytics (e.g., engagement trends) | |

PII was obtained from DOI employees and contractors, DOI records, and records associated with DOI information systems and the A&A process. Personnel seeking Xacta 360 accounts provided information necessary to establish and maintain their accounts and accessed the system using DOI AD credentials or PIV authentication. Official contact information and information identifying officials responsible for security, privacy, risk management, authorization, audit, and compliance functions could also be entered or maintained as part of system records and compliance artifacts.

4. Did the system collect, process, or retain information on: (Please check all that apply)

- | | |
|---|--|
| ☒ Federal Employees | ☐ Volunteers |
| ☒ Contractors | ☒ Other (Describe) |
| ☐ Members of the Public | |

The on-premise instance of Xacta 360 did not collect, process or maintain sensitive PII on individuals. Only the official contact information of employees, contractors, and auditors was collected for authorized purposes such as risk management functions, security authorizations, security or privacy risk assessments, audits, and compliance oversight.

5. How was PII used in the system? “(See latest approved PIA for details)”

The purpose of Xacta 360 was 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. Official contact information on employees, contractors, and auditors was collected and used in the on-premise instance of Xacta 360 to identify the officials responsible for the systems, as well as risk management functions, security authorizations, security or privacy risk assessments, and compliance oversight in accordance with federal law, policy, and standards.

6. What is the NARA-approved schedule(s) for data in the system?

Records are maintained under Departmental Records Schedule (DRS) 1 - Administrative Records (DAA-0048-2013-001), 1.4 – Information Technology. Information Technology Records under DRS 1.4 document the Department’s creation, management, and use of IT systems and applications to automate office functions, whether strictly administrative or not. Such records include 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.

Short-term Information Technology Records related to system maintenance and use that are not needed for extended retention (items 0013-0014) 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.

Long-term Information Technology Records related to the management, planning, and implementation of systems and applications, and related or supporting documents (item 0015) 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.

7. Have any unscheduled records been identified for data in the system? (if yes, describe the plan for scheduling or disposition)

No, there are no unscheduled records.

8. Has PII been transferred to another system or archived according to the records retention policy?

- ☒ Transferred to another system:
- ☒ Archived according to the records retention policy

Legacy records from the on-premise Xacta 360 environment were successfully transferred to the successor system, Bison GRC, and a post-migration data integrity review was conducted to verify completeness and accuracy. In addition, required audit logs, configuration records, and encrypted system backups have been

retained in controlled archival storage in accordance with the applicable Departmental Records Schedule. All user access to the decommissioned environment has been revoked, and no active accounts or interactive access remain.

9. If there are paper records associated with the system, please explain how the paper records will be handled.

N/A – There are no paper records associated with the system.

10. If PII has been deleted, were NIST SP 800-88: Guidelines for Media Sanitization methods used?

- ☒ No: *Provide justification why and a timeline for completion*
☐ Yes

Required Xacta 360 records containing PII were migrated to the successor system, Bison GRC, and are maintained there in accordance with applicable records retention requirements. In addition, OCIO Hosting Services retains a recoverable copy of the decommissioned Xacta 360 environment for one year following system retirement. Accordingly, PII contained in those retained records has not been deleted.

As part of decommissioning, user access to the legacy Xacta 360 environment was revoked, credentials and access-related information associated with the retired environment were removed as part of deprovisioning, and the active on-premises virtual hosting environment was removed from service.

At the end of the one-year retention period following the January 2026 system retirement, the retained legacy system copy will be disposed of in accordance with the applicable records retention requirements and DOI media-sanitization requirements. The appropriate sanitization method will be applied to the retained media when final disposition occurs.

11. Were users notified about the data disposition or system decommissioning?

- ☐ No: Explain
☒ Yes

Users were notified via agency-wide email messages and an in-system banner message two months prior to shutdown. The notice included key dates, data migration instructions, and points of contact for follow-up.

Section 3: System Dependencies & Third-Party Services

1. Does this system have any dependencies on other systems?

- ☐ No
☒ Yes

The system relied on DOI's AD for authentication. This dependency has been decoupled, and directory access has been revoked as part of the system shutdown process.

2. Are there any third-party service providers involved in system operations?

- ☐ No
☒ If yes, have contracts been reviewed for termination?

Telos developed the on-premise Xacta 360 platform and had a Master Administrator role with full control of all users, projects, and security settings. However, no third-party vendors participated in the decommissioning of Xacta 360 and the platform was independent of any Telos systems. All decommissioning tasks—including data migration to Bison GRC, system shutdown, and secure removal of infrastructure—were performed entirely by DOI personnel. All contractual privacy obligations were satisfied, and Telos's administrative access to the on-premise system concluded with system shutdown.

3. Were there any interconnections to external systems that required decommissioning?

- ☒ No
☐ Yes: *List the Connections and their decommissioning date*

4. If the system was cloud-based, has data been deleted per the cloud provider's policies?

- ☒ No
☐ Yes

N/A – the decommissioned Xacta 360 environment was hosted on-premises.

5. Have all data-sharing agreements (DSAs) and Memorandums of Understanding (MOUs) been reviewed and terminated?

- ☒ No
☐ Yes

N/A - No DSAs or MOUs requiring termination were identified for the decommissioned environment.

Section 4: Security & Compliance

1. Have all user accounts been disabled and access revoked?

- ☐ No: *Provide justification why and a timeline for completion*
☒ Yes

2. Has an exit security assessment been conducted by the ISSO?

- ☐ No
☒ Yes

The ISSO completed the final security review and decommissioning checklist on May 19, 2026. No outstanding vulnerabilities were noted. Completed deprovisioning activities were validated as part of the final security review.

3. Has a penetration test or vulnerability scan been conducted before decommissioning to identify residual risks?

- ☒ No
☐ Yes

No. A penetration test or vulnerability scan was not conducted specifically for decommissioning. The on-premises virtual hosting environment was subsequently removed in its entirety, eliminating residual exposure from the retired system environment.

4. Have all cryptographic keys and access credentials been securely deleted?

- ☐ No
☒ Yes
☐ N/A

All cryptographic keys and access credentials associated with the on-premise Xacta 360 environment were securely deleted as part of the deprovisioning process. The system's on-premise virtual hosting environment was fully removed, and any remaining key material or credential stores were deleted. No residual access paths or credential repositories remain in the decommissioned environment.

5. Has an audit of the system's last active logs been conducted before decommissioning?

- ☒ No
☐ Yes

No. A separate final audit of the last active system logs was not completed before shutdown. Following decommissioning, the on-premises virtual environment was removed and active logs are no longer available in that environment. Required audit records were retained separately in accordance with applicable records requirements.

6. Have all audit logs, configurations, and system documentation been retained per NARA General Records Schedule (GRS) 3.2 – Information System Security Records?

- ☐ No
☒ Yes
☐ N/A

Hosting will retain copies of the system, including system configuration files, security documentation, and audit logs, for one year. Records required for continued operational use were migrated to the Bison GRC Authority to Operate system.

7. Briefly describe any privacy risks associated with the decommissioning of this system and how information will be handled (e.g., destroyed, archive, transferred, etc.). For each risk identified, please indicate how that risk will be mitigated. "See current approved PIA for insight"

Privacy risks associated with decommissioning included the potential for unauthorized access to legacy records during migration, incomplete transfer of records to the successor system, and retention of legacy records or system copies longer than required. These risks were mitigated by transferring required records to Bison GRC, validating the migration as appropriate, revoking access to the on-premises Xacta 360 environment, removing the legacy virtual hosting environment from active service, and retaining any required archival records or system copies in controlled storage for only the applicable retention period. Records will be disposed of in accordance with applicable NARA-approved records schedules and DOI security and media-sanitization requirements.

Section 5: Final Approval

1. Who conducted the final review to confirm that all closure tasks, including data deletion and system/service retirement, were completed?

Theresa Beazer, System Owner, conducted the final system-owner review to confirm completion of the required decommissioning activities, including migration of required records to the successor environment and removal of the legacy on-premises environment from active service.

2. Were all required stakeholders (Privacy, Security, Records Management, IT, System Owner, Risk Manager) involved in sign-off?

- ☐ No
☒ Yes

All relevant stakeholders participated in the final decommissioning review and signed off on closure documentation, including representatives from Privacy, IT Security, Records Management, the System Owner, and Risk Management.

3. Who has been designated as the custodian of archived data?

Name: Alex Bahramzadeh
Title: IT Security Specialist/Bison GRC System Owner
Office: OCIO
Phone: (303) 445-2626
E-mail: alex_bahramzadeh@ios.doi.gov

The System Owner for Bison GRC, as the successor system, is the custodian of the Xacta 360 records that were migrated to and are maintained in Bison GRC. The OCIO Hosting Services team separately retains and safeguards a recoverable copy of the decommissioned on-premises Xacta 360 environment for one year following the January 2026 retirement. During that one-year period, the former Xacta 360 System Owner may assist in coordinating a recovery request if legacy data must be restored; however, the former Xacta 360 System Owner is not the custodian of the migrated records. At the end of the applicable retention period, the retained legacy copy will be disposed of in accordance with applicable records retention and media-sanitization requirements.