PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO Roster.docx

System Name: XACTA Cloud		**System Owner: Dylan Mitchell**	
Preparer: Dylan Mitchell/Helen Lewis		**Office:** OFA-CRMS	
Date: 6/12/2026		**Phone: (202) 566-1328**	
Reason for Submittal:			
New: ☐	Revised: ☐X	Annual Review: ☐	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: ☐X	Rescindment/Decommission: ☐		

Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).

Provide a general description/overview and purpose of the system:

Xacta Cloud is the EPA's "System of Record" for documenting and managing information and privacy risk processes for systems that support the Agency's mission and operations. Xacta Cloud is a Commercial Off-The-Shelf (COTS) Java and Oracle-based Federal Information Security Management Act (FISMA) Risk Management Framework (RMF) application. It enables the Office of Information Security and Privacy (OISP) to automate the processes involved in complying with government security mandates and allows OISP security professionals to provide a faster and more accurate response to review requests and audits from senior management, Office of Inspector General (OIG) and Office of Management and Budget (OMB). It is used internally by EPA personnel as a repository for managing EPA IT system security documentation (e.g., security control implementations, system security plans

(SSP's), security assessment reports (SARs), contingency/disaster recovery (CP/DR) plans, etc.), asset inventory data (e.g., hardware/software), vulnerability compliance and Plan of Actions and Milestones (POA&M's). Xacta Cloud is also used to conduct testing of security controls as required under FISMA and to maintain a record of the test results. The system is also used to document and maintain the remedial actions, i.e., Plans of Action and Milestones (POA&Ms), to address the deficiencies identified during the testing, which is also required by FISMA.

Xacta Cloud allows for IT asset information to be collected seamlessly from a variety of sources. It identifies, tracks, tests, and helps remediate security risks from the system up to the enterprise level and continuously monitors and audits compliance with the appropriate standards. Xacta increases efficiency and effectiveness in security authorization productivity through organizational improvements. Standardization, automation and organizational transparency are fundamental to Xacta. Xacta Cloud resides in the EPA AWS East/West Common and AWS ECHS.

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

- Federal Information Security Modernization Act of 2014, Public Law 113- 283, chapter 35 of title 44, United States Code (U.S.C.)
- OMB Circular A-130, "Management of Federal Information Resources," July 2016

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have, or will the system be issued an Authorization-to-Operate? When does the ATO expire?

ATO will expire on January 31, 2027.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR is required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FEDRAMP approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes. Xacta Cloud resides in the EPA AWS East/West Common and AWS ECHS. The primary location for the EPA AWS ECHS is US East (Northern Virginia).

Section 2. Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

The system collects data elements as follows: EPA Employee/Contractor First and Last Name, Office Phone Number, Home and Mobile Phone Number, Office Address, Work Email Address.

2.2 What are the sources of the information and how is the information collected for the system?

System documentation and IT inventory data is inputted by responsible system security personnel. Individuals may also upload system security documents associated with system certification, assessment and authorization processes. These include POA&Ms, SSPs, SARs, CPs and testing artifacts which may include names, phone numbers, email addresses and building addresses.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

NO

2.4 Discuss how accuracy of the data is ensured.

All information entered into Xacta is reviewed by the SO and ISSO for accuracy.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included

Privacy Risk:

Privacy risk is introduced by copying sensitive Agency data into the Platform. The ETL There is a risk of unauthorized use or compromise of PII and SPII or processing of inaccurate information due to processing errors and/or modification during maintenance.

Mitigation:

We deploy security and privacy controls from NIST 800-53 to secure PII and SPII processed by the system. Review of all documents and artifacts by supervisors prior and after entry as well as the use of input validation ensures accuracy.

Section 3. Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place, why have they been omitted?

This system utilizes role-based controls to prevent users from accessing information for which they do not have a need to know. System users are assigned roles based on their pre-determined A&A position (See: EPA Roles and Responsibilities Procedure). Each non-privileged account is only able to access certain fields within each project and restricted from viewing the account information of any other user. There are no temporary/emergency or group accounts. Privileged users are closely monitored, and the number of accounts limited based on need. In addition, system users are only granted access to folders and projects they are actively working on. The system's Primary Information Security Officer (PISO) grants this assignment only after written approval. Accounts are deactivated after 30 days of inactivity and upon removal of system responsibility.

Xacta Cloud Privileged Roles:

- Master Administrator
- Administrator
- Xacta cloud non-privileged

Roles:

- Auditor
- Power User
- User- Most users fall in this category. This role is further divided to limit access to specific tasks within projects:
  - Information Security Officer (ISO)
  - Information Security Officer (ISO) – Backup
  - Information Management Officer (IMO)
  - Information Owner (IO)
  - System Owner (SO)
  - System Owner (SO) – Backup
  - Information System Security Officer (ISSO)
  - Auditor

- Service Manager (SM)
- Authorizing Official (AO)
- Chief Information Security Officer (CISO)
- Privacy Officer (PO)
- Security Control Assessor (SCA)
- Authorizing Official Designated Representative (AODR)
- OISP Support Contractor

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Xacta implements access controls specified in EPA's Access Control Procedure. Other source documents are:

- XACTA Administration SOP_v2.5.docx
- Xacta 360 Admin Manual_v1.6.4.pdf
- Web Application Access Account Set Up v2.2.pdf
- Xacta Authentication Method v3.0.pdf

3.3 Are there other components with assigned roles and responsibilities within the system?

NO

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

This system is for internal EPA (government and contractor) use only. There are no external parties. The public does not have access to Xacta Cloud. User access to information is role-based. Only Xacta Cloud Administrators can view PII contained within the application. General user accounts are limited to accessing only assigned projects and any PII contained within.

EPA Acquisitions is responsible for adding the applicable FAR regulations to EPA contracts: FAR 52.232-8, Federal Acquisition Regulation (FAR) Subpart 42.15, FAR 31.205-43, FAR 31.205-46, FAR 52.252-2, FAR 52.209-5, FAR 52.209-7, FAR 52.209-9, FAR 52.217-5, FAR 52.217-8, FAR 52.217-9, FAR 52.224-1, FAR 52.224-2, FAR 52.232-25, FAR 52.232-33, FAR 52.232-99, FAR 52.237-3, FAR 52.239

4, and FAR 52.253-1

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

EPA Records Schedule 0090 and EPA Records Schedule 1012

https://www.epa.gov/sites/production/files/2019-08/documents/20190809_epa_records_schedules_in_final_status.pdf

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system

Privacy Risk:

There is risk that information may be maintained longer than authorized or needed.

Mitigation:

System documentation (especially the retention schedule) is reviewed periodically to ensure information is not retained longer than needed and that processing authority is current.

Section 4. Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local governments, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

NO

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

N/A

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

N/A

4.4 Does the agreement place limitations on re-dissemination?

N/A

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

Mitigation:

Section 5. Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

Procedures are in place to regulate assignment of roles and to ensure that user account information is only modified as appropriate. Users take mandatory annual Information Security and Privacy Training. System documentation (esp. PIA) is reviewed periodically, and the system is assessed periodically or as needed to ensure that system and information use is compliant. The system is also subject to continuous monitoring per the NIST RMF process.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

Users take the following mandatory training at least annually:

- EPA Information Systems Security and Privacy Awareness Training.
- System Owners Incident Handling Training.
- EPA Records Management Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

This is a function of the Agency source systems that collect the data. This is an agency requirement to ensure all employees take the annual Security and Privacy Awareness Training.

Privacy Risk:

There is a risk of failure of audit logging and unauthorized changes to system configuration that could result in a compromise (modification, exfiltration or misuse of PII).

Mitigation:

System audit logs are maintained and reviewed in accordance with EPA's Audit and Accountability (AU) procedure.

Section 6. Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

The primary reason the PII is maintained is to have contact information for the system. Xacta Cloud maintains employee and contractor information, including user first and last name, office and mobile phone numbers and email address to grant and maintain users' access. Xacta Cloud maintains personal information as described in section 2.2 as required for A&A, retains user information for systems, and to further control access to process steps.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: ☐ No: X☐ If yes, what identifier(s) will be used.

A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.

The only way to view system information is to go into "project personnel" which is used to generate the SSP, "POA&M Elements" which track vulnerability compliance, or to view an artifact in "Manage Project Artifacts".

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited

the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

The agency uses the PTA process, this PIA process, and CMA process to evaluate risk to individuals.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

The information might be used in ways outside the pre-determined scope. Information may be modified during maintenance with inaccurate data.

Mitigation:

The agency uses access control process, this PIA process and continuous monitoring of the system to ensure that information in the system is used only for authorized purposes and users. Xacta Cloud is not available to unauthorized users within the secure EPA network. User account information is not able to be viewed or modified by a non-privileged user. Project contact information will only be modified by individuals with authorization to do so (see Section 3.2). In addition, all EPA employees and contractors are required to attend Security Awareness and Record Management Training upon hire and annually thereafter. This training includes guidance on the appropriate use of PII. Users are mandated to read and agree to adhere to IT Rules of Behavior. Audit logs are maintained to ensure accountability.

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about

him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt-out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information.

Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

N/A

Mitigation:

N/A

Section 8. Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Xact is not a public-facing system. Privacy Act Request procedures that allow individuals to access their information stored in the system for any reason have limited or have no application to Xacta. In general, and for most systems of records documented in Xacta, the PAR procedure is applicable.

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Xact is not a public-facing system. Privacy Act Request procedures that allow individuals to access their information stored in the system for any reason have limited or have no application to Xacta. In general, and for most systems of records documented in Xacta,

the PAR procedure is applicable.

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and Freedom of Information Act (FOIA).

Privacy Risk:

N/A

Mitigation:

N/A

I attest as the Agency Privacy Officer that **XACTA Cloud** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

ROBERT KELLY

Digitally signed by ROBERT KELLY
Date: 2026.08.21 07:51:09 -04'00'

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt. Branch
EPA/OFA