



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: Case Application for Debarment and Suspension (CADS)		System Owner: Christopher Tran	
Preparer: Jamie Lemley		Office: OFA-OCGO	
Date: 05/07/2026		Phone: 202-564-5428	
Reason for Submittal:			
New: <input type="checkbox"/>	Revised: <input type="checkbox"/>	Annual Review: <input checked="" type="checkbox"/>	Rescindment: <input type="checkbox"/>
System Lifecycle Stage(s):			
Definition: <input type="checkbox"/>	Development/Acquisition: <input type="checkbox"/>	Implementation: <input type="checkbox"/>	
Operation & Maintenance: <input checked="" type="checkbox"/>		Rescindment/Decommission: <input type="checkbox"/>	
<p>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).</p> <p>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).</p>			

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

Case Application for Debarment and Suspension (CADS) is the official records management system for case files generated by the EPA’s Suspension and Debarment Program. CADS provides for “cradle to grave” management of all records entered into the system.

Section 1. Authorities and Other Requirements

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

Federal Property and Administrative Services Act of 1949, 41 U.S.C. 251 et seq.; Office of Federal Procurement Policy Act, 41 U.S.C. 401 et seq.; Executive Order 12549 (Feb 18, 1986); and Executive Order 12689 (Aug 16, 1989).

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?

The ATO for the Email and Collaboration Solutions security boundary expires on 10/31/2026

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 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. Microsoft Government Community Cloud (GCC) is a SaaS service that is FEDRAMP approved.

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).

Information collected includes name, DOB, mailing address, SSN, e-mail address, zip code, business activities and associations, and civil and/or criminal history information.

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

Information about an individual respondent (a person, as opposed to an organizational entity) is collected by EPA staff or submitted by the respondent. Information is collected electronically from the respondent, commercial and public databases, publicly available data, and from criminal investigators and other EPA staff in referring offices.

2.3 Does the system use information from commercial sources or publicly available

data? If so, explain why and how this information is used.

The system uses information from commercial databases (LexisNexis) and publicly available data (government websites such as City/County/State websites, SAM.gov, USASpending.gov, BoP.gov, and other publicly available internet sources such as company websites). The information is used to support suspension and debarment actions, which includes identifying a last known address for purposes of providing notice of a suspension or debarment proceeding. The information is also used to list excluded respondents on the System for Award Management (SAM) exclusion database maintained by the General Services Administration, available at www.sam.gov and to verify the identity of individuals listed on SAM.

2.4 Discuss how accuracy of the data is ensured.

Data obtained from commercial and public sources is presumed to be accurate. As needed, Suspension and Debarment Program personnel verify the accuracy of data by coordinating with referring offices, including the EPA Criminal Investigation Division (CID), Office of Inspector General (OIG), Office of Acquisition Services (OAS), Office of Grants and Debarment (OGD), and EPA Regional Offices.

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:

Risk that Suspension and Debarment Program personnel or others will distribute private data from the CADS system.

Mitigation:

Access to CADS is limited to specified EPA personnel. Any document with Confidential Business Information (CBI) or Sensitive Personally Identifiable Information (SPII) is placed in a specially designated "Secure" folder in CADS. Those documents are not released.

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?

Each user in CADS is designated a user function within the system based on their required access and assigned roles. All activities in CADS are tracked by individual, which provides backwards traceability of any changes. CADS is managed by the system administrator who

CUI//ISVI

For Official Use Only (FOUO)

assigns roles and responsibilities within the system to users in the Suspension and Debarment Program. User roles and responsibilities are determined by the Senior Debarring Official (SDO) and the Director of the Suspension and Debarment Division. User access is based on the roles users are assigned in the system.

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

The Access Control List is documented in the SSP. CADS is managed by the system administrator who assigns roles and responsibilities within the system to users in the Suspension and Debarment Program. User roles and responsibilities are determined by the Senior Debarring Official (SDO) and the Director of the Suspension and Debarment Division. User access is based on the roles users are assigned in the system.

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

No. Assigned roles and responsibilities within CADS are provided only to Suspension and Debarment Program personnel. There are no other components within the EPA that have assigned roles and responsibilities within the system.

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?

Only internal EPA federal and contractor technical staff under the EPA Enterprise Managed Application, Infrastructure, Networking, Enterprise, and Security Services (MAINES) contract have access to CADS data/information. Since this is a federal enterprise contract the required FAR clauses are included.

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.

Records are retained in accordance with EPA's Records Schedule 1016(d) and disposed of under National Archives and Records Administration (NARA) disposal authority DAA-0412-2013-0015-0003. This schedule was developed under EPA Records Management Guidelines established pursuant to 44 U.S.C. 3101 et seq. Suspension and debarment files related to the suspension and debarment of entities and individuals subject to debarment regulations, including IG reports, attorney recommendations for actions, notifications to respondents, respondents' submissions, hearing transcripts, briefs and motions, final determinations, and settlement agreements are disposable. Case files are closed when the case is closed, or activity or report is completed, and destroyed 5 years after file closure. The information is maintained for the minimum amount of time necessary in order to support the Suspension and Debarment Program discretionary and statutory suspension and debarment case actions.

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:

Information may be retained longer than needed.

Mitigation:

All cases are tracked during the entire case lifecycle, which includes setting destruction dates at the time a case is closed. Additionally, Suspension and Debarment Program personnel regularly run reports to identify any cases that need to be closed or do not have a destruction date.

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.

As part of the normal agency operations, information (respondent name and mailing address) is uploaded to the General Services Administration (GSA) website at www.SAM.gov (SAM) for use in the "List of Parties Excluded From Federal Procurement or Nonprocurement Programs." The SAM is covered by SORN GSA/GOVT-9. SAM is used by Federal agency award officials and entities that conduct business with the government to determine whether an individual is excluded from participation in federal procurement and nonprocurement programs. Suspension and Debarment Program personnel also confirm the identity of individuals on the list by providing a yes or no answer based on information submitted by the individual seeking confirmation. As part of the normal agency operations, name and civil or criminal history information is shared with organizations and individuals suspended, proposed for debarment or debarred in EPA proceedings; to the legal representatives of such organizations; and to the legal representatives of individuals suspended, proposed for debarment or debarred in EPA proceedings. Information is shared via certified mail, return receipt requested, to provide for the due process required under the regulations governing the EPA Suspension and Debarment Program. Other routine uses are set forth in SORN EPA-33. No agreements apply.

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

All external sharing is compatible with the routine uses specified in SORN EPA-33.

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?

Information sharing agreements, MOUs, new uses of the information, or new access to the system by organizations within the EPA and outside would be subject to review and approval by the Senior Debarring Official (SDO) in consultation with the Director of the Suspension and Debarment Division.

4.4 Does the agreement place limitations on re-dissemination?

No agreements apply.

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:

There is a low risk of unauthorized sharing or disclosure of information.

Mitigation:

Information is shared outside of the Suspension and Debarment Program only to the extent that it is compatible with the stated purpose and use of the original collection. To avoid unauthorized information sharing, access controls have been implemented. SPII, CBI, and DOB information is contained in a Secured section in CADS where the system allows the information to be viewed but does not permit the information to be emailed from the system.

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?

CADS maintains an audit trail (case history) documenting the actions that users take in the system. CADS is limited to staff in the EPA Suspension and Debarment Program with a need to know the information and use of the information in CADS is limited to the Routine Uses set forth in SORN EPA-33. EPA Suspension and Debarment Program staff are subject to the Suspension and Debarment Program Procedures for Handling Personally Identifiable Information (PII), the EPA Privacy Policy, the EPA Rules of Conduct for PII, and the Rules of Behavior for Remote Access to PII. The EPA Suspension and Debarment Program staff are required to certify a user agreement annually and must take Privacy Awareness training annually to maintain access to CADS. The EPA Suspension and Debarment Program staff are required to report all suspected or known breaches of all (sensitive and other) PII to the OCGO primary Information Security Officer and to the EPA Call Center.

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

The Information Security and Privacy Awareness Training is mandatory each year. The course includes information about policies and practices that all EPA computer users should follow. The course also discusses the threats and vulnerabilities associated with IT resources and how

to build good security habits when accessing information. Completion of the training is documented in a course completion certificate that is submitted to OCGO's primary Information Security Officer. EPA Suspension and Debarment Program staff are also required to take Privacy Awareness training annually to maintain access to CADS. Completion of the training is documented in a course completion certificate that is submitted to OCGO's primary Information Security Officer.

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?

Privacy Risk:

There is a low risk of unauthorized access to the system because the system has technical and policy-based safeguards and security measures that can be audited and users are held accountable for compliance with policy regarding access to the system and use of information in the system.

Mitigation:

CADS includes access controls and an audit trail for case history. Users of the system must agree to follow rules of behavior to maintain access to the system.

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 EPA Suspension and Debarment Program use the mailing address and email address information in CADS to send notices of suspension or debarment actions to individual respondents at their last known address. This information must be used to provide for the due process required under the applicable regulations governing the Suspension and Debarment Program. The EPA Suspension and Debarment Program use civil or criminal history information in CADS to support the causes for a suspension and debarment action as allowed under the applicable regulations. SSN and DOB information are necessary to verify the identity of individuals that are listed on SAM and are excluded from Federal procurement and nonprocurement programs.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: No: 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.

All cases in CADS are assigned a system-generated case number and identified by the case number and the respondent's name. Information may be retrieved by using the respondent's name and/or the case number.

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 Suspension and Debarment Program (SDP) adheres to the Privacy Act System of Records: Debarment and Suspension Files, System EPA-33. As discussed above, data is collected to comply with due process requirements and identification of excluded parties on SAM. SDP personnel are trained on handling private information, all such data is stored in secure folders within CADS, user access to CADS is controlled, and all user activities in CADS are tracked.

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:

There is a risk that information collected and contained in CADS could be misused for purposes unrelated to suspension or debarment.

Mitigation:

To mitigate any privacy risks with regards to the use of information in CADS, this PIA and SORN EPA-33 are clear about the uses of information in CADS. The information contained in CADS is limited to information that is relevant to the mission of the EPA Suspension and Debarment Program. Access to information in CADS is limited to staff in the EPA Suspension and Debarment Program with a need to know the information and use of the information in CADS is limited to the Routine Uses set forth in SORN EPA-33. EPA Suspension and Debarment Program staff are subject to the Suspension and Debarment Program Procedures for Handling Personally Identifiable Information (PII), the EPA Privacy Policy, the EPA Rules of Conduct for PII, and the Rules of Behavior for Remote Access to PII. The EPA Suspension and Debarment Program staff are required to certify a user agreement annually and must take Privacy Awareness training annually to maintain access to CADS.

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?

Providing information to the EPA Suspension and Debarment Program is voluntary. Individuals may decline to provide information to the EPA Suspension and Debarment Program. There are no other opportunities for individuals to consent to use or to 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:

The privacy risk related to notice is associated with potentially insufficient notice of privacy data collection prior to the agency providing actual or constructive notice of a suspension or debarment action.

Mitigation:

Notice is provided to the individual in this PIA and SORN EPA-33 regarding the collection and use of privacy information. The information is used only for the purpose for which the notice was provided. The Suspension and Debarment Program provides notice to the individual regarding how the program provides for redress including access and correction; the types of information; and controls over security, retention, and disposal.

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?

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?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations 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:

There is a risk that information collected is inaccurate.

Mitigation:

An individual is provided with an ability to find out whether the system maintains a record relating to him/her. Individuals are provided with opportunities to access and correct a record.

I attest as the Agency Privacy Officer that **Case Application for Debarment and Suspension (CADS)** 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,

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