

PRIVACY IMPACT ASSESSMENT

(Rev. 12/2019)

(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Case Application for Debarment and Suspension (CADS)		
Preparer: Carlyn Perry	Office: OMS-ARM-OGD	
Date: 02/18/2020	Phone: 202-564-5309	
Reason for Submittal: New PIA <input type="checkbox"/> Revised PIA <input type="checkbox"/> Annual Review <input checked="" type="checkbox"/> Rescindment <input type="checkbox"/>		
This system is in the following life cycle stage(s):		
Definition <input type="checkbox"/>	Development/Acquisition <input type="checkbox"/>	Implementation <input type="checkbox"/>
Operation & Maintenance <input checked="" type="checkbox"/> Rescindment/Decommissioned <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 <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f)</u>.</p> <p>The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u>OMB Circular No. A-123, Section VII (A) (pgs. 44-45)</u>.</p>		

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

Case Application for Debarment and Suspension (CADS) is an electronic records management system that supports the EPA in assembling information in order to conduct and document discretionary debarment and suspension proceedings under Federal Acquisition Regulation (FAR) or the Non procurement Common Rule (2 CFR part 180), as well as to carry out the EPA’s obligations to process statutory exclusions under Clean Air Act section 306 and Clean Water Act section 508. Discretionary and statutory suspension and debarment actions prevent companies and individuals from participating in government contracts, subcontracts, loans, grants and other assistance programs.

Section 1.0 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?**

Yes, August 31, 2020

- 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?**

No

Section 2.0 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 (West Law, Public Access for

Court Records (PACER)) and publicly available data (SAM.gov, BoP.gov, and other internet sources). The information is used to identify last known address for purposes of providing notice to an individual respondent regarding 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 from commercial and public sources and referring EPA offices is assumed to be accurate. As needed, EPA Suspension and Debarment Division (SDD) personnel verify the accuracy of data by coordinating with referring offices (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 EPA/OGD/SDD staff unintentionally distributing data in the CADS system.

Mitigation:

There are appropriate controls in place. ROB is also signed by EPA staff to prevent unauthorised information distribution. Mandatory annual Information Security and Privacy Awareness Training is completed by all Agency staff and contractors.

Section 3.0 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?

Yes, each user in CADS is designated a user function within the system based on their required access and assigned roles.

CADS is managed by the system administrator in the Office of Grants and Debarment who assigns roles and responsibilities within the system to users in the Suspension and Debarment Program. User roles and responsibilities for the Suspension and Debarment Official's Office staff is determined by the Senior Debarring Official (SDO) and roles and responsibilities for

Suspension and Debarment Division staff is determined by 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 in the Office of Grants and Debarment who assigns roles and responsibilities within the system to users in the Suspension and Debarment Program. User roles and responsibilities for the Suspension and Debarment Official's Office staff is determined by the Senior Debarring Official (SDO) and roles and responsibilities for Suspension and Debarment Division staff is determined by 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 in the Office of Grants and Debarment. 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?

The only contractors that have access to CADS are National Computer Center Hosting and the Science Applications International Corporation (SAIC). Since these are agency level contracts, they include the required clauses above.

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:

The records retention schedule applicable to CADS is properly followed.

Section 4.0 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 government, 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 disclosed to the General Services Administration (GSA) to compile and maintain the "List of Parties Excluded From Federal Procurement or Nonprocurement Programs" on the System for Award Management (SAM) available at www.sam.gov. The SAM is covered by SORN GSA/GOVT-9. SAM is used by Federal agency officials and entities that conduct business with the government to determine whether an individual is excluded from participation in federal procurement and nonprocurement programs. Information is also disclosed to entities requesting verification of an individual who is listed on the excluded parties list, but only the minimum amount of information needed to verify an identity is disclosed.

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 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 5.0 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 in accordance with stated practices in this PIA (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 OGD's 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 OGD'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 OGD's primary Information Security Officer.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a low risk of unauthorized access to the system. If a system does not have technical and policy based safeguards and security measures that can be audited and if users cannot be held accountable for compliance with policy regarding access to a system and use of information in a system, then the system may present a privacy risk.

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 6.0 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.

The EPA Suspension and Debarment Program uses the mailing address and e-mail 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 uses 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 X 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 name. Information may be retrieved by using the respondent name and/or the case number

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Privacy Act System of Records: Debarment and Suspension Files, System EPA-33

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 NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 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.

The EPA Suspension and Debarment Program posts a Privacy Act Statement discussing the collection and use of information governed by the Privacy Act on the EPA website. The Privacy Act Statement is also provided in notices sent to individual respondents.

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 uses 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 8.0 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?

Any individual who wants to know whether this system of records contains a record about him or her, who wants access to his or her record, or who wants to contest the contents of a record, may make a written request to the System Manager. Instructions are provided in SORN EPA-33.

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

Requests for corrections or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are set out in 40 CFR Part 16 and referenced in SORN EPA-33.

8.3 How does the system notify individuals about the procedures for correcting their information?

Complete EPA Privacy Act procedures are set out in 40 CFR Part 16 and referenced in SORN EPA-33.

8.4 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 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.