United States
Environmental Protection
Agency

PRIVACY IMPACT ASSESSMENT
(Rev. 2/2020)
(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%20Roster.docx

System Name: Information Collection Request, Review and Approval System (ICRAS)	
Preparer: Danny McGrath	**Office:** Office of Mission Support, OEIP, RSD
Date: 4/24/2020	**Phone:** 202-564-8434

Reason for Submittal: New PIA __x__   Revised PIA_____   Annual Review_____ Rescindment _____

This system is in the following life cycle stage(s):

Definition ☐   Development/Acquisition ☐   Implementation ☐

Operation & Maintenance ☒   Rescindment/Decommissioned ☐

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:

The Information Collection Request Review and Approval System (ICRAS) is used by EPA to prepare Information Collection Requests (ICRs) for submission to the Office of Management and Budget (OMB) as required by the Paperwork Reduction Act (PRA). An ICR includes structured data as defined by OMB as well as attached documentation.

The ICRAS system supports EPA by serving as a repository of previous ICRs and a workflow management, tracking, and notification tool for the development of new requests. Specifically, ICRAS is an Agency-wide workflow system that automatically notifies program offices when an ICR needs to be renewed, enables program offices to develop and ICR record, allows for multi-level internal approvals, and routes ICR packages to EPA's Regulatory Support Division for review.

All of the information in an ICR submission becomes part of the public record once it has been transferred to OMB. OMB stores submissions in their own system (ROCIS) and makes it accessible to the public through Reginfo.gov.

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?

From NIST SP 800-60 Volume II

Referencing section: C.2.2 Regulatory Development

Subsection: C.2.2.1 – Policy and Guidance Development Information Type

The information maintained within ICRAS is only that is information that is required by PRA (44 USC 3501) and the associated regulations (5 CFR 1320) to be included in an ICR package that is submitted to OMB for approval.

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, a security plan has been completed and an ATO has been issued. The original ATO expired April 9, 2020; however, an extension was obtained and the new expiration date is July 9, 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?

The data will not be maintained or stored in a Cloud.

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).

The information the system collects, uses, disseminates, or maintains is that information that is required to be part of an ICR under the Paperwork Reduction Act.

OMB Control Number

EPA Tracking Number

ICR Title

ICR Abstract

Citation of Associated Statutes and Regulations

Citation and Publication Date of Associated Federal Register Notices

EPA Point of Contact (Staff Name, EPA Email, EPA Phone Number)

Type of affected public, businesses or agencies

Burden of the collection (Number of Respondents, Number of Responses, Time to Respond and Collate, Cost to Respond and Collate)

Associated Documents (Supporting Statements, Instructions, Collection Forms, Public Comments, Associated Documents as Needed) and associated metadata identifying those documents.

OMB Notice of Action (Date OMB review was completed, Result of the Review, Expiration Date for approved collections, Burden Levels for approved collections, Reason for the approval or disapproval, Associated data)

EPA Users:

EPA User Name

EPA LAN ID

EPA Email

EPA Phone Number

EPA Offices:

EPA Office Name

OMB Control Number Prefix

Groups:

A combination of offices and level of access. EPA Users are assigned to groups to grant the level of access to ICRAS. The groups provide access to the collections the user is allowed to access and provide CRUD level access depending on the group's responsibilities.

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

Data developed by EPA staff that are developing an ICR for submission to OMB. The citation and data for Federal Register notices are collected from the Federal Register (www.federalregister.gov). The Notice of Action is collected from OMB upon the completion of the review (www.reginfo.gov).

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

ICRAS uses information from two publicly available data sources.

Federal Register – When a Federal Register notice about ICRs are published, the volume, page number and date the noticed was published are collected from www.federalregister.gov and recorded in ICRAS.

RegInfo – When a Notice of Action is issued by OMB, the Notice of Action is recorded in ICRAS.

2.4 Discuss how accuracy of the data is ensured.

The data for each ICR goes through multiple levels of review before being approved and submitted to OMB, including a review that is independent of the program responsible for the ICR as required under the PRA. Each reviewer of the data is recorded in the workflow process. If there are issues with the data, the ICR can be retracted to the previous reviewer for rework and resubmitted again for review.

In addition, users are assigned to the user groups, ensuring they only have access to the collections that are required to fulfil their work assignments. Users and groups are reviewed every six months to ensure users still need access to the application.

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:

Low risk that some of the data (EPA LAN ID) will be compromise.

Mitigation:

All data elements collected, except one, are made publicly available through publication in the Federal Register and/or through the OMB website RegInfo.gov. The only piece of data not made public is a user's EPA LAN ID. If for any reason a user's EPA LAN ID would be compromised, security would be notified. The collections in the database would be validated to ensure the integrity of the database. If data has been altered, a backup of the last unaltered database and document collection will be used to restore the repository.

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. There are three levels of user access and there are user groups for each of the offices. The super and admin accounts are assigned to the application administrators. All other users are granted access based on user groups. The user groups are broken up by the offices and level of access. This only allows users to access the offices at the designated level (ICR, Program Office, RPIO, Desk Officer) up through the EPA TL. Each level to review the ICR for submission to OMB. These user groups prevent access to material in other offices and access to the ICRs as the ICR is promoted to the next level. The level of access is determined by the Program Managers in the Office of Mission Support's Regulatory Support Division (OMS/RSD).

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

The controls were documented in the MAST form. That information has been transferred to the ICRAS Controls Implementation spreadsheet.

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

No, ICRAS does not contain additional components with 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?

Yes.

EPAAR 1552.235-80 Access to Confidential Business Information (OCT 2000) The contractor

shall not have access to CBI submitted to EPA under any authority until the contractor obtains from the Project Officer a certification that the EPA has followed all necessary procedures under 40 CFR part 2, subpart B (and any other applicable procedures), including providing, where necessary, prior notice to the submitters of disclosure to the contractor

EPAAR 1552.211-79 Compliance with EPA Policies for Information Resources Management (SEP 2013)

ICRAS Users, all of whom have an EPA LAN ID, will have access to the data in the system. If changes need to be made to user roles, approved system users and approving authorities are notified directly, outside of the system, then the changes are either made by System Administrators or Super Users, or eGlobal Tech.

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.

The system falls under EPA Records Schedule 1023. Information has a retention period of 5 years.

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.

The system falls under EPA Records Schedule 1023. Information has a retention period of 5 years.

Privacy Risk:

Low risk of over retention.

Mitigation:

Record control schedule 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.

Currently there is no information sharing occurring with ICRAS. The information collected in ICRAS is submitted to OMB, but the system does not carry out the transfer of data.

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?

n/a

Privacy Risk:

None, no information is shared.

Mitigation:

N o n e

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 as stated in Section 6.1?

Accountability, Audit, And Risk Management (This family enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk.)

Privacy Requirements for Contractors and Service Providers

Control: The organization:

a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and

b. Includes privacy requirements in contracts and other acquisition-related documents.

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

Information Security and Privacy Awareness and Training

Control: The organization:

a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;

b. Administers basic privacy training [Assignment: organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [Assignment: organization-defined frequency, at least annually]; and

c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [Assignment: organization-defined frequency, at least annually].

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk of improper audit.

Mitigation:

a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events along with the frequency of (or situation requiring) auditing for each identified event].

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.

Account Management

Control: The organization:

a. Identifies and selects the following types of information system accounts to support organizational mission's/business functions: (i.e., individual, group, system, and application)

b. Assigns account managers for information system accounts;

c. Establishes conditions for group and role membership;

d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

g. Monitors the use of information system accounts;

h. Notifies account managers:

1. When accounts are no longer required; 2. When users are terminated or transferred; and

3. When individual information system usage or need-to-know changes;

i. Authorizes access to the information system based on:

1. A valid access authorization;

2. Intended system usage; and

3. Other attributes as required by the organization or associated mission's/business functions;

j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and

k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

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.)*

Information is retrieved by EPA Tracking Number or OMB Control Number. Information cannot be retrieved by any personal identifier.

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

a. ICRAS users that obtain access to ICRAS use the Agency-standard log-on banner as documented in the Standard Configuration Documents.

b. ICRAS contractors see the EPA banner regarding privacy and security notices upon logging into the EPA network. Banner is displayed always upon entry. User muck click okay to remove banner.

c. ICRAS is not a publicly accessible system. Users must access the system through an EPA machine and must have unique credentials to log into the ICRAS system.

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:

Low risk of information misuse.

Mitigation:

System Use Notification

Control: The information system:

a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

1. Users are accessing a U.S. Government information system;

2. Information system usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and

4. Use of the information system indicates consent to monitoring and recording;

b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

c. For publicly accessible systems:

1. Displays system use information [Assignment: organization-defined conditions], before granting further access;

2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Includes a description of the authorized uses of the system.

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.

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 <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>:

<u>Mitigation</u>:

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?

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

8.3 <u>Privacy Impact Analysis</u>: Related to Redress

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

<u>Privacy Risk</u>:

<u>Mitigation</u>: