## Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

## Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

## General Information

PIA Identifier: 362
System Name: Regulatory Information Service Center (ROCIS II)
CPO Approval Date: 5/9/2022
PIA Expiration Date: 5/8/2025

## Information System Security Manager (ISSM) Approval

Gerald Weeks

## System Owner/Program Manager Approval

Elizabeth Harris-Marshall

## Chief Privacy Officer (CPO) Approval

Richard Speidel

## PIA Overview

**A:** System, Application, or Project Name:
Regulatory Information Service Center (ROCIS II)

**B:** System, application, or project includes information about:
The public, agency contacts, and system users.

**C:** For the categories listed above, how many records are there for each?
37,000 records about unique federal employees/contractors as of 2020 and 38,500 unique records about members of the public (21,000 EO 12866 meeting attendees, 3,500 EO 12866 meeting requestors and 14,000 information collection comment authors).

**D:** System, application, or project includes these data elements:

- Names of commenters, meeting attendees and meeting requestors
- Contact Information (e.g., telephone number, email address)
- Comments and supporting materials

## Overview:

ROCIS is used by OIRA and RISC to perform their duties related to preparation/publication of the Unified Agenda of Regulatory and Deregulatory Actions and The Regulatory Plan, EO 12866 regulatory reviews, information collection reviews, Privacy Act notice reviews and EO 13771 regulatory/deregulatory reporting. The system accepts electronic submissions from Federal agencies, allows RISC and OIRA staff to review materials electronically, and maintains all the associated records. ROCIS provides query and reporting services to RISC and OIRA, as well as to other Federal agencies, state governments, Congress, and the public.

ROCIS manages the flow of information submitted for review under the Paperwork Reduction Act, Executive Order 12866, the Privacy Act and Executive Order 13771 and will permit OIRA to meet its responsibilities attributed therein. It encompasses the processes used by RISC and OIRA when receiving agency submissions and provides an electronic interface between RISC, OIRA, and other Federal agencies. ROCIS does not include the proprietary processes used by agencies to prepare their data for submission to RISC and OIRA.

ROCIS handles the following materials: regulations identified by Regulation Identifier Number (RIN), regulatory reviews of significant regulations, reporting of regulatory/deregulatory actions, information collections identified by Information Collection Request (ICR) reference numbers or OMB control numbers, and reviews of Systems of Records Notices (SORN) and Computer Matching Agreements (MA). ROCIS provides links to citations in the Federal Register, Code of Federal Regulations, United States Code, and Public Laws. ROCIS also provides linkages between related regulations and information collections, as well as associations between related SORNs and matching agreements. These associations allow OIRA's reviews to be more closely coordinated and allows for historical reviews of the interconnected records. Rules may be associated with OMB control numbers, and ICRs submitted during development of a regulation may have an associated RIN. SORNs may be associated with other SORNs and matching agreements can be associated with SORNS and other matching agreements in ROCIS. ROCIS also includes the data necessary for the management of user accounts and role-based access.

The functional components of ROCIS are the following: agency projections of regulatory activity (Unified Agenda module), review or significant rulemakings (EO 12866 module), information collection review (PRA module), SORN and matching agreement review (Privacy module), agency reporting of regulatory/deregulatory actions (EO 13771 module) and user/system administration.

ROCIS must serve the needs of RISC and OIRA, as well as 70+ reporting agencies.

The Unified Agenda of Regulatory and Deregulatory Action and The Regulatory Plan are published on the ROCIS public website (PWS), Reginfo.gov. Information about OIRA's review of significant rules under EO 12866 and reviews of information collections under the Paperwork Reduction Act is also displayed on Reginfo.gov. Public users can submit EO 12866 meeting requests to OIRA on Reginfo.gov. Public users can submit public comments for information collections under review at OIRA on Reginfo.gov. Additionally, a mobile application called RegInfo Mobile provides functionality similar to Reginfo.gov for compatible mobile devices.

### 1.0 Purpose of Collection

**1.1:** What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
44 U.S.C. §§ 3504 is the law that grants authority. OMB's authority to operate ROCIS is found in Executive Orders 12866, 13563 and 13771; the Paperwork Reduction Act (44 U.S.C. §§ 3501-3521) and the Privacy Act (5 U.S.C. § 552a). ROCIS maintains information about users including first and last name, agency email address, phone, and agency and sub-agency name. Additionally, ROCIS generates and maintains the following information regarding the ROCIS user account: user login id, account status (locked/unlocked, active/inactive), employee number (which is

generated by ROCIS and only used within ROCIS), and role (which denotes what information the user has access to within ROCIS and their level of editing privileges).

**1.2:** Is the information searchable by a personal identifier, for example a name or Social Security number?
No

**1.2a:** If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
**1.2: System of Records Notice(s) (Legacy Text):** What System of Records Notice(s) apply/applies to the information?
"ROCIS sends the names of meeting participants and email address of the meeting requester to OIRA. The public, via reginfo.gov, can only access the names of the individuals who participate in third-party meetings with OIRA to discuss pending rules. OIRA users receive comments grouped by ICR/OMB control number. Any information that commenters choose to provide (e.g. name, email address, comment, etc.) is provided to OIRA users. However, only the commenter's name and comment are published on reginfo.gov after the ICR concludes. ROCIS system users and Reginfo.gov public users do not have the ability to search for meeting requestors or ICR commenters via a personal identifier, however, SORN GSA-OGP-1 applies to this PIA. "

**1.2b:** Explain why a SORN is not required.

**1.3:** Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

**1.3: Information Collection Request:** Provide the relevant names, OMB control numbers, and expiration dates.
ROCIS' collection of public comments does not require an ICR because public comments are exempt: https://pra.digital.gov/do-i-need-clearance/ ROCIS has an ICR for its meeting request portion: OMB Control No: 0348-0065, Title: "Information on Meetings with Outside Parties Pursuant to Executive Order 12866" and Expiration Date: 06/30/2022.

**1.4:** What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
Outline of Records Schedule Items for DAA-GRS-2017-0012 1. Records of proposed rule development. Disposition Authority: DAA-GRS-2017-0012-0001 (GRS 6.6, item 010) Retention: Destroy 6 fiscal years after publication of final rule or decision to abandon publication, but longer retention is authorized if needed for business use. 2. Proposed and final rule documents published in the Federal Register. Disposition Authority: DAA-GRS-2017-0012-0002 (GRS 6.6, item 020) Retention: Destroy 1 fiscal year after publication, but longer retention is authorized if required for business use. 3. Public comments. Disposition Authority: DAA-GRS-2017-0012-0003 (GRS 6.6, item 030) Retention: Destroy 1 year after publication of final rule or decision to abandon publication, but longer retention is authorized if needed for business use. 4. Federal Register notices other than proposed and final rules. Disposition Authority: DAA-GRS-2017-0012-0004 (GRS 6.6, item 040) Retention: Destroy when 1 fiscal year old, but longer retention is authorized if required for business use. 5. Agency input into the unified agenda. Disposition Authority Number: DAA-GRS-2017-0012-0005 (GRS 6.6, item 050) Retention: Destroy when 2 fiscal years old, but longer retention is authorized if needed for business use. "With one exception (see item 030), this schedule does not cover records created after a proposed rule first appears in the Federal Register (item 020 lists Â·points at which first publication might appear). Records created after first appearance in the Federal Register are contained in a case file, often called a "docket." Dockets may be of permanent value depending on the 'particular rule or an agency's mission. Therefore, each agency must schedule its rulemaking I dockets independently."

## 2.0 Openness and Transparency

**2.1:** Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

**2.1 Explain:** If not, please explain.

## 3.0 Data Minimization

**3.1:** Why is the collection and use of the PII necessary to the project or system?
ROCIS users provide their names (required), email addresses (required) and phone numbers (required), so that their identities can be verified and other users can contact them about system records, as needed. Meeting requestors provide their names (required), email addresses (required) and/or phone numbers (optional) and the names of

meeting attendees, so that OIRA can coordinate with all parties during the meeting scheduling process. ICR commenters provide their names (optional), email addresses (optional) and/or phone numbers (options), in case a response is warranted.

**3.2:** Will the system, application, or project create or aggregate new data about the individual?
No

**3.2 Explained:** If so, how will this data be maintained and used?

**3.3** What protections exist to protect the consolidated data and prevent unauthorized access?
ROCIS utilizes user information, combined with role/function/agency-access control, to enforce access to the system. Only a ROCIS System Administrator can modify information about agencies, employees, mailing lists, access privileges, and user-level access assignments in ROCIS. ROCIS System Administrators have privileges to activate, deactivate, and modify role/function/agency/agency assignments. ROCIS employs least privilege and separation of duties to ensure information is handled to sustain its mission. Security related privileges that relate to the host configurations; auditing, intrusion detection, and cryptographic implementations are the responsibility of the Enterprise Server Services (ESS). ROCIS and Reginfo.gov are web-applications only available from the internet. All of their components reside at GSA facilities and are only accessible via the GSA firewall. Unsecure internet traffic (HTTP) on port 80 is automatically redirected to secure HTTP (HTTPS) on port 443 using TLS connections to ensure that all communications to and from the internet are encrypted. All communications between system components are secured. The Oracle Advanced Security feature called Transparent Data Encryption (TDE) is employed to encrypt all of the databases.

**3.4** Will the system monitor the public, GSA employees, or contractors?
None

**3.4 Explain:** Please elaborate as needed.

**3.5** What kinds of report(s) can be produced on individuals?
Reports are not routinely produced on individuals. ROCIS is designed to produce reports that aggregate EO 12866 meeting information by non-PII data elements, such as regulatory identification number (RIN) or agency. ROCIS is not designed to produce reports that aggregate public comments received on information collections under review.

**3.6** Will the data included in any report(s) be de-identified?
No

**3.6 Explain:** If so, what process(es) will be used to aggregate or de-identify the data?

**3.6 Why Not:** Why will the data not be de-identified?
Not applicable.

## 4.0 Limits on Using and Sharing Information

**4.1:** Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?
No

**4.2:** Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
Federal Agencies

**4.2How:** If so, how will GSA share the information?
GSA publishes the Unified Agenda bi-annually and provides publicly available ROCIS data on Reginfo.gov. Published data includes federal employees contact information (first and last name, agency, telephone numbers and email

address) for regulatory activities and information collection requests that are entered by the agencies. For scheduled EO meetings, the name of the meeting requestor is displayed on Reginfo.gov. For completed EO meetings, the name of the meeting requestor and attendees are displayed on Reginfo.gov. For comments made pursuant to an information collection, the name entered by the public commenter will be displayed on the Reginfo.gov. The data entered into ROCIS by the agencies belongs to the agencies and it is their responsibility to ensure the accuracy of the data they submit. Agency users who enter publicly accessible data into ROCIS are trained to ensure that publicly accessible information does not contain non-public information.

**4.3:** Is the information collected:
Directly from the Individual

**4.3Other Source:** What is the other source(s)?
The data entered into ROCIS by the agencies belongs to the agencies and it is their responsibility to ensure the accuracy of the data they submit. Agency users who enter publicly accessible data into ROCIS are trained to ensure that publicly accessible information does not contain non-public information. All other personal information (ROCIS users, EO meetings and ICR comments) is collected directly from the individual.

**4.4:** Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
Yes

**4.4WhoHow:** If so, who and how?
ROCIS uses MAX.gov for user identity verification. ROCIS users click the Login button on the ROCIS login page and are redirected to MAX.gov to verify their identity. If they login to MAX.gov successfully, then they are redirected to ROCIS. ROCIS will use the identifying information in the response from MAX.gov to authenticate the user and provide access based on their user profile in ROCIS. A formal IAA agreement is in place to pay for the MFA services offered by Max. Publicly available ROCIS data is made available in XML format on Reginfo.gov. The public can use this data as needed. No formal agreement is in place with any Reginfo.gov XML consumers.

**4.4Formal Agreement:** Is a formal agreement(s) in place?
No

**4.4NoAgreement:** Why is there not a formal agreement in place?
Publicly available ROCIS data is made available in XML format on Reginfo.gov. The public can use this data as needed. No formal agreement is in place with any Reginfo.gov XML consumers.

## 5.0 Data Quality and Integrity

**5.1:** How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
The data stored within ROCIS belongs to the agencies and it is their responsibility to ensure the accuracy of the data they submit. Agency users who enter publicly accessible data into ROCIS are trained to ensure that publicly accessible information does not contain nonpublic information. Personal information used to create/update ROCIS user accounts is provided by the agencies and it is their responsibility to ensure the accuracy of the data they submit. Email addresses provided by EO meeting requestors are verified for accuracy. Before an EO meeting request can be submitted online, the requestor must enter a valid email and confirm the email address by entering it a second time. If the email addresses do not match, the requestor cannot proceed. The requestor also has to respond successfully to an on-screen reCAPTCHA to verify that a person, not an automated script or robot, is providing the information. Finally, Reginfo.gov sends an email to the email address provided and the requestor has to click the link in the verification email before submitting the EO meeting request online. Other personal information provided by the EO meeting requestor is not verified. Personal information provided by the public for ICR comments is not verified.

## 6.0 Security

**6.1a:** Who or what will have access to the data in the system, application, or project?
The ROCIS database stores user contact information and user roles. The ROCIS database also stores the information that underlines the ROCIS business processes, including workflow, versioning, and user access. User

accounts include: Name, Agency, Title, Work Telephone, Work TDD, Work Fax, Work Email and Work Address, username (system generated) and user number (system generated). All ROCIS users are either Federal Government employees or contractors acting on their behalf.

**6.1b:** What is the authorization process to gain access?
The user account information is entered via the ROCIS application user interface. The ROCIS System Administrator enters it when creating an account from information provided by the agencies. The users themselves are also able to update some of their own personal information. Only a ROCIS System Administrator can modify information about agencies, other employees, mailing lists, access privileges, and user-level access assignments in ROCIS. ROCIS System Administrators have privileges to activate, deactivate, and modify role/function/agency/agency assignments. Users must request access to the system and are required to sign the security agreement/rules of behavior document before obtaining an account. Users only have access to modify data entered by their respective agencies. Reports provide users with view access to publicly available data for all agencies. System admins have access to all data. The roles and responsibilities are documented. See the ROCIS "USER INFORMATION" and "HOW TO" guides for additional information. ROCIS employs least privilege and separation of duties to ensure information is handled to sustain its mission. Security related privileges that relate to the host configurations; auditing, intrusion detection, and cryptographic implementations are the responsibility of the Enterprise Server Services (ESS). In addition to the annual GSA Security and Privacy Awareness training that GSA staff must complete, each ROCIS user is required to recertify their account annually and agree to the latest security agreement/rules of behavior.

**6.2:** Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

**6.2a:** Enter the actual or expected ATO date from the associated authorization package.
6/2/2020

**6.3:** How will the system or application be secured from a physical, technical, and managerial perspective?
ROCIS and Reginfo.gov are web-applications only available from the internet. All of their components reside at GSA facilities and are only accessible via the GSA firewall. Unsecure internet traffic (HTTP) on port 80 is automatically redirected to secure HTTP (HTTPS) on port 443 using TLS connections to ensure that all communications to and from the internet are encrypted. All communications between system components are secured. The Oracle Advanced Security feature called Transparent Data Encryption (TDE) is employed to encrypt all of the databases. ESS provides the backend support for GSA applications, secures the data center, and audits relevant security events. The list of auditable events is reviewed and updated annually or as needed in response to changes in the business/technical environment that impact the security risk of the ROCIS application. Each ROCIS user is required to recertify their account annually and agree to the latest security agreement/rules of behavior.

**6.4:** Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?
Yes

**6.4What:** What are they?
ROCIS audit records include information such as the operation that was audited, the user performing the operation, and the date and time of the operation. Audit records can be stored in a data dictionary table called the database audit trail. The audit trail records can contain different types of information, depending on the events audited and the auditing options set. The following information is always included in each audit trail record, provided that the information is meaningful to the particular audit action:

- User name
- Session identifier
- Terminal identifier
- Name of the schema object accessed
- Operation performed or attempted
- Completion code of the operation
- Date and time stamp

- System privileges used ESS provides the backend support for GSA applications.

The list of auditable events is reviewed and updated annually or as needed in response to changes in the business/technical environment that impact the security risk of the ROCIS application.

## 7.0 Individual Participation

**7.1:** What opportunities do individuals have to consent or decline to provide information?
Users must request access to the system and are required to sign the security agreement/rules of behavior document before obtaining an account. Users only have access to modify data entered by their respective agencies. Reports provide users with view access to publicly available data for all agencies. ROCIS System Administrators have access to all data. The roles and responsibilities are documented. Project and system roles and responsibilities are documented.

**7.1Opt**: Can they opt-in or opt-out?
Yes

**7.1Explain**: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

**7.2:** What are the procedures that allow individuals to access their information?
ROCIS users can access and update their own personal information in ROCIS. ROCIS System Administrators have access to all data. If a ROCIS user submits incorrect or erroneous personal information about an agency contact, that user may contact their RISC analyst, OIRA desk officer, the GSA help desk or a ROCIS System Administrator in order to discuss the change. Some changes can be made by the users, others would require assistance. EO meeting requestors and ICR commenters may contact RISC, OIRA or the GSA help desk to discuss changes to their personal information in ROCIS.

**7.3:** Can individuals amend information about themselves?
Yes

**7.3How**: How do individuals amend information about themselves?
ROCIS users can access and update their own personal information in ROCIS via the ROCIS application user interface. Agency contacts in ROCIS without access to the system, EO meeting requestors and ICR commenters may contact RISC, OIRA or the GSA help desk to discuss changes to their personal information in ROCIS.

## 8.0 Awareness and Training

**8.1:** Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.
The ROCIS security requirements/rules of behavior document advises users of the sensitive and proprietary data associated with the purpose of the mission. Users are also prohibited from unauthorized disclosure of predecisional or other deliberative information. The document also advises users of their authorized uses and responsibilities for maintaining the confidentiality and integrity of sensitive data. Users must re-certify their awareness of the ROCIS security requirements/rules of behavior annually in order to maintain their access. In addition to signing the security requirements and rules of behaviors, users are greeted with the GSA "For Official Use Only" warning banner upon entering the system and are required to agree to the terms before access.

## 9.0 Accountability and Auditing

**9.1:** How does the system owner ensure that the information is used only according to the stated practices in this PIA?
The system owner is responsible for reviewing and updating (as needed) this privacy impact assessment on an annual basis. In addition, the system provides input validation for certain PII fields (phone number and email address). Between the time that the PII is submitted, if at all, and the time it would be displayed, the content is validated/reviewed for public viewing to ensure the content is appropriate.