Privacy Impact Assessment

Regulatory Information Service Center (RISC) RISC/OIRA Combined Information System (ROCIS)

May 30, 2018

Privacy Impact Assessment (PIA) for the

Office of Government-wide Policy (OGP)

Regulatory Information Service Center (RISC)

RISC/OIRA Combined Information System (ROCIS)

May 2018

Contact Point:

Joseph Hoyt
General Services Administration (GSA) Information Technology (IT)
GSA IT – Services ISSO Support Branch (IST)
202.969.7181

Abstract

RISC/OIRA Combined Information System (ROCIS) resides within the Regulatory Information Service Center (RISC), within the Office of Government-wide Policy (OGP). The ROCIS application, which provides mission critical support for the Office of Information and Regulatory Affairs (OIRA), provides a system to manage the workflow process in which agencies submit their regulatory activities to OIRA for review, as well as submitting their information collection requests (ICR), and system of records notices (SORN). ROCIS maintains information about Federal employee users including first and last name, user ID, email address, phone, agency, sub-agency, role, employee #, account status (active/inactive, and locked/not locked).

Overview

ROCIS is the primary means by which OIRA and RISC perform their duties related to regulatory and information collection reviews, and preparation of the Unified Agenda and Regulatory Plan. The system accepts electronic submissions from Federal agencies, allows RISC and OIRA staff to review materials electronically, and maintains all the associated records, both paper and electronic. ROCIS provides query and reporting services to RISC and OIRA, as well as to the Government Accounting Office (GAO), other Federal agencies, state governments, Congress, and the public.

ROCIS manages the flow of information submitted for review under the Paperwork Reduction Act and Executive Order 12866, and will permit OIRA to meet its responsibilities under the Government Paperwork Elimination Act. 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 has two separate series of materials it handles: regulations identified by Regulation Identifier Number (RIN) and information collections identified by Information Collection Request (ICR) reference numbers or OMB control numbers. For both regulations and information collections, ROCIS provides links to citations in the Federal Register, Code of Federal Regulations, United States Code, and public laws. ROCIS also provides linkages between regulations and information collections. This association allows OIRA's review of rules and ICRs to be more closely coordinated and allows for historical reviews of the links between rules and ICRs. Rules may be associated with OMB control numbers, and ICRs submitted during development of a regulation may have an associated RIN.

The functional components or areas of ROCIS are the following: rulemaking action review, information collection review, user administration and the Unified Agenda/Regulatory Plan preparation.

ROCIS was created to support the publication of the Unified Agenda in the Federal Register. ROCIS must serve the needs of RISC and OIRA, as well as 64 reporting agencies and 300-400 sub-agencies.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the application in question?

OMB authority to operate ROCIS is found in Executive Orders 12866 and 13563; the Paperwork Reduction Act (44 U.S.C. §§ 3501-3521) and the Privacy Act (5 U.S.C. § 552a).

ROCIS II 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 What Privacy Act System of Records Notice(s) (SORN(s)) applies to the information?

There is no SORN for this system because the information is not retrieved by a personal identifier; the records are keyed to agency information. ROCIS users can find other ROCIS users via the system's search capability; however, this collection of information is offered as an administrative aid to enable ROCIS users to identify and communicate with one another more effectively. For example, if you would like to send another agency's SORN Privacy Officer (SPO) an email, you are able to search on the SPO role for the agency and receive a list of contacts. If a SORN Administrative Contact wants to identify a list of preparers (SORN Preparer or SPs) for his/her agency, this system allows you to conduct such a search. See the ROCIS "USER INFORMAITON" and "HOW TO" guides for additional information.

1.3 Has a System Security Plan (SSP) been completed for the information system(s) supporting the application?

Yes. GSA granted ROCIS an ATO on 12/12/2017.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No official records are maintained by this system.

1.5 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, this information is not covered by the PRA.

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 application collects, uses, disseminates, or maintains.

ROCIS includes rulemaking information (Agenda), rule reviews (REGS), Paperwork Reduction Act (PRA) information, and System of Records Notice (SORN) reviews.

The ROCIS database also 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), user number (system generated), and password. All ROCIS users are either Federal Government employees or contractors acting on their behalf.

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

The user accounts information is entered via the ROCIS application user interface. The system administrator enters it when creating an account from information provided by each agency. The user themselves is also able to update some of their own information. There are no system interconnections.

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

No, ROCIS does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

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.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: PII Data Leakage

Mitigation: ROCIS utilizes user IDs and password authorization, combined with role/function/agency-access control, to enforce access to the system. The administrative and security module of ROCIS that contains information about agencies, employees, mailing lists, access privileges, user names and passwords, and user-level access assignments is only accessible to the ROCIS Application Manager. The ROCIS Application Manager has privileges to activate, deactivate, and modify role/ function/ agency/ agency assignments.

Privacy Risk: Data Integrity

Mitigation: 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).

Section 3.0 Uses of the Information

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

3.1 Describe how and why the application uses the information.

GSA is responsible for publishing the Unified Agenda bi-annually and providing data on reginfo.gov. Published data includes federal employees contact information (first and last name, agency, telephone numbers and email address) for regulatory activities that is entered by the agencies.

3.2 Does the application use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how GSA plans to use such results.

No, the system does not use technology to look for predictive patterns or anomalies.

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

Yes, Office of Management and Budget (OMB) users have assigned roles and responsibilities, for example to review and approve submissions.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Users may disclose sensitive information without or in excess of authorization

Mitigation: All ROCIS users must complete training and orientation before accessing the system.

Section 4.0 Notice

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

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

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 view or modify rulemaking, rule review and SORN data for their assigned agencies. For PRA, users only have access to modify their data. PRA Reports provide users with view access to publicly available PRA data for all agencies. System admins have access to all data. The roles and responsibilities are documented. See the ROCIS "USER INFORMAITON" and "HOW TO" guides for additional information.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the application?

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 view or modify rulemaking, rule review and SORN data for their assigned agencies. For PRA, users only have access to modify their data. PRA Reports provide users with view access to publicly available PRA data for all agencies. System admins have access to all data. Yes, the roles and responsibilities are documented.

4.3 Privacy Impact Analysis: Related to Notice

The ROCIS security requirements advise users of the sensitive and proprietary data associated with the purpose of the mission. Users are also prohibited from unauthorized disclosure of pre-decisional or other deliberative information. The Rules of behavior advises users of their authorized uses and responsibilities for maintaining the confidentiality and integrity of sensitive data.

In addition to signing the security requirements and rules of behaviors, users are greeted with the GSA warning banner upon entering the system and are required to agree to the terms before access.

Section 5.0 Data Retention by the application

The following questions are intended to outline how long the application retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

All ROCIS data is retained indefinitely. ROCIS has least privilege and separation of duties in place to prevent data protected from unauthorized access. One of the two Apache servers are dedicated to public access and the primary Internet firewall is configured to only allow Secure Hypertext Transfer Protocol (HTTPS) communications. The second Apache server is dedicated to OIRA, RISC, and other agency users and uses the Transport Layer Security (TLS) protocol as a secure transmission mechanism. The firewall is configured to allow TLS connections to the second server.

5.2 Privacy Impact Analysis: Related to Retention

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the application information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 Is information shared outside of GSA as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The RISC/OIRA Consolidated Information System (ROCIS) is the primary means by which agencies provide regulatory data for publication in the Unified Agenda and Regulatory Plan and the Federal Register. ROCIS allows agencies to request that OMB review and approve a variety or documents.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Not applicable. Agencies use ROCIS to submit information to OMB for review and approval. There is no external sharing beyond OMB.

6.3 Does the application place limitations on re-dissemination?

There is no re-dissemination; see 6.2 above.

6.4 Describe how the application maintains a record of any disclosures outside of the Agency.

ROCIS allows each user to track what they have submitted to OMB for review and approval.

6.5 Privacy Impact Analysis: Related to Information Sharing

ROCIS allows each user to track what they have submitted to OMB for review and approval. Therefore, the user is able to control and review what has been submitted.

Section 7.0 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.

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

Roles are enforced throughout the ROCIS system. Users are provided a unique user name that uniquely identifies each individual. Each user account is assigned one or more roles that grant specific access (e.g. view, update, etc.) to each of the ROCIS modules. Each role is associated with one or more agency codes. When a ROCIS page is rendered, only data for the assigned agencies are displayed to the user.

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

Roles are enforced throughout the ROCIS system. Users are provided a unique user name that uniquely identifies each individual. Each user account is assigned one or more roles that grant specific access (e.g. view, update, etc.) to each of the ROCIS modules. Each role is associated with one or more agency codes. When a ROCIS page is rendered, only data for the assigned agencies are displayed to the user.

If a user submits incorrect or erroneous information, that user may contact their RISC analyst, OIRA desk officer, GSA help desk or system administrator in order to discuss a change. Some changes can be made by the users, others would require assistance.

7.3 How does the application notify individuals about the procedures for correcting their information?

Roles are enforced throughout the ROCIS system. Users are provided a unique user name that uniquely identifies each individual. Each user account is assigned one or more roles that grant specific access (e.g. view, update, etc.) to each of the ROCIS modules. Each role is associated with one or more agency codes. When a ROCIS page is rendered, only data for the assigned agencies are displayed to the user.

7.4 Privacy Impact Analysis: Related to Redress

If a user submits incorrect or erroneous information, that user may contact their RISC analyst, OIRA desk officer, GSA help desk or system administrator in order to discuss a change. Some changes can be made by the users, others would require assistance.

Section 8.0 Auditing and Accountability

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

8.1 How does the application ensure that the information is used in accordance with stated practices in this PIA?

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 database audit trail is a single table named AUD$ in the SYS schema of each Oracle database's data dictionary. Several predefined views are provided to help you use the information in this table.

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 and has the following additional controls in place at the data center.

- Severity of the event;
- Number of times this message has appeared;
- Date of the event;
- Time of the event;
- Name of the node affected;
- Application that generated the event;
- Group that generated the message (e.g. security, performance, and so forth);
- Lists the name of the event if there is one (e.g. a security incident would list the name of the attack); and
- Description of event (e.g. success or failure).

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.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the application.

In addition to the annual GSA Security and Privacy Awareness training that GSA staff must complete, each ROCIS is required to recertify their accounts annually and agree to the security agreement/rules of behavior.

8.3 What procedures are in place to determine which users may access the information and how does the application determines who has access?

Users only have access to view or modify rulemaking, rule review and SORN data for their assigned agencies. For PRA, users only have access to modify their data. PRA Reports provide users with view access to publicly available PRA data for all agencies. System admins have access to all data. Yes, the roles and responsibilities are documented.

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

Not applicable as the information is provided by each agency to OMB, in accordance with Executive Orders.