Regulatory Information
Service Center (RISC)

RISC/OIRA Combined Information
System (ROCIS)

Privacy Impact Assessment

November 20, 2019

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to assist GSA employees and contractors in complying with the E-Government Act of 2002, Section 208, which requires GSA to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The template also accords with 1878.2A CIO P - Conducting Privacy Impact Assessments; is designed to align with GSA businesses processes; and can cover all of the systems, applications or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application or project's life cycle. The completed PIA demonstrates how GSA ensures that privacy protections are built into technology from the start, not after the fact when they can be far more costly or could affect the viability of performing GSA's work. Completed PIAs are made available to the public at gsa.gov/privacy (https://www.gsa.gov/portal/content/102237).

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles ("FIPPs"), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. For example:

This document contains important details about *[system, application or project name]*. *[GSA office]* may, in the course of *[program name]*, collect personally identifiable information ("PII") about the people who use such products and services.

An example of a completed PIA is available at:
https://www.gsa.gov/portal/getMediaData?mediaId=167954

Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.

Stakeholders

Name & Email of Information System Security Manager (ISSM):

- Joseph Hoyt
  General Services Administration (GSA) Information Technology (IT)
  GSA IT – Services ISSO Support Branch (IST)
  joseph.hoyt@gsa.gov
  202.969.7181

Name & Email of Program Manager/System Owner:

- Connie Jordan, Deputy Director, Regulatory Information Service Center (RISC)
  Office of Government-wide Policy (OGP)
  Connie.jordan@gsa.gov
  202-208-0508

Signature Page

Signed:

DocuSigned by:
Joseph Hoyt
CA8EF810EDA7425...

Information System Security Manager (ISSM)

DocuSigned by:
Connie Jordan
1BD64E405F4D4AE...

Program Manager/System Owner

DocuSigned by:
Richard Speidel
171D5411183F40A...

Chief Privacy Officer. Under the direction of the Senior Agency Official for Privacy (SAOP), the Chief Privacy Officer is responsible for evaluating the PIAs for completeness of privacy related information.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third party services and robotics process automation (RPA).	2.0
6/26/2018	New question added to Section 1 regarding "Information Collection Requests"	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed CPO email address	2.3
11/28/2018	Added new Stakeholders section to streamline process when seeking signatures & specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
07/17/2019	Added information regarding collection of PII within the EO meeting request and ICR comments features.	2.5

Table of contents

4.2 Will GSA share any of the information with other individuals , Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

4.4 Will the system, application or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

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

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about the Regulatory Information Service Center (RISC) Office of Information and Regulatory Affairs (OIRA) Consolidated Information System (ROCIS). ROCIS may collect personally identifiable information ("PII") from the users entering information into the system. 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, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of 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 that are codified in the Privacy Act of 1974.[2]

System, Application or Project

Regulatory Information Service Center (RISC) Office of Information and Regulatory Affairs (OIRA) Consolidated Information System (ROCIS II)

System, application or project includes information about

- The public, agency contacts, and system users

System, application or project includes

- *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.

The functional components or areas 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 (Document Review module), agency reporting of regulatory/deregulatory actions (EO 13771 module) and user/system administration.

ROCIS serves 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 similar functionality for compatible mobile devices.

SECTION 1.0 PURPOSE OF COLLECTION

1.1 Why is GSA collecting the information?

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.

The Paperwork Reduction Act allows for the public to comment on Information Collections during the first 30 days of OIRA's review. Until now, the public has been provided with an email address at OIRA to which they can submit comments. We will now allow the public to submit comments to OIRA from Reginfo.gov. Commenters may provide name, email address and affiliation as part of their comment submission. Information provided may be used by OIRA to follow-up with commenter if needed. If provided, the commenter's name will be displayed on Reginfo.gov along with the comment when OIRA completes their review.

EO 12866 requires that OIRA meet with outside parties at their request. In order to facilitate this, users are able to request meetings with OIRA. When requesting a meeting with OIRA, names, email addresses and phone numbers are required. OIRA is required to provide information to the public after the meetings have occurred. This information includes the names of meeting participants and how they attended the meeting, i.e. teleconference, etc.

1.2 What legal authority and/or agreements allow GSA to collect the information?

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).

In Regulatory Reform under Executive Order 13771: Final Accounting for Fiscal Year 2018, the Office of Information and Regulatory Affairs compiles the regulatory reform results from fiscal year 2018. President Trump emphasized the importance of reducing regulatory burdens and directed agencies to eliminate two regulations for each new one and to cap their total incremental costs in Executive Order 13771 ("Reducing Regulation and Controlling Regulatory Costs," January 30, 2017). Agencies have focused on comprehensive and common-sense regulatory reform, protecting health and safety while eliminating unnecessary costs. These reforms adhere to the longstanding principles and good regulatory practices in Executive Order 12866 ("Regulatory Planning and Review," September 30, 1993), which highlights that "the private sector and private markets are the best engine for economic growth."

EO 12866 requires that OIRA meet with outside parties at their request. In order to facilitate this, users are able to request meetings with OIRA. When requesting a meeting with OIRA, names, email addresses and phone numbers are required. OIRA is required to provide information to the public after the meetings have occurred. This information includes the names of meeting participants and how they attended the meeting, i.e. teleconference, etc.

1.3 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?

No. ROCIS sends the names of meeting participants and email address of the meeting requestor 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 and reginfo.gov users do not have the ability to search via a personal identifier and therefore no SORN is required for the ROCIS system.

1.4. Has any information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, 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 and ICR Reference No: 201904-0348-001.

1.5. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

GSA handles its records in accordance with NARA-approved records schedules. Records related to proposed rule development are maintained for six years after publication of final rule or decision to abandon publication, but longer retention is authorized if required for business use. Records related to: proposed and final rule documents published in the Federal Register; public comments received in response to a proposed rule; and Federal Register notices other than prepared and final rules (e.g. announcing public stakeholder meetings, hearings, investigations, petition filing, application filing, license issuance, license revocation, grant application deadlines, environmental impact statement availability, delegations of authority, hours of public opening, use of an agency's seal, guidance, System of Records Notices (SORNs), Paperwork Reduction Act Information Collection Requests (PRA ICRs), and other matters not codified in the Code of Federal Regulations) are are all maintained for one year after publication, but longer retention is authorized if required for business use.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

Possibly inappropriate information disclosure. The voluntary PII that is collected is encrypted both at rest and in transit.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

The information is submitted voluntarily by the individual they submit their comments, if they choose to provide it.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

No. ROCIS is designed to operate openly and transparently.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system, application or project?

Privileged users, agency users, and members of the public who choose to provide personal information along with their comments.

3.2 What PII will the system, application or project include?

The ROCIS database stores user contact information and user roles. 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.

The Paperwork Reduction Act allows for the public to comment on Information Collections during the first 30 days of OIRA's review. Until now, the public has been provided with an email address at OIRA to which they can submit comments. We will now allow the public to submit comments to OIRA from Reginfo.gov. Commenters may provide name, email address and affiliation as part of their comment submission. Information provided may be used by OIRA to follow-up with commenter if needed. If provided, the commenter's name will be displayed on Reginfo.gov along with the comment when OIRA completes their review.

EO 12866 requires that OIRA meet with outside parties at their request. In order to facilitate this, users are able to request meetings with OIRA. When requesting a meeting with OIRA, names, email addresses and phone numbers are required. OIRA is required to provide information to the public after the meetings have occurred. This information includes the names of meeting participants and how they attended the meeting, i.e. teleconference, etc.

3.3 Why is the collection and use of the PII necessary to the system, application or project?

User contact information is required in order to generate user accounts within the system. Public contact information is not required to comment, but is optional data that members of the public may choose to enter. Name and contact information is necessary in order for verification for meeting requests.

3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

No.

3.5 What protections exist to protect the consolidated data and prevent unauthorized access?

Not Applicable.

3.6 Will the system monitor the public, GSA employees or contractors?

No.

3.7 What kinds of report(s) can be produced on individuals?

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.

3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

Not applicable.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

No.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

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?

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.

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.

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).

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share 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.

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.

For comments made pursuant to a PRA, the name entered by the public commenter will be displayed on the public website.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

All user information 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? If so, who, how and is a formal agreement(s) in place?

No

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

No

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected 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.

PII provided by the public for the ICR comments is not verified.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

No

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?

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

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.

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.

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 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 is required to recertify their accounts annually and agree to the security agreement/rules of behavior.

6.2 Has GSA completed a system security plan for the information system(s) or application?

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

6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

PII info are encrypted using Advanced Encryption Standard (AES) Galois/Counter Mode (GCM) encryption, while passwords are encrypted using one-way hashing, or DES crypt.

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.

ROCIS users must review and sign security agreement annually.

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, 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.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

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).

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 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

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 INFORMATION” and “HOW TO” guides for additional 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 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.

7.2 What procedures allow individuals to access their information?

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.

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

7.3 Can individuals amend information about themselves? If so, how?

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 are also able to update some of their own information.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

No

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application or project.

GSA requires all staff to complete privacy and security training.

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. Users must re-certify that they agree with the 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 warning banner upon entering the system and are required to agree to the terms before access.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

No

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system, application or project ensure that the information is used in accordance with the stated practices in this PIA?

The system owner is responsible for reviewing and updating (as needed) this privacy program plan 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.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

No

[1]OMB Memorandum *Preparing for and Responding to a 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.