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: 453
System Name: eRulemaking
CPO Approval Date: 1/16/2024
PIA Expiration Date: 1/15/2027

Information System Security Manager (ISSM) Approval

Joseph Hoyt

System Owner/Program Manager Approval

Peter Nguyen

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
eRulemaking

B: System, application, or project includes information about:
Federal employees, contractors, and the public

C: For the categories listed above, how many records are there for each?
FDMS is an online public docket and comment system. The FDMS facilitates the submission of public comments. PII collected includes name, address, government issued email address, phone number, fax number and organizational affiliation. The eRulemaking Program Management Office collects this type of information for managing federal employee accounts for FDMS. Regulations.gov submitter information is collected at the discretion of each partner agency in accordance with their policy and requirements to collect and process regulatory comments from the public.

D: System, application, or project includes these data elements:
Regulations.gov and the Federal Docket Management System (FDMS.gov)

Overview:

The eRulemaking Program is a federal E-Government shared Line of Business identified as part of the President's E-Government Strategy from February 27, 2002. The eRulemaking information systems provide shared services to partner agencies that comply with mandates under Section 206 of the E-Government Act of 2002 (H.R. 2458/S. 803).

The eRulemaking Management Office (PMO) manages the eRulemaking Program and is responsible for the development and implementation of two interrelated information systems. The logical and physical security boundaries for eRulemaking encompass these two systems.

FDMS.gov

The **Federal Docket Management System (FDMS)** is an electronic docket management system. Dockets (i.e., file folders) consist of supporting materials (i.e. documents) that provide context around proposed rules or other actions under consideration by regulatory agencies. The primary purpose of the system is to create a docket, associate it with any related published notifications from the Federal Register, populate it with documents, and make these materials available to the public through Regulations.gov. In turn, the public can review the supporting materials to submit informed comments on the proposed action. The public can also upload attachments with comments and information. The comments and attachments become documents in the docket, and the regulatory agencies can use FDMS to process, review and publish the comments back out through Regulations.gov for other members of the public to see. In addition to these primary functions, FDMS offers the federal agencies an adaptable solution to service a wide array of routinely performed regulatory activities, including the ability to:

- Run quick and advanced searches on dockets and documents
- Mark dockets and documents to "My Favorites" and "Flagged Documents"
- Manage and post attachments individually
- Simultaneously process the same action on a batch of multiple documents
- Run the deduplication engine to detect near duplicate public comment submissions (e.g., mass mail campaigns)
- Automatically categorize public comment submissions for easier distribution and review
- Conduct searches, including full text, document metadata, and the text of the first attachment file

Regulations.gov

Regulations.gov is the public-facing counterpart to FDMS. Public users are provided "one-stop" access to regulatory content that has been uploaded by multiple agencies through FDMS. On Regulations.gov, the public can:

- Search all publicly available regulatory materials, e.g., posted public comments, supporting analyses, FR notices and rules
- Submit a comment and/or upload an attachment related to an agency action or on another comment about the action
- Download agencies regulatory materials as a .csv file
- Access Regulations.gov API Terms of Service and link to api.data.gov/docs/regulations
- Submit an application or adjudication document
- Sign up for email alerts about a specific regulation
- Quickly access regulations that are popular, newly posted or closing soon - directly from the home page

All agency and public users' access ERM from the Internet. The preliminary design goal is to deliver as many of the ERM functions as possible to the end user via a web browser that is functioning only as the presentation layer (all the non-display and input/output (I/O) functions are performed by the central services). In those cases where application code must be executed on the workstation, the code will be small code modules that are only temporarily loaded on the workstation for execution. In the case of the imaging subsystem, fully functional client applications will need to be loaded on some agency workstation and/or an ERM server deployed at an agency location. The imaging subsystem components included at the agency support large volumes image processing (hard copy document conversion). These distributed imaging components are not included within the SSP. Maintaining these systems will be the responsibility of each agency with ERM technical support.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
The eRulemaking Program fulfils requirements for participating federal agencies established under Section 206 of the 2002 E-Government Act (H.R. 2458/S. 803). On July 1, 2019, The Office of Management and Budget released a memorandum directing the transfer of the e-Rulemaking Program Management Office (PMO) from the EPA to GSA. The memorandum authorized GSA to serve as the managing partner of the e-Rulemaking Program, effective October 1, 2019.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
GSA/OGP

https://www.federalregister.gov/documents/2019/10/08/2019-21885/privacy-act-of-1974-system-of-records

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.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
The records stored in this application fall into 2 groups; those for GSA, and those publicly-posted items for all other agencies. Group 1. For GSA's rulemaking records (for GSA only): Records of Proposed Rule Development DAA-GRS-2017-0012-0001 (GRS 06.6/010) Description: Records of internal development of agency rules in preparation for Federal Register publication as a proposed rule, including case files that result in final rules, case files that do not result in final rules, and case files of exemptions to rules. Includes: -briefing papers and options papers presented to management -rule/regulation drafts presented to management -internal comments in response to drafts presented to management -stakeholder input -analyses -clearances -summary sheets -background and supporting materials -records documenting a notice of inquiry (NOI) advance notice of proposed rulemaking (ANPRM), or request for information (RFI) in the Federal Register inviting comments on a not-yet-proposed rule, and comments received in response -concept releases -petitions to issue, amend, or repeal a rule -petitions for exemption -decision memoranda -reports and white papers -meeting minutes documenting evaluation of options and decisions made -work plans and timelines -correspondence Note: GRS 5.2, item 020, covers "drafts produced"¦for"¦internal discussion, reference, or consultation." Exclusion: Schedule and retain as part of a docket any records this item describes that the agency incorporates into that docket. Retention: Temporary. Destroy 6 years after publication of final rule or decision to abandon publication, but longer retention is authorized if required for business use. Proposed and Final Rule Documents Published in the Federal Register DAA-GRS-2017-0012-0002 (GRS 06.6/020) Description: Agency copy of rule forwarded to the Federal Register for publication, copy of published notice, and correspondence with the Office of the Federal Register generated at these rulemaking process milestones: -advance notice of proposed rulemaking (ANPRM) or notice of inquiry (NOI) inviting participation to help shape a rule still in development -notice of proposed rulemaking (NPRM) to add a new rule or to amend or repeal an existing rule -supplemental notice of proposed rulemaking (SNPRM) or further notice of proposed rulemaking (FNPRM), soliciting comment on a proposed rule significantly altered in response to comments received in response to the NPRM -notice responding to summarized comments -final rule, interim final rule, or direct final rule Retention: Temporary. Destroy 1 year after publication, but longer retention is authorized if required for business use. Public Comments DAA-GRS-2017-0012-0003 (GRS 06.6/030) Description: Public comments agency receives in response to a proposed rule, provided that agency retains a summary of those comments with the rulemaking docket in a docket management system. Exclusion: If the agency does not create a summary of comments, it must schedule individual comments as part of the final rule case file or docket. Retention: Temporary. Destroy 1 year after publication of the final rule or decision to abandon publication, but longer retention is authorized if required for business use. Federal Register Notices Other than Prepared and Final Rules DAA-GRS-2017-0012-0004 (GRS 06.6/040) Description: Records of notices 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. Note 1: SORNs per se are covered by GRS 4.2, item 150. Note 2: PRA Information Collection reports are covered by GRS 5.7, item 050. Note 3: Notices of meetings of committees established under the Federal Advisory Committee Act (FACA) are covered by GRS 6.2, item 050. Retention: Temporary. Destroy when 1 year old, but longer retention is authorized if required for business use. Group 2. For publicly-posted eRulemaking information for agencies other than GSA, use GSA schedule 352.2/011 and 021. Publicly-posted Information Records DAA-0352-2016-0001-0004 (352.2/011) Description: This series consists of content (information and documents) in a variety of formats posted by GSA on agency web sites hosted by GSA, and content posted on, or submitted via, those web sites by the public. Included are static web pages, historically insignificant public dialogues such as forums, surveys, and comment postings, regulatory or statutorily mandated public postings, and related records. This schedule item covers copies of content received from agencies and posted by GSA on the web sites. The record copy of the content (retained by the originating agency) is covered by the records schedules of the agencies that originated the content. The content posted to the web sites by the public is covered by this schedule item. Retention: Temporary. Cutoff at the end of the fiscal year in which the posting becomes superseded, obsolete, or canceled. Destroy 3 years after cutoff. Longer retention is authorized in order to comply with requirements for public posting stipulated by regulation, agency directives, OMB or GAO mandates, or similar authorities. Information Service Program Management Records DAA-0352-2016-0001-0005 (352.2/021) Description: This series of records is concerned with creating and managing an information resource (e.g., Data.gov and USA.gov) for use or reference by the public and/or Federal agencies in carrying out their work. Included are change management decisions, planning documents, promotional materials, review reports, correspondence, and related records. Retention: Temporary. Cut off at the end of the fiscal year. Destroy 3 years after cutoff. Longer retention is authorized if required to comply with requirements set forth in statutes, directives, agreements, contracts, OMB or GAO mandates, or similar authorities.

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?
PII collected may include name, address, email address, phone number, fax number and organizational affiliation. Partner agencies using the system do not require or request social security numbers, credit card numbers, bank account numbers, or other analytics data linkable back to the individual. The potential exists, however, for public users to submit unsolicited sensitive information, including PII, through Regulations.gov in the comment forms or uploaded documents. The eRulemaking Program Management Office collects limited personal information for managing federal employee accounts for FDMS. This is an inherent aspect of meeting federal information security requirements for identifying and authenticating privileged users, thus protecting the integrity, confidentiality and availability of regulatory information. Regulations.gov end users have the option to submit comments on proposed rulemakings and other federal agency actions anonymously, and this can fulfil requirements under the Administrative Procedure Act and E-Government Act for electronically receiving and considering public comment. For public users who choose to remain anonymous and/or wish to minimize the time and burden associated with data entry, this supports the mission of eRulemaking for increasing participation in the federal rulemaking process. However, Regulations.gov users are also given the option to submit as an individual or as a member of an organization. In these cases, the end users will be prompted to provide personal or organizational information. For both the public and the federal rule writers, this additional context may be helpful in supporting further outreach, identifying trends, and communicating the impacts of a rulemaking on specific stakeholders or sectors. For those users who wish to offer this context, this enhances public participation. The option of providing submitter information has been deemed necessary by partner agencies. Through governance decisions, the partner agencies have requested that the eRulemaking program support the collection of this information. Regulations.gov end users may also voluntarily provide email addresses to receive personalized services. For example, when signing up for notifications or filling out the "Contact Us" webform. This likewise supports the mission of increasing participation in the federal rulemaking process by reducing research burden, facilitating outreach, and improving user experience.

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?
System protections that prevent unauthorized access to eRulemaking data include the encryption of all data at rest as well as a role-based account system, the implementation of which allows the designation of varying degrees of data and control access.

3.4 Will the system monitor the public, GSA employees, or contractors?
Public

3.4 Explain: Please elaborate as needed.
FDMS maintains an audit trail of items posted to Regulations.gov. To the extent that public submitter information is collected, the system has 18 months of details of who was involved in posting. FDMS also contains the ability to allow users in agencies to assign and track the completion of dockets to other federal employees according to the level of responsibility deemed appropriate by that agency's designation of user-based roles.

3.5 What kinds of report(s) can be produced on individuals?
FDMS Agency Administrators can run the following two reports to support account management: List of Registered Users - List of active and locked out users in the agency with contact information. The purpose of the monitoring is to

support account management. List of Locked Out Users - List of locked out users in the agency with contact information. Other FDMS users can run a search on Documents by Submitter to support comment analysis. Controls for identification, authentication and role-based access help to prevent abuse by ensuring that partner agencies authorize access for appropriate individuals based on their roles.

3.6 Will the data included in any report(s) be de-identified?
Yes

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?
FDMS users can redact identifying information prior to publicly-posting comments on Regulations.gov. Original versions of the unredacted comments are maintained in the database, which cannot be accessed by public users through Regulations.gov. Original data in the backend FDMS database can be manually de-identified by agencies on a case-by-case basis. Access to agency data is limited to employees belonging to the same agency with the appropriate role-based access to do so. In all cases, the policies and processes of individual partner agencies drive decisions on de-identification.

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

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?
Yes

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?
Access to information in the backend FDMS database is limited to federal employees of the agency that owns the data for relevant dockets. Access is further limited by role-based access controls. Data that has been posted to Regulations.gov for the explicit purpose of public access through Regulations.gov is also shared through an application programming interface (API).

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?
FDMS account information is collected directly from the individual federal employee. Information collected from comment submitters who identify themselves as an individual on Regulations.gov is intended to be from the individual, although no mechanisms are in place to verify identity or authenticate the submitter. Information collected from submitters who identify themselves as a representative of an organization on Regulations.gov is likewise intended to be from the individual representative. In some cases, a document uploaded through the Regulations.gov comment form will include a compilation of multiple comments from various individuals in a group or organization. In these cases, the submitter is asked to confirm whether they are attaching files with multiple comment submissions, and if so, to provide the number of submissions. Whether the comment is direct from the individual or on behalf of one or more other individuals is the sole discretion of those making the comment. As described above, the collection of privacy information is limited to: user information for FDMS account setup; submitter information related to comment collection on Regulations.gov; and email addresses for users who wish to receive notifications or fill out the "contact us" form. The systems do not collect information from sources other than the individual or organization representative, including other IT systems, system of records, commercial data aggregators, or other Federal, state or local agencies.

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?
Data that has been posted to Regulations.gov for the explicit purpose of public access is also shared through an application programming interface (API). This is a one-way transmission of data that does not afford access to eRulemaking systems or otherwise require verification that the receiving system has undergone a security assessment and authorization to operate. Entities who wish to receive data through the API must request an API key from Regulations.gov API site hosted on open.gsa.gov/api/regulationsgov. In reverse fashion, FDMS receives a one-way data feed from the Government Publishing Office for Federal Register documents. These documents and related data do not include PII. A web form for submitting comments to Regulations.gov for specified Federal Register notices is embedded in FederalRegister.gov using the Regulations.gov API. This interconnection will be governed by an interconnection security agreement, which will include roles and responsibilities for reporting suspected or confirmed security incidents or breaches of PII. This will be put in place as part of the eRulemaking security authorization update. As part of this process, the Government Publishing Office, which supports this functionality for the Office of the Federal Register, will commit to complying with security requirements for an assessment and authorization to operate. Lastly, a public API for commenting is available to verified entities and is provided as a convenience to facilitate the bulk upload of comments from a number of different commenters. The use of the Comment API requires a key, which may be obtained through the open GSA website. By registering for, receiving and using a key to the Comment API, the key holder agrees to the following terms and conditions: When developing interfaces for commenters who will submit comment language and/or attachments through the Comment API, the key holder will include in the interface: -A link to the same terms of participation and privacy notice that users encounter on the comment form for Regulations.gov, and -A link to the Federal Register notice or other specific document in Regulations.gov for which the key holder is collecting or facilitating comments to be delivered through the Comment API. The key holder certifies that: -I will only submit comments through the Comment API that it has gathered through lawful means and that, to the best of the key holder's knowledge, represent comments from real persons, and -It has not and will not submit comments of its own creation under fictitious or misappropriated identities or otherwise in violation of federal law. -The API key may be disabled if an API key holder is determined to have violated these Terms of Participation. eRulemaking does not store or reveal the IP addresses in the API's HTTP request message for "POST" from the incoming client endpoints.

4.4Formal Agreement: Is a formal agreement(s) in place?
Yes

4.4NoAgreement: Why is there not a formal agreement in place?

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
All partner agencies maintain sole responsibility for the management of their records. Partner agency and program staff must all read and comply with the Rules of Behavior. Information requested and or posted is the sole responsibility of the partner agency.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
In FDMS user access is granted based on user role. Partner agencies manage user roles and access for their respective data. Those roles are agency administrator, docket manager, agency viewer, records manager and rule writer. The agency administrator can control agency accounts, determining which level of restrictions a user should have. Agencies can only access and manage data related to their own dockets.

6.1b: What is the authorization process to gain access?
The agency administrator can control agency accounts, determining which level of restrictions a user should have. Agencies can only access and manage data related to their own dockets.

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.
10/11/2023

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
Records in FDMS are maintained in a secure, password protected electronic system that utilizes security hardware and software to include multiple firewalls, active intrusion detection, encryption, identification and authentication of users, and role-based access controls. Any additional safeguards vary by the partner agency responsible for them. The systems are hosted at EPA's National Computer Center in Research Triangle Park, NC. The facility is protected by physical walls, security guards, and identification badges. Rooms housing the system infrastructure are locked, as are the individual server racks managed by the eRulemaking PMO. Backup servers for disaster recovery are housed in EPA's Potomac Yards building in Arlington, VA, which offers the same level of security. All security controls are reviewed on a periodic basis by external assessors. The controls themselves include measures for access control, security awareness training, audits, configuration management, contingency planning, incident response, and maintenance.

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?
The eRulemaking PMO employs the following methods for this purpose Scans for vulnerabilities in the information system are conducted once per week. Additional scanning is performed as needed to ensure vulnerabilities have been addressed. Web application scanning activities occur once per month. Vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: enumerating platforms, software flaws, and improper configurations; formatting and making transparent, checklists and test procedures; and measuring vulnerability impact; PMO personnel and contractors analyze vulnerability scans and results from security control assessments. Remediation of legitimate vulnerabilities in accordance with an organizational assessment of risk.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
In FDMS there is no requirement to submit a public comment. The user can decide whether to provide requested information or not. The standardized comment form on Regulations.gov affords users the opportunity to comment anonymously. Users consenting to provide submitter information are presented with the privacy and user notices at https://www.regulations.gov/privacyNotice and https://www.regulations.gov/userNotice.

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?
Requests must be submitted to the agency contact indicated on the initial document for which the related contested record was submitted. Privacy Act rules of both the partnering agency and GSA apply.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
FDMS information is controlled by individual partner agencies. The system collects public comments. All comments are assigned a tracking number. Requests for correction or amendment must identify the record to be changed and

the corrective action sought. Requests must be submitted to the agency contact indicated on the initial document for which the related contested record was submitted.

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.

It is the responsibility of each partner agency to train personnel on the Privacy Act and related internal agency policies. The eRulemaking provides general training services to FDMS users as part of its support contract. The FDMS training topics refer to privacy practices in the following ways: Privacy and user notices: Where the notices can be found on Regulations.gov, and when Regulations.gov users are presented with the notices in their workflow. Configuration: Which comment submitter fields can or cannot be selected for posting to Regulations.gov. Posting comments and using redaction capabilities: A recommendation that agency partners consider the existence of sensitive information, including PII, when making decisions on posting and redacting comments. That agency partners must adhere to their own agency policies, including the Privacy Act, on decisions for configuration, posting comments or redaction.

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?

This Privacy Impact Analysis is included in the package of materials required for information security reviews. GSA periodically facilitates third-party assessments to review all information security artifacts for compliance with the requirements, including the use of information in accordance with the PIA.