e-Rulemaking Program Administrative System

Privacy Impact Assessment

05/26/2021

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer
GSA IT
gsa.privacyact@gsa.gov

1800 F Street NW
Washington, DC 20405

Stakeholders

Name of Information System Security Manager (ISSM):

- Joseph Hoyt

Name of Program Manager/System Owner:

- Jennifer Hanna

Signature Page

Signed:

DocuSigned by:
Joseph Hoyt
CA8EE810EDA7425...

Information System Security Manager (ISSM)

DocuSigned by:
Jennifer Hanna
DBA226F2B0EA4C5...

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 making sure the PIA contains complete 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
5/17/2021	Updated with verbiage describing regulation entity validation.	3.0
5/26/2021	Approved	4.0

Table of contents

SECTION 4.0 LIMITS ON USES AND SHARING OF 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?

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 eRulemaking Program's systems. The Office of Government-wide Policy (OGP) may, in the course of eRulemaking, 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, 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

eRulemaking Program Administrative System

System, application or project includes information about

Federal employees, contractors, and the public

System, application or project includes

Regulations.gov and the Federal Docket Management System (FDMS.gov)

Overview

The eRulemaking Program is a collaborative, inter-agency initiative intended to establish a common automated and integrated approach to managing the federal government's rulemaking function. The project has consolidated the rulemaking systems of various Federal Departments and Agencies and centrally manages them in a web-based environment through two URLs:

- Regulations.gov provides the public with one-stop access to rule(s) and notices, supporting docket content, search capabilities, and the ability to comment on rules and notices published in the Federal Register. Other docket types that accept public comment are also posted through the FDMS by partner agencies.
- FDMS.gov provides secure log-in for Federal users of the system to upload and post electronic dockets to Regulations.gov, and to review and post comments.

SECTION 1.0 PURPOSE OF COLLECTION

1.1 Why is GSA collecting the information?

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.

1.2 What legal authority and/or agreements allow GSA to collect 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.

1.3 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?

Publicly searchable information stored by FDMS may include name, address, government issued email address, phone number, fax number, and organizational affiliation. The inclusion of such data and the responsibility to comply with privacy laws and regulations for respective records is the sole responsibility of the partnering agency that uses the eRulemaking systems. All FDMS users must take steps to protect all transferred and stored data in accordance with the Privacy Act (5 U.S. Code 552a), Trade Secrets Act (18 U.S. Code 1905), and the Unauthorized Access Act (18 U.S. Code 2701 and 2710). This information is stored in the FDMS database. Partner agencies are responsible for uploading and downloading their respective information. eRulemaking maintains the repository but is not responsible for the content. GSA has a SORN in place for its e-Rulemaking Program Administrative System, which allows GSA to manage partner agencies' users' credentials: names, government issued email addresses, telephone numbers, and passwords:

GSA-OGP-1, e-Rulemaking Program Administrative 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.

No ICRs apply specifically to eRulemaking systems. Participating partner agencies who use Regulations.gov and FDMS are responsible for meeting any requirements under the Paperwork Reduction Act for the individual rulemakings or other actions for which electronic dockets are established.

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.

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.

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

The eRulemaking Program Management Office collects information for managing federal employee accounts for FDMS. As part of the process of submitting comments through Regulations.gov, public end users (submitters) may be asked to complete fields for submitter information, including name, address, email address, phone number, fax number, and organizational affiliation. For the comments themselves, end users can either type information related to their comment into a free-form field or upload an electronic file with their comments. The potential exists for end users to submit sensitive information, including PII, in the comment forms or uploaded documents. Regulations.gov end users may also voluntarily provide email addresses when signing up for notifications or filling out the "Support" webform. The data from these submitter information fields and comments are processed and stored in FDMS. This involves two categories of privacy risk:

- Publicly posting privacy information: Comments and public submitter information sent through Regulations.gov are initially only accessible through FDMS to the agency that manages the document being commented on. Through FDMS, each partner agency chooses which comments will be posted to Regulations.gov for other end users to see on the publicly-accessible Regulations.gov website. Each agency also has the ability to redact sensitive information and choose which fields of submitter information will be displayed prior to posting the comments. As of May 17, 2019 the FDMS settings give partner agencies the option to publicly post: first name; last name; city, state and zip code of private address (without the street address); and organizational information, including organization address. Personal street address, email, phone and fax information cannot be posted. It is at the partner agency's discretion for whether they review all comments and uploaded documents for sensitive information or whether they choose to make use of FDMS redaction capabilities. All end users submitting comments are exposed to a privacy notice (https://www.regulations.gov/privacyNotice) and user notice (https://www.regulations.gov/userNotice) prior to submitting information.
- Unauthorized access to database information not publicly posted: System protections that prevent unauthorized access to FDMS user account information and information for Regulations.gov submitters 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.

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.

Yes, please see the Privacy Notice (https://www.regulations.gov/privacyNotice) and User Notice (https://www.regulations.gov/userNotice) regarding comment submission. Excerpt follows:

"Any information (e.g., personal or contact) you provide on this comment form or in an attachment may be publicly disclosed and searchable on the Internet and in a paper docket and will be provided to the Department or Agency issuing the notice. To view any additional information for submitting comments, such as anonymous or sensitive submissions, refer to the Privacy Notice and User Notice, the Federal Register notice on which you are commenting, and the Web site of the Department or Agency."

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

Aside from the measures for restricting partner agencies from posting certain privacy-related information about public submitters, the FDMS system does not present risks to openness and transparency. Agencies using FDMS are fully empowered to decide whether a particular document in the rulemaking docket is public. As the owner of publicly submitted comment data, the decision to post or not post submitted information is a matter of policy and discretion of the particular partnering agency.

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?

Federal employees, contractors, and members of the public commenting on regulations.

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

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.

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

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.

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

FDMS does not aggregate data in such a way that new sensitive data can be derived about individuals.

3.5 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.

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

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.

3.7 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.

3.8 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?

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.

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

All privacy-related data is collected solely for the stated purposes described in section 3.3 of this document. In the case of submitter data, Regulations.gov users have the option to submit comments anonymously. In a modernization of Regulation.gov in September 2019, the eRulemaking PMO implemented a standard form that provided all submitters this option for comments to all agencies.

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 eRulemaking Program Management Office collects limited privacy 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 purpose of the collection 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 purpose of the collection for increasing participation in the federal rulemaking process by reducing research burden, facilitating outreach, and improving user experience.

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?

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 or is it taken from another source? If so, 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? If so, who, how and is a formal agreement(s) in place?

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.

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

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). Although certain fields of submitter information are not posted, potential exists for end users to submit sensitive information, including PII, in the comment forms or uploaded documents.

All end users submitting comments are exposed to a privacy notice (https://www.regulations.gov/privacyNotice) and user notice (https://www.regulations.gov/userNotice) prior to submitting information. This includes the following language, "The material you submit to a federal department or agency through Regulations.gov may be seen by various people. Any personal information included in the comment form or in an attachment will be provided to the department or agency to which your comment is directed and may be publicly disclosed in a docket or on the Internet (via Regulations.gov, a federal agency website, or a third-party, non-government website with access to publicly-disclosed data on Regulations.gov)."

Through FDMS, each partner agency chooses which comments will be posted to Regulations.gov for other end users to see on the publicly-accessible Regulations.gov website and API. Each agency also has the ability to redact sensitive information. It is at the partner agency's discretion for whether they

review all comments and uploaded documents for sensitive information or whether they choose to make use of FDMS redaction capabilities.

The only alternatives for fully mitigating the risk of public users including privacy information in comments would be for agencies to review every comment and/or to not post comments back to Regulations.gov and the API for other users to access. The partner agencies in the eRulemaking governance structure have deemed it necessary to post comments, or representative comments, despite not having certainty that sensitive information is contained within the comments.

System protections that prevent unauthorized access to FDMS user account information and information for Regulations.gov submitters 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.

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?

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.

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?

In FDMS Information use is the sole responsibility of the partner agency collecting the information. FDMS maintains the integrity and availability of the information. Risk would thereby be defined by any associated agency policy or practice with respect to the use of personal information. Maintaining the

integrity and verification of data quality is performed in accordance with those policies and practices.

As a mitigation strategy each partner agency has access to training that would ensure their ability to use the system in accordance with their needs. Partnering agencies also sit in governance bodies that allow their input to the policy needs that drive system development.

There is a risk that unauthorized access to database information would allow third parties to alter the information. The eRulemaking systems mitigate risk to data integrity through 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.

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?

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.

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

GSA completed a system security plan for the eRulemaking information systems. This plan will be periodically reviewed and updated as part of external security assessments.

6.3 How will the system or application be secured from a physical, technological, 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 suspected or confirmed security incidents and breaches of PII? If so, 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.

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?

Risks inherent to a network connected system exist for FDMS. As a mitigation strategy, 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, and role-based access controls. Managing partner agencies are responsible for compliance with the Privacy Act and related privacy laws, regulations, and policies for their respective records in the system. Responses to external requests for their respective records in the system. Responses to external requests for access to partner agency information within the system is the sole discretion of the partner agency that owns the data. All users must take steps to protect all transferred and stored data in accordance with the Privacy Act (5 U.S. Code 552a), Trade Secrets Act (18 U.S. Code 1905), and the Unauthorized Access Act (18 U.S. Code 2701 and 2710). This information is stored in an eRulemaking database. Partner agencies are responsible for uploading and downloading their respective information. eRulemaking maintains the repository but is not responsible for the content. Signed MOUs and a SORN are in place.

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.

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.

7.2 What procedures 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? If so, how?

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.

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?

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). Although certain fields of submitter information are not posted, potential exists for end users to submit sensitive information, including PII, in the comment forms or uploaded documents.

All end users submitting comments are exposed to a privacy notice (https://www.regulations.gov/privacyNotice) and user notice (https://www.regulations.gov/userNotice) prior to submitting information. This includes the following language, “The material you submit to a federal department or agency through Regulations.gov may be seen by various people. Any personal information included in the comment form or in an attachment will be provided to the department or agency to which your comment is directed and may be publicly disclosed in a docket or on the Internet (via Regulations.gov, a

federal agency website, or a third-party, non-government website with access to publicly-disclosed data on Regulations.gov)."

Through FDMS, each partner agency chooses which comments will be posted to Regulations.gov for other end users to see on the publicly-accessible Regulations.gov website and API. Each agency also has the ability to redact sensitive information. It is at the partner agency's discretion for whether they review all comments and uploaded documents for sensitive information or whether they choose to make use of FDMS redaction capabilities.

The only alternatives for fully mitigating the risk of public users including privacy information in comments would be for agencies to review every comment and/or to not post comments back to Regulations.gov and the API for other users to access. The partner agencies in the eRulemaking governance structure have deemed it necessary to post comments, or representative comments, despite not having certainty that sensitive information is contained within the comments.

System protections that prevent unauthorized access to FDMS user account information and information for Regulations.gov submitters 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.

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.

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.

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?

There is a risk that partner agencies do not train their own personnel on the Privacy Act and related internal agency policies. Agency decisions on system configuration and processes for comment review and posting should be made in compliance with those policies. To mitigate this risk, eRulemaking PMO training highlights these issues and encourages FDMS users to seek out Privacy guidance and training from their own agencies.

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?

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.

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?

There is a risk that periodic third-party assessments would not have information to support their audits. To mitigate this risk, the PMO retains audit logs of comment posting activities for a retention period of 18 months.

---

[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.