Executive Office for Immigration Review

Privacy Impact Assessment
for
DocketScope

Issued by:
Justine Fuga
Senior Component Official for Privacy

Approved by: Christina Baptista
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: June 30, 2025

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

DocketScope is a FedRAMP authorized, Software-as-a-Service (SaaS) offering by the Regulatory Group, Inc., that the Executive Office of Immigration Review (EOIR), Office of Policy (OP), uses to manage public comments received pursuant to the notice-and-comment rulemaking process. Members of the public may submit rulemaking-related comments to the General Services Administration's (GSA's) Federal Docket Management System (FDMS) via the public-facing analog, Regulations.gov or by mail. [1] DocketScope automatically downloads comments from FDMS for EOIR-related rulemakings. EOIR is also able to scan and upload comments received by mail to Docketscope. EOIR then reviews submitted comments in DocketScope for consideration and response.

The DocketScope system involves processing public comments received in response to rulemaking, which may contain the following information types: regulatory, policy, and agency guidance information; names, contact information, and geographic location (city and state) of public commenters, and any other personal information that a member of the public may choose to disclose about themselves through their comments; user account and system activity/audit information for authorized EOIR users. Because the system collects, maintains, and/or disseminates personally identifiable information (PII), EOIR is conducting this privacy impact assessment (PIA) in accordance with Section 208 of the E-Government Act of 2002.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

DocketScope is used to manage public comments to proposed rulemakings and other documents published in the Federal Register. Public comments may be received electronically or by mail. DocketScope provides a variety of capabilities to efficiently gather, group, categorize, organize, review, and redact public comments. DocketScope leverages artificial intelligence to group

[1] More information about the FDMS and Regulations.gov websites is available at https://www.fdms.gov/about-us.

comments together as duplicates or near duplicates by detecting similarities among comments. To expedite review, EOIR users view these groups using a comparison tool that highlights differences between comments. EOIR also creates issue outlines in DocketScope and labels comments by issue area to facilitate review of these comments by subject and to begin the process of drafting final regulations. A report is created by grouping the text of the comments by issue and subject. The report is used to assist EOIR staff in analyzing and addressing public comments as the agency proceeds through the rulemaking process.

DocketScope manages public comments that often contain personal information about members of the public submitting comments, such as the commenter's name, contact information (email, phone number, address), and geographic location (city and state). Commenters may also choose to disclose other personal information about themselves, though EOIR does not actively solicit such information. Commenters may submit their comments anonymously and are not required to provide personal information to submit a public comment. Commenters may also request that any PII be redacted from their comments before their comments are publicly posted on the Regulations.gov website.

Authorized EOIR personnel access DocketScope through a web browser on approved DOJ devices. Users establish unique user accounts with usernames and passwords. DocketScope also requires multi-factor authentication of user identities with each user's attempt to log in to the system.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	5 U.S.C. § 553(c) (codifying Administrative Procedure Act (APA), Pub. L. 79-404, 60 Stat. 237, requirement mandating agencies to consider and respond to significant comments received during public comment periods in administrative rulemaking process). Section 206 of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2915-16 (codified at 44 U.S.C. § 3501 note) (requiring agencies to accept public comments by electronic means to the extent practicable). EOIR Authorizing Statutes: 8 U.S.C. §§ 1101 et seq., 1103(g), 1158, 1159, 1154, 1229a, 1255, 1255a, 1324a, 1324b, 1324c.
Executive Order	
Federal regulation	EOIR Regulations: 8 C.F.R. Parts 1000 – 1399.

	8 C.F.R. § 1003.0(b) (describing role and authorities delegated to EOIR Director to direct and supervise the agency in performing its mission). 8 C.F.R. § 1003.0(e) (describing role and authorities delegated to Office of Policy to include regulatory development and implementation).
Agreement, memorandum of understanding, or other documented arrangement	DOJ EOIR entered into a subscription agreement with The Regulatory Group, Inc., the developer of DocketScope (formerly DocketCAT), on August 4, 2021, and this subscription agreement remains in effect.
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, D	Names of EOIR personnel, other federal government personnel, and members of the public (USPER and non-USPER)
Business contact information, e.g., email address, phone number, address of a business	X	A, B, C, D	Business address, email and/or phone number of EOIR personnel, other federal government personnel, and members of the public (USPER and non-USPER).
Personal contact information, e.g., email address, phone number, home address	X	C, D	Personal address, email and/or phone number of members of the public (USPER and non-USPER) submitting comments
Date of birth or age	X	C, D	Members of the public (USPER and non-USPER) may voluntarily provide this information in comments
Place of birth	X	C, D	Members of the public (USPER and non-USPER) may voluntarily provide this information in comments
Sex	X	C, D	Members of the public (USPER and non-USPER) may voluntarily provide this information in comments
Race, ethnicity, or citizenship	X	C, D	Members of the public (USPER and non-USPER) may voluntarily provide this information in comments
Religion	X	C, D	Members of the public (USPER and non-USPER) may voluntarily provide this information in comments
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	C, D	Members of the public (USPER and non-USPER) may voluntarily provide this information in comments
Passport number			
Mother's maiden name			
Vehicle identifiers			
Medical records number			
Medical notes or other medical or health information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Financial account information	X	C, D	Members of the public (USPER and non-USPER) may voluntarily provide this information in comments
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	Usernames or user ID of EOIR personnel authorized to access the system
- **User passwords/codes**	X	A	Password of EOIR personnel authorized to access the system
- **IP address**	X	A	IP address of EOIR personnel authorized to access the system
- **Date/time of access**	X	A	Date/time of access of EOIR personnel authorized to access the system
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Although EOIR anticipates the above categories of PII, it is possible that other types of PII may be included in public comments. Given the varied nature of rulemaking, it is not possible to identify all the possible categories of PII that could be received.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax	X	Online	X
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): Federal, state, local, tribal, and foreign government entities may comment on rulemakings.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers					
Other (specify): Members of the public, including individuals and businesses, are permitted to comment on rulemakings.					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X	X	X	EOIR internally shares information with personnel who need to know the information to perform their job duties.
DOJ Components				
Federal entities				
State, local, tribal gov't entities				
Public				

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

Comments are publicly made available on the Regulations.gov website. An individual may submit comments anonymously, and commenters may request that any personal information included in a comment be redacted or removed prior to public posting of the comment. Before comments are publicly posted on Regulations.gov, EOIR reviews all comments and removes or redacts PII in accordance with any requests received from commenters to withhold their personal information. It is also EOIR's practice to redact PII relating to third parties that may have been submitted as part of a comment.

Section 5: Notice, Consent, Access, and Amendment

5.1 What kind of notice, if any, will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Privacy Act § 552a(e)(3) notice? Will a System of Records Notice (SORN) be published in the Federal Register providing generalized notice to the public? Will any other notices be provided? If no notice is provided to individuals or the general public, please explain.

In each notice of proposed rulemaking and other Federal Register publications seeking public comment, EOIR includes the following warning to commentors who may want any PII redacted from their comments: "If you want to submit personally identifying information (such as your name, address, etc.) as part of your comment, but do not want it to be posted online, you must include the phrase 'PERSONALLY IDENTIFYING INFORMATION' in the first paragraph of your comment and identify what information you want redacted."

A Privacy Notice (https://www.regulations.gov/privacy-notice) and User Notice (https://www.regulations.gov/user-notice) are also available to all individuals on the Regulations.gov website and inform individuals about how their information is collected, used, shared, and otherwise processed in the federal regulatory process supported by the website. Similar notices are available on the FDMS.gov website (https://www.fdms.gov/privacy-notice).

Finally, EOIR generally informs individuals about how the agency collects, uses, shares, and processes their PII through: (1) SORNs published in the Federal Register and available on the DOJ website (https://www.justice.gov/opcl/doj-systems-records#); (2) Privacy Act § 552a(e)(3) notices displayed on EOIR information collections and public-facing applications that collect PII; and (3) the DOJ Privacy Policy, linked on the common footer of the EOIR website (https://www.justice.gov/doj/privacy-policy). The DocketScope website also provides a privacy and security notice (https://www.docketscope.com/legal/) describing how the company collects, uses, and shares personal information when using the DocketScope product.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals are not required to submit comments in response to Departmental rulemaking or Federal Register notices, but individuals may voluntarily choose to do so. PII is not required to submit a comment. An individual may submit comments anonymously, and commenters may request that any personal information included in a comment be redacted or removed prior to public posting of the comment. Individual members of the public submitting comments have control over the inclusion of PII and any other information identified in the content of a comment, and do so knowing that their comments will be maintained, used, and disseminated by EOIR.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Individuals may submit a Privacy Act access or amendment request with EOIR's Freedom of Information Act (FOIA) Office. Instructions for making such requests are available on the EOIR website (https://www.justice.gov/eoir/freedom-information-act-foia). Individuals may also follow the record access and amendment procedures described in applicable SORNs identified in Section 7 of this PIA.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** This system was most recently authorized on July 23, 2024, and this authorization expires July 23, 2025. EOIR is currently completing the process for ongoing authorization beyond July 23, 2025. **If an ATO has not been completed, but is underway, provide status or expected completion date:** N/A **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** There are no outstanding POAMs for any privacy controls.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain: N/A
X	**This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** EOIR has assigned a FIPS 199 security categorization of Moderate, consistent with the categorization assigned to DocketScope through the FedRAMP authorization process. Because EOIR inherits many of the controls from the vendor operating the system, EOIR is assigning its instance of the product the same Moderate security categorization.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The Regulatory Group conducts monthly vulnerability scans, annual incident response testing, and annual penetration testing of the operating system, databases, and web applications, and all system inventory components of DocketScope. Vulnerability findings are evaluated monthly. When vulnerabilities are identified, DocketScope creates a plan of action and milestones to correct, reduce, or eliminate identified vulnerabilities. Before implementing any changes to the system, DocketScope tests, validates, and documents changes, and changes are only approved after a Security Impact Analysis. DocketScope also monitors daily physical access to system hardware to monitor for suspicious activity.

	In accordance with DOJ Order 0908, *Use and Monitoring of DOJ Information Technology, Information Systems, and Access to an Authorized Users' Electronic Information*, EOIR performs daily monitoring of cybersecurity incidents and conducts annual cybersecurity incident response testing and evaluation of alerts for cyber threats to safeguard and protect EOIR's data from spills and/or leaks.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The following types of events are logged by DocketScope for auditing purposes: successful and unsuccessful account log on events, account management events, object access, policy change, privilege functions, process tracking, system events, all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. Audit logs are configured to generate audit records that include the time, where, source of event that occurred, host information, the outcome of the event, and the identity or service associated with the event. Audit records are maintained for at least 90 days but not longer than one year. Audit logs are reviewed weekly for indications of inappropriate or unusual activity. EOIR collects and maintains audit logs for 120 days and reviews audit logs weekly to ensure compliance with security and privacy standards.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** A user manual is available to ensure system users know how to properly use the system for its intended purposes, including how to use the system to adequately maintain the confidentiality, integrity, and availability of information within the system. EOIR OP coordinates as needed with DocketScope to provide demonstrations of the system to authorized EOIR users.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

Access to the DocketScope system is limited to authorized EOIR employees and contractors responsible for reviewing comments or as system administrators. User permissions and access to information in the system are tailored based on the particular user's role. To maintain access to the system, EOIR users are required to annually complete cybersecurity and privacy awareness trainings and to review and sign EOIR's Rules of Behavior regarding use of EOIR information

systems. Authorized users may only access the system by entering a correct username and password and after verifying their identity with multi-factor authentication. EOIR user accounts are reviewed annually to determine whether continued access is necessary, and users accounts are automatically disabled after 90 days of inactivity. Users are required to reset passwords every 90 days. User accounts are locked for specified periods of time after a specified number of unsuccessful log-in attempts. Users will be disconnected from the system after 15 minutes of idle time.

Comments are shared between FDMS/Regulations.gov and DocketScope through an encrypted connection. The Regulatory Group conducts regular vulnerability scanning and configuration management activities on DocketScope to minimize privacy risks associated with the download of public comments from the publicly accessible Regulations.gov website.

System and user activity is regularly monitored, logged, and audited to detect suspicious activity. Data is encrypted in transit and at rest. DocketScope also utilizes a variety of other security mechanisms to minimize privacy and security risks, including but not limited to firewalls and antivirus software.

Data stored in the DocketScope system is backed up daily and weekly.

Before comments are publicly posted on Regulations.gov, EOIR reviews all comments and removes or redacts PII in accordance with any requests received from commenters to withhold their personal information. It is also EOIR's practice to redact any PII included in a comment pertaining to third parties.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.

The comments uploaded to DocketScope, and associated agency work product contained therein, are unscheduled records and may not be deleted or disposed of. Any comments that have been posted publicly are also available and maintained on Regulations.gov.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. _X_ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 64 FR 73585 (Dec. 30, 1999); 66 FR 8425 (Jan. 31, 2001); 72 FR 3410 (Jan. 25, 2007) (rescinded by 82 FR 24147); and 82 FR 24147 (May 25, 2017).

JUSTICE/DOJ-003, "Correspondence Management Systems (CMS) for the Department of Justice," 66 FR 29992 (Jun. 4, 2001); 66 FR 34743 (Jun. 29, 2001); 67 FR 65598 (Oct. 25, 2002); 72 FR 3410 (Jan. 25, 2007) (rescinded by 82 FR 24147); 82 FR 24147 (May 25, 2017); and 28 C.F.R. § 16.130 (exemptions claimed pursuant to 5 U.S.C. §§ 552a(j),(k)).

Copies of these SORNs are available online at https://www.justice.gov/opcl/doj-systems-records#.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Type of technology employed (e.g. AI/ML),***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

There is a risk that the system inadvertently collects more information than may be necessary for EOIR to complete the administrative notice-and-comment rulemaking process. The FDMS/ Regulations.gov website does not restrict the amount or type of information that members of the public may include in comments on rulemakings, including any PII voluntarily included by the commenter. To mitigate this risk, several notices are provided to proactively inform and remind

the individual that the individual voluntarily chooses the information to include in comments, how such information may be used by the agency, and how the individual may request that any PII included in a comment be withheld before a copy of the comment is made publicly available. Those notices are described in Section 5 of this PIA.

There is a risk that commenters provide PII about third parties who do not have an opportunity to consent to the inclusion or public publication of their information. Therefore, it is EOIR's practice to redact any third-party PII from comments before making the comments publicly available online.

EOIR currently does not have a record retention schedule for records maintained in the DocketScope system. The longer that EOIR retains information about individuals, the more opportunities exist for a spill or breach of that information. Such risk will be mitigated once EOIR completes a record retention schedule that permits EOIR to appropriately dispose of records maintained in the system. EOIR is in the process of developing a record retention schedule for approval by the National Archives and Records Administration.

EOIR may receive numerous comments from a variety of commenters. Given the volume and varied nature of comments received by EOIR during the rulemaking process, the system maintains significant quantities of information, including PII. EOIR must carefully monitor access and use of the information to protect against unauthorized activity. EOIR mitigates this risk by only granting access to employees and contractors who complete the requisite security clearance, identity validation, and annual security and privacy training, and who annually review and acknowledge DOJ's Rules of Behavior to maintain system access. System access and activity are all restricted to users with an authorized need to know, and permissions are tailored to the particular user's role. User accounts are reviewed regularly and deactivated after a specified period of inactivity. Moreover, user activity audits are conducted regularly to monitor suspicious activity. Several virtual and physical security measures are in place to safeguard information, including IT monitoring tools; firewalls; intruder detection and data loss prevention mechanisms; and audit logs. System hardware, such as servers, are located in secure facilities. Data is also encrypted in transit and at rest.