Form FMC-15
Federal Maritime Commission
Privacy Impact Assessment (PIA)

Published 11/6/2026

System: Privacy Act Requests

Section 1. System Overview:

1.1 Describe the project/system and its purpose. (Note: this section is an overview; the questions below elicit more detail.)

The Privacy Act Requests system at the Federal Maritime Commission (FMC or Commission) maintains/stores all records related to: requests made pursuant to the Privacy Act (including access and consent forms in digital format pursuant to OMB M-21-04); accountings of disclosure of Privacy Act records; and appeals of adverse agency determinations.

All records are stored within SharePoint folders, accessible via FMC-issued laptops and phones (though the latter would very rarely, if ever, be used for this purpose). External users are unable to access records. Only internal FMC users who are given access by the Office of Information Technology (OIT) to the Office of the Secretary's Sharepoint folder will be able to access the folders that contain these records. Information will be collected from point of receipt of a Privacy Act-based request until the FMC makes a determination about the request, and when relevant, until the point that an appeal of an adverse determination is decided; during and after the processing of the request, the information related to each request will then be stored in its own SharePoint folder.

Additionally, requests for disclosure of Privacy Act records will be collected from point of receipt of the request until the FMC completes an accounting of the disclosure. During and after the processing of the request, the information related to each request will then be stored in its own SharePoint folder.

	Authority	Citation/Reference
	Statute	5 U.S.C. § 552a(c) and (d)
	Executive Order	
	Federal Regulation	46 C.F.R. §§ 503.60-503.69
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3. Data Type, Sources and Use

3.1 Indicate in the table below what general categories of PII are being collected Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

General Categories of PII		
☒ Full Name	☐ Credit Card Number	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)
☒ Date of Birth	☐ Facsimile Number	☐ Geolocation Information
☒ Home Address	☒ Medical Information	☒ Passport Number
☒ Phone Number(s)	☐ Education Records	☐ User ID
☒ Place of Birth	☒ Social Security Number	☐ Internet Cookie Containing PII
☒ Age	☐ Mother's Maiden Name	☒ Employment Status, History, or Information
☐ Race/ethnicity	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ Employee Identification Number (EIN)

☐ Alias	☐ Audio Recordings	☐ Salary
☐ Sex	☐ Photographic Identifiers (e.g., image, x-ray, video)	☐ Military Status/Records/ ID Number
☒ Email Address	☒ Certificates (e.g., birth, death, marriage, etc.)	☐ IP/MAC Address
☒ Work Address	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Investigation Report or Database
☒ Taxpayer ID	☐ Vehicle Identifiers (e.g., license plates)	☒ Driver's License/State ID Number (or foreign country equivalent)
☐ Other (Please Specify):		

3.2 Provide the source(s) of the information (e.g., directly from the individual to whom the information pertains; Government (Federal, State, local, tribal); non-government sources (members of the public, public media, internet).

The sources of the information the system collects, maintains, and uses are from external individuals who request access to Privacy Act records; internal FMC employees; and employees from other Agencies.

Section 4. Information Sharing:

4.1 What are all the Federal Maritime Commission's intended uses of the PII collected (e.g., civil enforcement, administrative matters, or human resources)?

The FMC's Office of the Secretary (OS) administering the Privacy Program does not request PII/SSNs for the purpose of intended use, but SSNs may incidentally be collected when obtaining agency records to process and review Privacy Act requests and appeals for access to, correction of, or an accounting of disclosure of records under the Privacy Act.

4.2 Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the intended uses described above and to further the Federal Maritime Commission's mission.

To support the FMC's internal mission activities, the information collected is necessary to process and review requests and appeals for access to, correction of, or an accounting of disclosure of records under the Privacy Act; to determine the status of requested records or the request for correction or disclosure; to respond to such requests and appeals; and to maintain records documenting the consideration and disposition of these requests.

4.3 With whom does the FMC intend to share the information in the system (e.g., within the agency, foreign/federal/state/local authorities, public, etc.) and how will the information be shared (e.g., case-by-case basis, bulk transfer, or direct access)?

Only internal FMC users who are given access by the OIT to the Office of the Secretary's SharePoint folder will be able to access the folders that contain these records. The system does not share data with the public or external users, and they cannot access any records stored within it.

4.4 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.

Information is not intended for "Open Data" purposes.

Section 5. Data Accuracy and Security:

5.1 What procedures are in place to ensure that the information is accurate, complete, and up to date?

It is generally the responsibility of the person (includes companies) submitting the information to ensure the completeness, accuracy, and currency of data before

submission. Since records within the Privacy Act Requests system include compiled agency records from other systems of records, authorized personnel who collect, use, or maintain the source information and records in those systems of records will review the accuracy, completeness, and currency of the data as needed to perform their duties. This review considers multiple factors, such as reliability of the source providing the data and comparing the information submitted with previously submitted information.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system (e.g., access/security controls, monitoring/testing/evaluation, auditing, privacy training, automatic purging of information, MOUs)?

The FMC protects its information resources with a dynamic set of security measures. Some of these measures (e.g., network firewalls, physical security) protect the entire FMC enterprise, while other measures (e.g., user access restrictions, encryption) are applied to specific information systems. Following the risk-based policy established in the Federal Information Modernization Act (FISMA), the FMC applies more security measures (also known as security "controls") to information systems that present higher operational risks. Consistent with this policy, the FMC applies specific security controls to systems that collect and process PII. A comprehensive list of the security and privacy controls the FMC may apply to its information systems can be found in National Institute of Standards and Technology (NIST) Special Publication No. 800-53 (revision 5), https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

The FMC purchases cloud computing services from providers that have been authorized under the Federal Risk and Authorization Management Program (FedRAMP). Cloud service providers that have received this authorization have demonstrated that they apply security controls to their computing resources in a manner that is consistent with the federal risk-based information security requirements the FMC follows. New and current staff are required to complete a self-paced privacy awareness course available through the FMC's Learning Management System.

Section 6. Data Retention and Disposal

6.1 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 or necessary.

The records pertaining to Privacy Act requests are retained and disposed of in accordance with the National Archives and Records Administration's General Record Schedule 4.2—Information Access and Protection Records.

Section 7. Notice, Consent, and Redress:

7.1 Will individuals be notified if their information is collected, maintained, or disseminated by the system (e.g., system of records notice, Privacy Act 552a(e)(3) notice)? Please specify. If no notice is provided, please explain.

Yes. A system of records notice (SORN) will be published in the Federal Register, and on FMC's privacy program webpage. Also, a Privacy Act 552a(e)(3) notice (i.e., Privacy Act Statement) will be provided at the point of collection, specifically, on the Privacy Act Requests digital access and consent forms. These forms will list the SORN for this Privacy Act Requests System and provide a direct link to the SORN.

7.2 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.

Providing the requested information on the Privacy Act Requests digital access and consent forms is voluntary, and submission of these forms triggers the collection of information into the Privacy Act Request system. However, Privacy Act requests will not be processed if requested information is not furnished.

7.3 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 follow the procedure described in 46 C.F.R. Part 503, Subpart H, as well as in the SORN once the SORN is published in the Federal Register and posted on FMC's privacy program webpage. To seek access to and amendment of records, please visit Submit a Privacy Act Request webpage.

Section 8. Website Privacy Evaluation

8.1 Does the project/system employ the use of a website or application?

All records are stored within SharePoint folders, accessible via FMC-issued laptops and phones. SharePoint Online is part of Microsoft 365 Government Community Cloud (GCC) environment. SharePoint is Software-as-a-Service (SaaS) solution authorized at FedRAMP moderate level.

8.2 If so, describe any tracking technology used by the website or application and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

Not applicable.

8.3 Does the project/system employ the use of a third-party website or application?

SharePoint is Microsoft application/service and is considered a third-party application.

8.4 If so, include: the specific purpose of the agency's use of the third-party website or application; ii. any PII that is likely to become available to the agency through public use of the third-party website or application; iii. the agency's intended or expected use of PII; iv. with whom the agency will share PII; v. whether and how the agency will maintain PII, and for how long; vi. how the agency will secure PII that it uses or maintains; vii. what other privacy risks exist and how the agency will mitigate those risks; and viii. whether the agency's activities will create or modify a "system of records" under the Privacy Act. (This may be done as a separate PIA.)

Parts i though vi are answered in the above Sections 1 through 6. Part viii is answered in the below Section 9. Regarding the remaining Part vii about identifying privacy risks and mitigating such risks, please see below.

Risk	Mitigation Strategy
There is a risk that information in the SharePoint system will be used by or shared with unauthorized user	Prior to receiving access to the FMC's network, all users must agree to the FMC Rules of Behavior, which includes consenting to monitoring and restrictions on data usage. Also, all users are required to complete Privacy and Information Security Awareness Training, which includes information on rules and regulations regarding the sharing of PII.
Unauthorized system access	External users are unable to access records. Only internal FMC users who are given access by OIT to the Office of the Secretary's SharePoint folder will be able to access the folders that contain these records. Additionally, all FMC users must have a government issued personal identity verification (PIV) card to access the SharePoint system. FMC's user identity management processes include authentication with enterprise directory to control and manage access restrictions to authorized personnel on an official need-to-know basis. Auditing procedures are in place that comply with OMB Memorandum M-26-14 to ensure compliance with security and privacy auditing standards. Event logging is ingested into and analyzed by our Security Information and Event Management (SEIM) system using user and entity behavior analytics (UEBA). All user access is controlled by rule-based access control (RBAC). File access is monitored, audited and reviewed continuously by a member of the information system security team.

	For any unauthorized system access or accidental disclosure, we will follow the FMC's incident response and privacy breach procedures.
A user (whether within the FMC or outside) could download infected or malicious files and compromise the security of the SharePoint system.	To address this risk, files downloaded into the SharePoint system are scanned for viruses, and files found to be infected are rejected. The Microsoft Defender anti-virus software receives daily updates to active virus signatures. The FMC recognizes that, despite these precautions, zero-day viruses (defined as a previously unknown virus for which specific anti-virus software signatures are not yet available) remain possible threats.

Section 9. Privacy Act Compliance:

9.1 Is a Privacy System of Records being developed or modified for this System? If so, provide the status or link to the System of Record Notice published in the Federal Register below:

This is a new system of records being housed within an existing system (SharePoint). A system of records notice (SORN) will be published in the Federal Register, and on FMC's privacy program webpage. Also, a Privacy Act 552a(e)(3) notice (i.e., Privacy Act Statement) will be provided at the point of collection, specifically, on the Privacy Act Requests digital access and consent forms. These forms will list the SORN for this Privacy Act Requests System and provide a direct link to the SORN.