FEDERAL MARITIME COMMISSION
PRIVACY IMPACT ASSESSMENT

A. SYSTEM INFORMATION

1. **What is the system name?** FMC Data Base (FMCDB)

2. **Why is the information being collected (e.g., to determine eligibility)?**
The information is being collected to enable the successful performance of FMC duties in regulating various activities of regulated maritime entities.

3. **What is the intended use of the information (e.g., to verify existing data)?**
The data is used to manage internal tasks, upkeep of internal services, permit entity registration, entity record keeping, public listing of registered entities, public listing of agreements, report generation and application user management.

4. **Does this system contain any personal information about individuals? (If no, a PIA is not required. Complete a Privacy Impact Analysis.)**
Yes.

5. **What legal authority authorizes the purchase or development of this system/application? (List the statutory provisions or Executive Orders that authorize the maintenance of this information to meet an official program mission or goal.) Also list the OMB Clearance number and expiration date, if applicable.**
Title 46 USC - Shipping
Agreements and Service Contracts 46 USC 40304, 40306, 41307 (6)-(d)-, 46VSC40502, NSA 46 CFR part 531
OMB # 3072-0045 (Expires 9/30/2013
OMB #3072-0070 (Expires 09/30/2014)
OMB NO. 3072-0018 (Expires 02/28/2014)
OMB No. 3072-0018 (Expires 7/31/2016)
OMB No. 3072-0012 (Expires 10/31/2014)

6. **For new systems, describe how privacy is addressed in documentation related to system development, including as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and especially, the initial risk assessment.**
The FMCDB is not a new system.

B. DATA IN THE SYSTEM

1. **What categories of individuals are covered in the system (for example, employee, contractor, public)?**
The FMCDB covers external individuals such as organization registrants, filers, and general public viewers of published lists.

It also covers internal FMC individuals such as transportation analysts, economists, attorneys, filers, administrators, developers, and contractors.

2. **What are the sources of information in the system?**
External information comes from Organization user registration, form filing, and file upload. Applications such as Form 18 also have a messaging feature to necessitate communications between external users and internal analysts. Internally, the information submitted is used by FMC staff and administrators to record processes and record decisions made regarding FMC regulated entities and tasks.

a. Is the information collected directly from the individual or is it taken from another source? If Information is not collected directly from the individual, describe the source of the information.
Information is collected directly from the individual/organization.

b. What Federal agencies provide data for use in the system?
None

c. What state and local agencies provide data for use in the system?
None.

d. What other third parties will data be collected from?
Filers.

e. What information will be collected from the employee and the public?
Identification such as user account and person name, social security number and date of birth is collected from internal employees to control application authentication and access permissions.

The public provides general information for application accounts such as name and organization. General organization information is necessary to have active Form 1 registration. Form 18 requires an applicant to provide their name and address, business information, qualifying individuals, organization ownership and affiliations, branch offices, and certifications.

The public may also file complaints regarding the performance of FMC regulated entities.

3. **How does the FMC ensure that data are sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations about any individual?**
Externally submitted information is manually reviewed by individual specialized FMC departments.

a. How is data accuracy ensured?
Data accuracy is ensured through manual review by appropriate FMC staff

b. How will data be checked for completeness?
Web applications have fields that must be filled in order to submit. If the submission is from an external source, FMC analysts will manually review the submission to approve or deny. If the submission is internal, FMC stafft and

Application administrators are tasked to ensure that sufficient information is provided.

c. Are the data current? What steps or procedures are taken to ensure the data are not out of date?

Since submitted data are from an outside source, it is up to external users to maintain updated registration using the provided website interfaces.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Since there are many applications present on the FMCDB, there is no single document detailing all the data elements. Data elements are often detailed by the physical FMC Forms that they represent and departmental record keeping needs.

e. How will data collected from sources other than FMC records be verified for accuracy?

Data accuracy is ensured through manual review by FMC staff.

4. Describe what opportunities individuals have to decline to provide information (that is, where providing information is voluntary) or to consent to particular uses of information (other than required or authorized uses), and how individuals can grant consent.

FMC by default does not require or use information for anything other than required or authorized uses as stated on FMC registration forms and documents. Additional information may be provided to FMC at the discretion of the individual.

C. ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes. The data is relevant to the daily performance of FMC.

2. Will the system derive new data or create previously unavailable data about an individual through the aggregation of information collected? (If no, skip to D.3.)

Yes, the new data mainly pertains to an individual's registration status.

a. Will the new data be placed in the individual's record?

Yes, the individual is able to access the record data through the relevant web application where the decision was made.

b. Can the system make determinations about employees or the public that would not be possible without the new data?

No, the management functionalities of FMC rely on the entity status information of the new data.

c. How will the new data be verified for relevance and accuracy?

New data decisions are made with a combination of application requirements as well as manual review by FMC analysts in order to verify relevance and accuracy.

3. **Do the records in this system share the same purpose, routine use, and security requirements?**
While not all records in the system are strongly tied, they are all necessary for FMC tasks. Applications are routinely used by departments to complete their respective tasks and security is controlled by a combination of Form and Network authentication.

a. If the data are being consolidated, what technical, management, and operational controls are in place to protect from unauthorized access or use? Explain.
Security to applications and system controls are controlled by a combination of form and Network.

b. If processes are being consolidated, are the proper technical, management, and operational controls remaining in place to protect the data and prevent unauthorized access? Explain.
Unauthorized access is prevented through the inability for an account to gain permissions unless granted by specialized administrative accounts.

4. **How will the data be retrieved? Can a personal identifier be used to retrieve data? Are personal identifiers used to retrieve data on a routine, occasional, or ad hoc basis? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**
Since the FMCDB consists of many applications, the data for individual applications may be retrieved in a number of ways. The way for authorized users to retrieve data is through web interface but the data is also available via distributed executables and generated report files. Personal identifiers such as email and phone number are used to retrieve data on a routine basis in applications that require external user submission in order to facilitate various communication needs.

5. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
Status reports may be produced on individuals in relation to registered organizations. These reports are used by FMC staff and administrators to review and manage the performance of the registered organizations.

D. MAINTENANCE OF ADMINISTRATIVE CONTROLS

1. **If the system is hosted and/or used at more than one site, how will consistent use of the system and data be maintained at all sites?**
The database portions of applications are hosted on the FMCDB Server. Administrative intranet websites are hosted on the FMCINET Server and regular user extranet websites are hosted on the FMCSMTP Server. Each server has a distinct usage and the data is stored in a single location for consistency.

2. **What are the retention periods of the data in this system?**
Data is retained indefinitely.

3. **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

There is no data disposal procedure. Reports are generated and downloaded as distinct files by system users and are kept at their individual discretion.

4. **Is the system using technologies in ways that the FMC has not previously employed (for example, monitoring software, CallerID)? If yes, how does the use of this technology affect public/employee privacy?**
No.

5. **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**
Yes, the system stores general account information and submitted entity registration information such as organization ownership and certifications.

a. What kinds of information are collected as a function of the monitoring of individuals?
The system tracks general system usage such as form submissions and communications with FMC.

b. What controls will be used to prevent unauthorized monitoring?
The monitoring detailed in 5.a. is based on general application usage for individual accounts.

6. **Under which Privacy Act systems of records notice does the system operate? Provide name and number.**
FMC SQL Database (FMCDB) - FMC 41

7. **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**
No. The system is not being modified at this time. If there is a significant modification to the system the Privacy Act system of records notice will be amended or revised.

E. ACCESS TO DATA

1. **Who will have access to the data in the system (for example, contractors, users, managers, system administrators, developers, other)?**
External users will have access to their own submitted data along with available organization and agreement data.

Applications have individual controls for user access but permissions are granted on an individual basis. Application staff will be able to see their assigned cases while administrators will be able to view most information.

System administrators and select contractors are able to directly access the FMCDB hosting environment for maintenance and development tasks.

2. **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access by external users is granted via review by application analysts. Access by internal users is granted per individual based on documented job responsibilities pertaining to system applications.

3. **Will users have access to all data on the system or will the user's access be restricted? Explain.**
Permission to data is granted on a per application basis and will be restricted based on the user's role.

4. **What controls are in place to prevent the misuse (for example, unauthorized browsing) of data by those having access? List procedures and training materials.**

Formal policies and procedures have been documented and published to guide all personnel in managing logical access and security to systems and data. FMC IT management is responsible for the development, approval, communication, and monitoring of these policies and procedures.
FMC IT management provides overall direction, guidance, and governance for system information security and is responsible for the implementation, adherence to, and monitoring of information security policies and procedures.
FMC has also documented the policy and procedures guidance for FMC NETWORK environment that is followed for implementing the access controls (see OIT-P14 and OIT-P04).

5. **Are contractors involved with the design and development of the system and/or will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**
Yes, contractors are currently involved in maintenance, design, and development of the system.

Yes. FAR 52.224-1, and FAR 52.224-2 are both in the GSA contract.

6. **Do other systems share data or have access to the data in the system? If yes, explain.**
No

7. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**
N/A

8. **Will other agencies share or have access to the data in this system? If yes, list agencies.**
DOD, USDA, DHS

9. **How will the data be used by the other agency?**
To support their statutory authority.

10. **Who is responsible for ensuring proper use of the data?**
The Office of the Managing Director, Federal Maritime Commission.

APPENDIX II

FEDERAL MARITIME COMMISSION
PRIVACY IMPACT ANALYSIS

SYSTEM OF RECORDS IDENTIFICATION

1. **Is a system of records being created under the Privacy Act, 5 U.S.C. 552a? If no, skip questions 2 through 4.**
   Yes

2. **Have privacy and IT risk assessments been conducted that consider the alternatives to collection and handling as designed and the appropriate measures to mitigate risks identified for each alternative?**
   Yes

3. **What impact will this system have on an individual's privacy? (Consider the consequences of collection and flow of information and identify and evaluate threats to individual privacy.)**
   The system's impact on an individual's privacy is minimal because it is only accessible by authorized FMC personnel on a need to know basis.

4. **As a result of the PIA, what choices have been made regarding the IT system of collection of information? Have adequate measures been designed and implemented to mitigate risk? What is the rationale for the final design choice or business process?**
   None. Yes. As required by the Federal Information Security Management Act 2002. The FMCDB system undergoes a certification and accreditation every three years. The FMCDB system also undergoes an annual Inspector General audit.

APPENDIX III

FEDERAL MARITIME COMMISSION
SYSTEM DEVELOPMENT LIFE CYCLE
PRIVACY REQUIREMENTS WORKSHEET

A. CONTACT INFORMATION

1. Person who completed the Privacy Impact Assessment document

Name: Gregory Francis
Title: Information Systems Security Officer
Bureau/Office: Office of Information Technology
Phone number: 202 523 1930

2. System Owner

Name: Anthony Haywood
Title: Chief Information Officer
Phone number: 202 523 0001

3. Business Owner

Name: James Nussbaumer
Title: Deputy Director, Bureau of Licensing and Certification
Phone number: 202 523 5816

Name: Sandra Kusumoto
Title: Director Bureau of Trade Analysis
Phone number:202 523 5796

4. Chief Information Officer

Name: Anthony Haywood
Title: Chief Information Officer
Phone number: 202 523 0001

5. Senior Agency Official for Privacy

Name: Austin Schmitt
Title: Director, Strategic Planning and Regulatory Review
Phone number: 202 523 5800

B. PRIVACY IMPACT ASSESSMENT SUMMARY

	System Category **(Check all categories that apply)**	**Requirement**
X	System of Records	Publish System of Records Notice
	Website available to the public	Publish Privacy Impact Assessment

	Website or information system operated by a contractor on behalf of the FMC for the purpose of interacting with the public	Publish Privacy Impact Assessment
X	New or significantly altered information technology investment administering information in an identifiable form collected from or about members of the public	Conduct Privacy Impact Assessment
	New or significantly altered information technology investment administering information in an identifiable form collected from or about FMC employees	Conduct Privacy Impact Assessment
	Contains medical information	Determine if system is subject to HIPAA
	Other	
	None of the above	Privacy Impact Assessment not required

C. PRIVACY IMPACT ASSESSMENT APPROVAL

Approval of Privacy Impact Assessment accuracy and completeness.

System Owner: ______________________________ ______________________

Signature Date

Business Owner: ______________________________ ______________________

Signature Date

Approval of IT System Risk Assessment

Chief Information Officer: ______________________________ ______________________

Signature Date

Approval of Privacy Assessment and Resulting System Categorization

Senior Agency Official for Privacy: ______________________________ ______________________

Signature Date