FEDERAL MARITIME COMMISSION
PRIVACY IMPACT ASSESSMENT

A. SYSTEM INFORMATION

1. What is the system name? FMC General Support System (FMCGSS)

2. Why is the information being collected (e.g., to determine eligibility)?
The FMCGSS is a communications system. The FMCGSS does not actively collect information; it is used by FMC staff and contractors in the course of conducting official FMC business to store and communicate information that they receive from, or generate for inclusion in, other systems that constitute systems of record.

3. What is the intended use of the information (e.g., to verify existing data)?
There is the potential for PII to reside within the FMCGSS, as the result of being typed into the text of an email message or attached to an email message sent or received by a FMC staff or contractor, or by being downloaded from another system and saved by that system's user to the FMCGSS. Examples of records containing PII that could be stored or transmitted using the FMCGSS include travel, payroll, time and attendance, and other agency personnel records containing PII pertaining to employees and contractors; agency program records containing PII pertaining to members of the public; and employees and contractors personal records (non-agency records).

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 (46 U.S.C. app. sections 1701–1720); section 19 of the Merchant Marine Act, 1920 (46 U.S.C. app. section 876); the Foreign Shipping Practices Act of 1988 (46 U.S.C. app. section 1710a); and other applicable statutes.

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 FMCGSS 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 FMCGSS covers external individuals such as organization, registrants and filers. FMCGSS also covers internal FMC individuals such as staff, transportation analysts, economists, attorneys, filers, administrators, developers, and contractors.

2. What are the sources of information in the system?

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.
The FMCGSS is a communications system. The FMCGSS does not actively collect information; it is used by FMC staff and contractors in the course of conducting official FMC business to store and communicate information that they receive from, or generate for inclusion in, other systems that constitute systems of record.

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?
None.

e. What information will be collected from the employee and the public?
Identification such as user account and person name is collected from internal employees to control application authentication and access permissions.
None

3. How does the FMC ensure that data are sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations about any individual?

a. How is data accuracy ensured?
Data accuracy is ensured through manual review by OIT staff and individual specialized FMC departments.

b. How will data be checked for completeness?
If the submission is internal, Department 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?
Yes. Periodic review by FMC staff.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?
Yes. The FMCGSS houses multiple “Minor” systems through office automation documents such as word processing documents and spreadsheets. The Data elements are described in detail and documented for each of these “Minor” systems in their corresponding SORNs that are available on the FMC website. The “Minor” systems are listed below:

1. FMC – 7 (Licensed Ocean Transportation Intermediaries Files – paper and electronic system)
2. FMC – 8 (Official Personnel Folder – electronic system)
3. FMC – 9 (Training Program Records – electronic system)
4. FMC – 14 (Medical Examination File – electronic system)
5. FMC – 16 (Classification Appeals File – electronic system)
6. FMC – 19 (Financial Disclosure Reports and Other Ethics Program Records – electronic system)
7. FMC – 22 (Records Tracking System – paper and electronic system)
8. FMC – 25 (Inspector General File – electronic system)
9. FMC – 28 (Equal Employment Opportunity Complaints Files – electronic system)
10. FMC – 29 (Employee Performance File System Records – electronic system)
11. FMC – 31 (Debt Collection Files – paper and electronic system)
12. FMC – 34 (Travel Charge Card Program – electronic system)
13. FMC – 35 (Transit Benefits File – electronic system)
14. FMC – 36 (SmartPay Purchase Charge Card Program – electronic system)

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

FMCGSS does not collect data.

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.

N/A

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.

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.)

No.

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

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

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

3. Do the records in this system share the same purpose, routine use, and security requirements?

Yes.

a. If the data are being consolidated, what technical, management, and operational controls are in place to protect from unauthorized access or use? Explain.

Critical components of the FMCGSS are accessed by the system administration group which manages user IDs and passwords, security settings, and patching/upgrades. Each FMC employee and contractor is allowed access to his or her LAN account only. Physical access to the system is restricted through security guards and access badges required to enter the FMC facility. All FMC employees and contractors are subject to the Information Systems Rules of Behavior and receive annual security awareness training. The FMCGSS is secured by a combination of firewalls, anti-virus controls, intrusion detection and prevention systems, network controls, access lists and account creation, policing and termination processes.

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.

Critical components of the FMCGSS are accessed by the system administration group which manages user IDs and passwords, security settings, and patching/upgrades. Each FMC employee and contractor is allowed access to his or her LAN account only. Physical access to the system is restricted through security guards and access badges required to enter the FMC facility. All FMC employees and contractors are subject to the Information Systems Rules of Behavior and receive annual security awareness training. The FMCGSS is secured by a combination of firewalls, anti-virus controls, intrusion detection and prevention systems, network controls, access lists and account creation, policing and termination processes.

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.

N/A

5. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

There are no reports produced on individuals.

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?

N/A

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 currently no permanent disposition of data.

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.
No.

a. What kinds of information are collected as a function of the monitoring of individuals?
N/A

b. What controls will be used to prevent unauthorized monitoring?
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).

6. Under which Privacy Act systems of records notice does the system operate? Provide name and number.
FMC-39 FMC General Support System (FMCGSS)

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)?
System administrators, FMC Staff, and select contractors are able to directly access the FMCGSS system.

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

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).

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 an individual basis and is 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.**
No.

9. **How will the data be used by the other agency?**
N/A.

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 FMCGSS system undergoes a certification and accreditation every three years. The FMCGSS 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. Chief Information Officer

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

4. 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

Approval of IT System Risk Assessment

Chief Information Officer: _____ _____
Signature Date

Approval of Privacy Assessment and Resulting System Category

Senior Agency Official for Privacy: _____ _____
Signature Date