

**FEDERAL MARITIME COMMISSION
PRIVACY IMPACT ASSESSMENT**

A. SYSTEM INFORMATION

1. What is the system name?

FMC SERVCON

2. Why is the information being collected (e.g., to determine eligibility)?

The information is being collected pursuant to title 46 USC Shipping §40502 Service Contracts (b)(1) – which states “Each service contract entered into under this section by an individual ocean common carrier or an agreement shall be filed confidentially with the Federal Maritime Commission.”

3. What is the intended use of the information (e.g., to verify existing data)?

To record, review, and manage contractual arrangements by organizations performing services as registered VOCCs and NVOCCs in order to ensure legal operating requirements are met.

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.

Service Contracts 46 USC 40502, NSA 46 CFR part 531

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.

FMC SERVCON 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 system users include external registered filing representatives of VOCC and NVOCC Organizations as well as internal FMC staff.

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

The sole data source are filed contracts and notices from registered VOCC and NVOCC Organizations and their representatives.

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 information is collected directly from representatives or automated filing systems via the ServconWebService.

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?

Information as needed to carry out 46 CFR parts 530 & 531.

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

The FMC SERVCON System has initial checks upon contract filing to ensure requirements for data formatting and contract meta data are acceptable by checking filing information and providing warnings or errors to filers. If there are filer errors, FMC may be contacted to perform a manual review and correction.

a. How is data accuracy ensured?

Data accuracy is ensured at contract filing by checking new filing data against existing contract history records.

b. How will data be checked for completeness?

The contract filing functionality will not officially accept contract records if all required metadata is not present during filing.

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 What steps or procedures are taken to ensure the data are not out of date?

The data is current and any change to a contract record is filed via amendment to keep a record history.

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

Data elements contained in 46 CFR 530.8-Essential terms of service contracts and the SERVCON user manual.

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

FMC SERVCON records all come from VOCC and NVOCC organizations. There are required data checks in place for initial contract filings and amendment filings that will accept or reject input depending on success.

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.

A requisite of being a VOCC or NVOCC Organization is consenting that all contracts must be filed with FMC in order to be carried out. The FMC SERVCON system has been set up for the Organizations to meet this requirement.

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.

External filers for VOCCs must complete Form FMC-83 and filers for NVOCCs must complete Form FMC-78. Once submitted to FMC, internal Analysts will review the information and request application account creation.

External users are provided with account and password in order to access the SERVCON website that limits functionality to contract filing and individual filing history. Internal users have network credentials in order to access the FMC SERVCON intranet with administrative functionality to view all uploaded files.

The SRVCONDB Server where FMC SERVCON data resides is managed by OIT and only select technical internal users have credentials for access.

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.

Yes, the FMC SERVCON System registration requires Form FMC-83 and FMC-78 and authentication is built to use the application authentication detailed in 3.a.

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.**

Users may retrieve data via the website interface. Filers may view their own filed records while FMC staff may retrieve all filed records. Notable identifiers for contract data are username and organization identification number. Organization number is routinely used as an identifier to retrieve data. Contracts can also be searched by keywords such as the names of signatories to a contract.

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?**

The majority of FMC SERVCON applications are hosted on the SRVCONDB Server. The administrative FMC SERVCON application is hosted on both the SRVCONDB and FMCINET Server. Since this portion does not manipulate data, no inconsistencies are created due to different hosting environments.

2. **What are the retention periods of the data in this system?**

Currently, 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 and reports. Basic contract and NSA filing counts are available on the public Servcon website (<https://servcon.fmc.gov/stat/>) with previous statistics backed up in the same directory.

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, the FMC SERVCON System employs standard usage of application and database functionality for contract filing.

5. **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

This system is able to identify individuals through information provided at user account creation. Persons signing service contracts are also identified.

- a. **What kinds of information are collected as a function of the monitoring of individuals?**

Contract filing activity may be tracked through successful and unsuccessful contract filing records.

- 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.

SERVCON FMC-40

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 filers will have access to their own filed contracts. FMC SERVCON staff may view all file contract data through the administrative website interface. System administrators, developers, and contractors are able to access the hosting server.

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

External filers will have access to their own filed contracts and access is documented in the initial registration forms. FMC SERVCON staff requires access to filed contract data to perform FMC regulated work tasks. Developers and Contractors are granted access if their work contract specifically requires access to the system.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

The FMC SERVCON System is separated into two websites for contract filers and administration. The contract filing website search functionality is limited to the records of the filer while the administrative website search functionality may search all records.

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.

External users can only access their own filings.

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.
- 9. How will the data be used by the other agency?**
The data will be used to assess reasonable rate levels..
- 10. Who is responsible for ensuring proper use of the data?**
The Office of the Managing Director, Federal Maritime Commission.

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.**
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.

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.)**

Names of signatories as well as filers of specific service contracts will be identifiable. The threat to individual privacy is Because SERVCON is as minimal as possible because SERVCON is confidential and accessible only by authorized 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 SERVCON system undergoes a certification and accreditation every three years. The SERVCON system also undergoes an annual Inspector General audit.

**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: 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
X	Website available to the public	Publish Privacy Impact Assessment
X	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

	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