6730-01-P

This document is scheduled to be published in the Federal Register on 09/11/2013 and available online at **http://federalregister.gov/a/2013-22071**, and on **FDsys.gov**

FEDERAL MARITIME COMMISSION

Privacy Act of 1974; Proposed New Systems of Records

AGENCY: Federal Maritime Commission.

ACTION: Notice of proposed new systems of records.

SUMMARY: This notice is necessary to meet the requirements of the Privacy Act of 1974 to publish in the *Federal Register* notice of the existence and character of record systems maintained by the Federal Maritime Commission.

DATES: *Effective Date:* These systems will be adopted without further notice on **[INSERT DAETE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** unless modified to respond to comments received from the public and published in a subsequent notice.

Comment Date: Comments must be received in writing on or before **[INSERT DAETE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments:

by Postal Mail/Commercial Delivery or via email to:

Karen V. Gregory, Secretary
Federal Maritime Commission
800 N. Capitol Street, N.W.
Washington, D.C. 20573-0001
Secretary@fmc.gov
Email comments to: Secretary@FMC.gov (email Comments as an attachment in MS Word or PDF). Include in the Subject Line: “Comments on Systems of Records Notice”

FOR FURTHER INFORMATION CONTACT:

Karen V. Gregory, Secretary
Federal Maritime Commission
800 N. Capitol Street, N.W.
Washington, D.C. 20573-0001
(202) 523-5725
Secretary@fmc.gov

SUPPLEMENTARY INFORMATION:

The Commission proposes to adopt the following additional Systems of Records (SOR). Interested parties may participate by filing with the Secretary, Federal Maritime Commission their views and comments pertaining to this Notice. All suggestions for changes in the text should be accompanied by draft language necessary to accomplish the desired changes and should be accompanied by supportive statements and arguments. Comments must be submitted in the prescribed time or the proposed SOR will become effective as scheduled.

Notice is hereby given, that pursuant to the Privacy Act of 1974, 5 U.S.C 552a, the Commission proposes to establish the following new Systems of Records. The five (5) new systems are proposed to read as follows:

FMC- 37

System name:

Personal Identity Verification Management System (USAccess Credentials).

System location:

Records covered by this system are maintained by a contractor at the contractor's site.

This system is covered by the Office of Personnel Management's government-wide system notice, GSA/GOVT-7.

FMC–38

System name:

Parking Operation Plan-FMC.

Security Classification:

Unclassified.

System location:

Office of Management Services, Federal Maritime Commission, 800 North Capitol Street, N.W., Washington, DC 20573-0001.

Categories of individuals covered by the system:

This system maintains information on FMC headquarters' employees who are holders of FMC-issued parking permits.

Categories of records in the system:

Records in this system may include information about individuals, including name, home address, home telephone number, work telephone number, personal vehicle make and model, personal vehicle license number, and state of vehicle registration. These records are captured on applications for parking permits.

Authority for maintenance of the system:

40 U.S.C. Section 486(c); 41 C.F.R. Section 101-20.0 and 41 C.F.R. Section 102-74.305 and the Occupancy Agreement with the General Services Administration (GSA).

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

The records in this system of records are used or may be used:

1. By Commission officials to determine the assignment of parking permits to eligible employees.
2. To conduct a quarterly parking revalidation to verify continued employee eligibility for parking permits.
3. To appropriate agencies, entities, and persons when (a) the Federal Maritime Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the agency or another agency or entity) that rely upon the

compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the agency's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are maintained in file folders.

Retrievability:

Records are indexed alphabetically by name.

Safeguards:

Records are maintained in locked file cabinets.

Retention and disposal:

Records are maintained and disposed of in accordance with General Records Schedule 11, Items 2a and 4a (records destroyed 2 years after termination of parking assignment).

System manager(s) and address:

Director of Management Services, Federal Maritime Commission, 800 North Capitol Street, N.W., Washington, DC 20573-0001.

Notification procedure:

All inquiries regarding this system of records should be addressed to: Director, Office of Management Services, Federal Maritime Commission, 800 North Capitol Street, N.W., Washington, DC 20573-0001.

Record access procedures:

Requests for access to a record should be directed to the Secretary listed at the above address. Requests may be in person or by mail and shall meet the requirements set out in section 503.65 of title 46 of the Code of Federal Regulations.

Contesting record procedures:

An individual desiring to amend a record shall direct such a request to the Secretary at the above listed address. Such requests shall specify the desired amendments and the reasons therefor, and shall meet the requirements of section 503.66 of title 46 of the Code of Federal Regulations.

Record source categories:

Applicants or FMC employees who are holders of FMC-issued parking permits.

FMC-39

System name:

FMC General Support System (FMC GSS)

Security Classification:

Unclassified.

System location:

Office of Information Technology, Federal Maritime Commission, 800 N. Capitol Street, N.W., Washington, D.C. 20573-0001

Categories of individuals covered by the system:

1. Authorized Employees of the Federal Maritime Commission.
2. Authorized Users from other Federal Agencies (DOTS, Military) authenticated via local accounts.
3. All persons/ Entities regulated by the FMC.
4. Companies and individuals that have become subject of an investigative or enforcement action.
5. Entities who have requested alternative dispute resolution services.

Categories of records in the system:

The FMC GSS contains Employee, Filer, Licensee, and Complainant information such as first name, last name, e-mail address, user ID, organization number, social security number

(Form-18), carrier name, contract number, amendment number, date filed, effective date, and confirmation number.

Authority for maintenance of the system:

E-Government Act of 2002 (Title III) and OMB Circular A-130.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

The FMC Network is a general support system (GSS) that provides core and critical information technology support to a number of hosted applications and databases.
The FMC GSS is designed to facilitate the services and resources needed to support FMC operations and FMC's end user community. The purpose of the FMC GSS is to provide FMC employees and/or contractors access to the FMC domain, E-mail account management, individual and shared electronic storage, interconnection(s) between all FMC end users and the Internet, as well as provide access to agency applications.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are maintained electronically. The FMC GSS system is managed and maintained by FMC OIT staff at its Washington, DC headquarters. The FMC GSS is made up of servers, switches, gateways, and two firewall devices. The servers, switches, gateways, and firewall devices are physically housed in the Data Center at FMC Headquarters. The Data Center is monitored 24 hours a day 7 days a week

Retrievability:

Data is retrievable by: first name, last name, user ID, telephone number, social security number (Form-18), company name, carrier name, contract number, amendment number, date filed, effective date, confirmation number, etc.

Safeguards:

Currently each user of the FMC GSS must have a unique profile in the Active Directory (AD). When a login is attempted, the entered user ID and encrypted password are verified against the AD. If the user login credentials are not validated, the login attempt fails.

Access to each layer of the network is controlled and monitored by personnel through formal defined authorization, approval, and monitoring processes. Authentication at the network layer incorporates a number of additional security layers, including firewalls, routers, and VPNs. Access to the network, operating system, and database is restricted and granted only to specific pre-approved individuals by the system owner.

User profiles define individual FMC GSS users linked to one or more roles. Permission lists are added to each role, which controls a user's access level.

Each user of the information system has a unique profile and login attempts are verified and validated against a user access list. The system authenticates users with the values specified in the User ID and Password field. All unverifiable login attempts are denied access to the system.

FMC is in the process of implementing Homeland Security Presidential Directive 12 (HSPD-12). This implementation is expected to be completed by the 2nd Quarter FY 2014.

HSPD-12 requires the use of two-factor authentication for access to government computer systems. To achieve two-factor authentication individuals require a Personal Identity Verification (PIV) card and a Personal Identification Number (PIN). Upon HSPD-12 implementation, FMC GSS will be accessed by individuals utilizing a PIV and PIN.

Retention and disposal:

Agency data is backed up and retained for five years at which point the backup tapes are overwritten.

System manager(s) and address:

Anthony Haywood, CIO Federal Maritime Commission, 800 North Capitol Street, N.W., Washington, DC 20573-0001.

Notification procedure:

All inquiries regarding this system of records should be addressed to: Anthony Haywood, CIO 800 North Capitol Street, N.W., Washington, DC 20573-0001.

Record access procedures:

All personnel and contractors sign non-disclosure agreements prior to accessing the information system following the performance of background investigations that commensurate with the sensitivity of the information and the risk to the FMC GSS. FMC is responsible for determining the position sensitivity levels (or risk levels) for all personnel whose jobs require access to mission critical information. This responsibility includes ensuring that all personnel and contractors have undergone the appropriate background suitability checks and security awareness training. User access is granted based on the principle of least privilege. In accordance with this principle, users are granted only the amount of system access they require to perform their duties. Upon termination or reassignment individuals are re-screened immediately.

Contesting record procedures:

N/A

Record source categories:

Office of Personnel Management report, and reports from other Federal agencies.

FMC-40

System name:

SERVCON

Security Classification:

Unclassified.

System location:

Office of Information Technology, Federal Maritime Commission, 800 N. Capitol Street,

N.W., Washington, D.C. 20573-0001

Categories of individuals covered by the system:

1. Authorized employees of the Federal Maritime Commission.
2. Authorized users from other Federal Agencies (DOTS, military) authenticated via local accounts.
3. Authorized VOCC and NVOCC Users.

Categories of records in the system:

1. Successful Contract Filings, Contract Corrections, and Notices records and file data.
2. Unsuccessful Contract Filings and Contract Corrections records.
3. Contract Filing Statistics.
4. Users' file viewing history.

Authority for maintenance of the system:

E-Government Act of 2002 (Title III) and OMB Circular A-130.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

The SERVCON records are used or may be used:

1. By Authorized Organization Representatives for official filing of VOCC and NVOCC related contracts to FMC.
2. By Authorized Organization Representatives to make approved changes and amendments to filed contracts.
3. By Authorized Organization Representatives to upload Notices with various information relevant to filed contracts that may be viewed by Commission Officials.
4. By Commission Officials and Authorized Local Users from other Federal Agencies to verify and review the validity of the contract and operations of registered VOCCs and NVOCCs.
5. To refer, where there is an indication of a violation or potential violation of law,

whether civil or criminal or regulatory in nature, information to the appropriate agency, whether Federal, State, or local, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation or order issued pursuant thereto.

6. By a court of law or appropriate administrative board or hearing having review or oversight authority.
7. To appropriate agencies, entities, and persons when (a) the Federal Maritime Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the agency or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the agency's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Electronic records are maintained within the confines of FMC-39, FMC General Support System (FMC GSS) and FMC-41, FMC SQL Database (FMCDB).

Retrievability:

Data is retrievable by: user ID, organization number, carrier name, contract number, amendment number, date filed, effective date, confirmation number, filer user name, file name file size, file type.

Safeguards:

Electronic records are secured in accordance with FMC-39, FMC General Support System (FMC GSS) for internal users.

External users' must authenticate against the Passport user database records and are only able to search for files, which the account has uploaded.

Retention and disposal:

Specific uploaded files are individually removed from the live data tables and placed in a file data removed data table upon disposal request from the filing organizations.

All data records are currently being kept indefinitely.

System manager(s) and address:

Anthony Haywood, CIO Federal Maritime Commission, 800 North Capitol Street, N.W., Washington, DC 20573-0001.

Notification procedure:

All inquiries regarding this system of records should be addressed to: Gary Kardian 800 North Capitol Street, N.W., Washington, DC 20573-0001.

Record access procedures:

Individuals may receive an external user account by filing form FMC-83 for VOCCs or form FMC-78 for NVOCCs to: Federal Maritime Commission, Bureau of Trade Analysis, 800 North Capitol Street, N.W., Washington, DC 20573-0001

FMC employees and employees from other Federal Agencies will be given individual review and may gain access if it is within the scope of their responsibilities.

All other inquiries regarding this system of records should be addressed to: Gary Kardian, 800 North Capitol Street, N.W., Washington, DC 20573-0001.

Contesting record procedures:

The SERVCON system allows external filers to file a Corrected Transmission to edit contract files within two days of the effective date.

Record contests beyond that point in tie should be addressed to: Gary Kardian, 800 North Capitol Street, N.W., Washington, DC 20573-0001.

Record source categories:

Contract files submitted by authorized Organization representative filers

FMC-41

System name:

FMC SQL Database (FMCDB)

Security Classification:

Unclassified.

System location:

Office of Information Technology, Federal Maritime Commission, 800 N. Capitol Street, N.W., Washington, D.C. 20573-0001

Categories of individuals covered by the system:

1. Authorized employees of the Federal Maritime Commission.
2. Authorized persons from other Federal agencies (DOTS, military) authenticated via local accounts.
3. External Persons registered via form or web submission authorized by FMC analysts for web application access.

Categories of records in the system:

1. User database for the Form 1, Form 18, and SERVCON web applications.
2. Identification, configuration, and activity records for management of FMC office needs such as BlackBerry usage.
3. User mail and web submitted information and documents for the purpose of registration, review, and reporting of FMC regulated entities such as freight forwarders, vessel-operating common carriers, etc.

4. User mail and web submitted statements and documents regarding FMC regulated entities and analyst response/actions performed in regards to the information.
5. Private internal database tracking analyst statements and rulings regarding persons and organizations derived from user mail and web submitted information.
6. Public external database on the active status of certain FMC registered and managed entities.

Authority for maintenance of the system: E-Government Act of 2002 (Title III) and OMB Circular A-130.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

The FMCDB major application is the Federal Maritime Commission's SQL Database that is the main data store that facilitates the functionality of various FMC minor applications.The routine uses of records include:

1. By maintenance of application user registration, identification, access permissions, and authentication.
2. BlackBerry user identification and activity.

   Provision of file repository functionality for digitized documents used by the FMC Office of the Secretary.
3. Registration, review, and status recording for FMC managed entities such as freight forwarders, vessel-operating common carriers, etc.
4. Display of publically available information such as approved organization registrations and agreements.
5. Reviewing user submitted concerns and complaints regarding FMC managed entities to officially address.
6. Record keeping of FMC internal audits and investigations.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of

records in the system:

Storage:

Electronic records are maintained within the confines of FMC-39, FMC General Support System (FMC GSS).

Retrievability:

Data Retrievability is application dependent. Records for applications involving external user access or organizational records are retrievable in end user applications by the following categories: first name, last name, user ID, telephone number, social security number (Form-18), company name, carrier name, contract number, amendment number, date filed, effective date, confirmation number, etc.

Data may also be retrievable by: Case Number, Case Name, File Name, Active Status, Country, State, Various User Activities, etc.

Safeguards:

Electronic records are secured in accordance with FMC-39, FMC General Support System (FMC GSS) for internal users.

External users' accounts must authenticate against the Passport user database records and are only able to search files, which the account has uploaded.

Retention and disposal:

Agency data is backed up and retained for five years at which point the backup tapes are overwritten.

System manager(s) and address:

Anthony Haywood, CIO - Federal Maritime Commission, 800 North Capitol Street, N.W., Washington, DC 20573-0001.

Notification procedure:

All inquiries regarding this system of records should be addressed to: Anthony Haywood, CIO, 800 North Capitol Street, N.W., Washington, DC 20573-0001.

Record access procedures:

All personnel and contractors sign non-disclosure agreements prior to accessing the information system following the performance of background investigations that commensurate with the sensitivity of the information and the risk to the FMCDB. FMC is responsible for determining the position sensitivity levels (or risk levels) for all personnel whose jobs require access to mission critical information. This responsibility includes ensuring that all personnel and contractors have undergone the appropriate background suitability checks and security awareness training. User access is granted based on the principle of least privilege. In accordance with this principle, users are granted only the amount of system access they require to perform their duties. Upon termination or reassignment individuals are re-screened immediately.

External users may attain access to various external facing applications by submitting a mail or web registration form. Access will be granted upon review by authorized Commission officials.

Contesting record procedures:

External user applications enable users to submit edits to a person or organization registration for review.

Further inquiries may be directed towards individual departments responsible for record analysis.

Record source categories:

1. User submitted person and organization registration information and documentation.
2. Analyst reviews and rulings on appropriated tasks.
3. Automated record keeping from user devices.

By the Commission.

Karen V. Gregory,

Secretary.

[FR Doc. 2013-22071

Filed 09/10/2013 at 8:45

am; Publication Date:

09/11/2013]