Office of Inspector General

Evaluation of the FMC's
FY 2012 Privacy and Data Protection

A13-02

December 2012

FEDERAL MARITIME COMMISSION

FEDERAL MARITIME COMMISSION
800 North Capitol Street, N.W.
Washington, DC 20573

December 6, 2012

Office of Inspector General

TO: Chairman Richard A. Lidinsky
Commissioner Joseph E. Brennan
Commissioner Mario Cordero
Commissioner Rebecca F. Dye
Commissioner Michael A. Khouri

FROM: /Adam R. Trzeciak/
Inspector General

SUBJECT: OIG Report on Privacy and Data Protection

The Office of Inspector General (OIG) performed a review of privacy and data protection policies and procedures to determine if the Federal Maritime Commission (FMC) is complying with Section 522 of the Consolidated Appropriations Act, 2005, (42 U.S.C.A. § 2000ee-2).

Section 522 requires an independent third-party review of agency use of personally identifiable information (PII) and of its privacy and data protection policies and procedures at least every two years. PII is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. This evaluation satisfies the required third-party review.

The agency has improved its privacy program since our last review in 2010. For example, it closed two of four deficiencies and has created policies and procedures to log, verify and reassess data extracts from databases holding sensitive information for longer than 90 days. Also, the agency removed the FMC-18 Privacy Impact Assessment (PIA) from its website because FMC-18 is a component of another system, FMC Database, and did not require a PIA.

We also identified areas where controls in select areas can be improved. The FMC's Senior Agency Official for Privacy, the Privacy Act Officer, the Chief Information Officer and senior managers have responsibility for agency systems and compliance with Federal laws, regulations, and policies relating to information privacy. Although there is interaction and communication between these individuals, communication and coordination on information privacy, including review of systems and determinations for

PIAs, could be improved. Many subsidiary systems have not had an analysis performed to identify if a PIA is required for completion. We also identified concerns with System of Records Notices (SORNs) postings and "routine uses" for systems. Three existing PIAs are outdated and the agency has not informed the public about some systems containing PII.

Apart from this mandated review of Privacy Act compliance, the OIG also opened a nonpublic investigation into privacy matters involving the use of computer monitoring software at the FMC between June 2011 and December 2011.

The OIG met with management who concurs with our findings and recommendations. Management comments are attached to this report.

The OIG wishes to thank the Privacy Act Officer, the Senior Agency Official for Privacy and the Chief Information Officer for their assistance. I am available at your convenience to discuss the report's findings and recommendations.

cc: Ronald Murphy, Managing Director
Karen Gregory, Privacy Act Officer
Austin Schmitt, Senior Agency Official for Privacy
Anthony Haywood, Chief Information Officer

FEDERAL MARITIME COMMISSION

OFFICE OF INSPECTOR GENERAL

Evaluation of the FMC's FY 2012 Privacy and Data Protection

TABLE OF CONTENTS

BACKROUND

Your Internal Controls (contractor), on behalf of the Federal Maritime Commission (FMC), Office of Inspector General (OIG), conducted an independent evaluation of the quality of the FMC privacy program and its compliance with applicable federal computer security laws and regulations.

The Privacy Act of 1974 regulates the use of personal information by the United States Government. Specifically it establishes rules that determine what information may be collected and how information can be used in order to protect the personal privacy of U.S. citizens.

The Privacy Act applies to *Federal Government Agencies* and governs their use of a system of records, which is defined as "any group of records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

The following rules govern the use of a system of records:

- No Federal Government record keeping system may be kept secret.
- No agency may disclose personal information to third parties without the consent of the individual (with some exceptions).
- No agency may maintain files on how a citizen exercises their First Amendment rights.
- Federal personal information files are limited only to data that is relevant and necessary.
- Personal information may be able to be used for the purposes it was originally collected unless consent is received from the individual.
- Citizens must receive notice of any third party disclosures including with whom the information is shared, the type of information disclosed and the reasons for its disclosure.
- Citizens must have access to the files maintained about them by the Federal Government.
- Citizens must have the opportunity to correct or amend any inaccuracies or incompleteness in their files.

EXECUTIVE SUMMARY

The OIG performed a Privacy and Data Protection review in accordance with privacy and data protection related laws and guidance (e.g. Privacy Act of 1974, OMB memorandums, Consolidated Appropriations Act of 2005 etc.). The Consolidated Appropriations Act of 2005 requires agencies to assign a Chief Privacy Officer (CPO) who is responsible for identifying and safeguarding personally identifiable information (PII) and requires an independent third-party review of agency use of PII and of its privacy and data protection policies and procedures at least every two years.

The agency has improved its privacy program since our last review in 2010. For example, it closed two of four deficiencies and has created policies and procedures to log, verify, and reassess data extracts from databases holding sensitive information after 90 days. Also, the agency removed the FMC-18 Privacy Impact Assessment (PIA) from its website because FMC-18 is a component of another system (FMCDB) and did not require a PIA. We also identified

areas where controls in select areas can be improved. These issues are discussed in this report as noted below.

OBJECTIVES AND SCOPE

The objective was to perform a privacy and data protection review. The contractor performed the following:

- Conducted a review of the FMC's privacy and data security policies, procedures and practices in accordance with regulations.
- Reviewed the agency's technology, practices and procedures with regard to the collection, use, sharing, disclosure, transfer and storage of information in identifiable form.
- Reviewed the agency's stated privacy and data protection procedures with regard to the collection, use, sharing, disclosure, transfer, and security of personal information in identifiable form relating to agency employees and the public.
- Performed a detailed analysis of the agency's intranet, network, and website for privacy vulnerabilities (through vulnerability scans and review of source documents):
    - Assessed compliance with stated practices, procedures, and policy.
    - Assessed the risk of inadvertent release of information in an identifiable form from the website of the agency.
- Issued recommendations for improvements or enhancements to management of information in identifiable form, and the privacy and data protection procedures of the agency.
- Assessed the agency's progress toward implementing corrective actions in prior audit reports.

CURRENT YEAR FINDINGS

The agency has taken steps to enhance Privacy Act compliance efforts. All employees are required to undergo annual privacy training to include safeguarding PII. The agency also developed and implemented a number of formal policies and/or guidelines. For example, in June of 2012, the agency issued a memorandum informing employees of their responsibilities for safeguarding PII. Additionally, in March of 2011, the agency developed and implemented policies regarding security of data on Personal Digital Assistants (PDA) and a Management Directive addressing Cybersecurity awareness briefings for all new employees and annual security awareness training for current employees. The Management Directive also addresses specialized training for select IT personnel to ensure they are properly deploying security awareness throughout the agency. The training focuses on security, which includes privacy over the data residing on the FMC's network. The agency also has well-established policies documenting the various privacy act requirements, as well as procedures for complying with the various privacy regulations and developing a PIA.

While we identified program strengths, we also noted areas where improvement is possible. The FMC's SAOP, CIO, PAO and senior managers have responsibility for the agency's systems and compliance with Federal laws, regulations, and policies relating to information privacy. Although there is interaction and communication between these individuals, communication and coordination on information privacy, including review of systems and determinations for PIAs, could be improved. Many subsidiary systems, including FMC-2, FMC-7, and FMC-24 have not had an analysis performed to identify if a PIA is required for completion. We also identified concerns with System of Records Notices (SORNs) postings and "routine uses" for systems. Three existing PIAs are outdated and the agency has not informed the public about some systems containing PII.

MANAGEMENT RESPONSES

We have included management's response to the OIG recommendation(s) at the end of the report. The OIG has closed two of four recommendations based on management's response and OIG follow up. The OIG was unable to assess corrective actions on the remaining two recommendations without detailed follow up and/or additional fieldwork. The OIG will perform all necessary verification processes in the FY 2013 FISMA cycle.

01 SAOP, CIO, OIT Director, and PAO Coordination

Condition:

There are 25 systems at the FMC that reside within different offices at the agency. The areas of responsibility reside with the Privacy Act Officer, Senior Agency Official for Privacy (SAOP), and the respective managers of systems of records. The Privacy Act Officer works toward the implementation and enforcement of the Privacy Act by, for example, publishing systems of records in the Federal Register, reviewing privacy policies and coordinating with the SAOP. The SAOP ensures steps are taken to protect personal data from unauthorized use in consultation with managers and the Privacy Act Officer. The SAOP also conducts periodic reviews of privacy documentation. The managers of systems of records inform the Privacy Act Officer regarding the existence of systems, monitor routine use, and assist in the safeguarding of privacy data. The list of agency systems is noted below:

Privacy Systems
1. GSS Network (electronic system) a. FMC – 2 (Non-Attorney Practitioner File – paper and electronic system) b. FMC – 24 (Informal Inquiries and Complaints Files – paper and electronic system) c. FMC – 32 (Regulated Persons Index – electronic system) 2. SERVCON (electronic system) 3. FMCDB (electronic system) a. FMC-1 (paper system) b. FMC-18 (paper system) 4. Systems residing on personal computers or storage media a. FMC – 7 (Licensed Ocean Transportation Intermediaries Files – paper and electronic system) b. FMC – 22 (Records Tracking System – paper and electronic system) c. FMC – 25 (Inspector General File – electronic system) d. FMC – 31 (Debt Collection Files – paper and electronic system) 5. Office of Personnel Management (OPM) systems a. FMC – 8 (Official Personnel Folder – electronic system) b. FMC – 9 (Training Program Records – electronic system) c. FMC – 14 (Medical Examination File – electronic system) d. FMC – 16 (Classification Appeals File – electronic system) e. FMC – 19 (Financial Disclosure Reports and Other Ethics Program Records – electronic system) f. FMC – 28 (Equal Employment Opportunity Complaints Files – electronic system) g. FMC – 29 (Employee Performance File System Records – electronic system) 6. Paper based systems a. FMC – 10 (Desk Audit File – paper based system) b. FMC – 26 (Administrative Grievance File – paper based system) c. FMC – 33 (Payroll/Personnel System – paper and electronic system) d. FMC – 34 (Travel Charge Card Program – electronic system) e. FMC – 35 (Transit Benefits File – electronic system) f. FMC – 36 (SmartPay Purchase Charge Card Program – electronic system)

Specifically, the following was noted:

1. The SAOP, PAO, CIO, and OIT Director are recognized as needing better coordination of privacy related requirements to ensure compliance with Privacy regulations.

2. All systems housing PII should be assessed to determine if a PIA is warranted. The PIA will help to ensure that controls are deployed on those systems that are commensurate with the PII residing on those systems. There are 22 systems where management has not determined whether a PIA is required and, if so, whether the PIA should be placed on the agency's website. This deficiency focuses on the lack of PIA determination and not the controls over the PII residing on those systems. Some of the systems are managed by third parties and do not require a PIA. Some of the systems are also protected physically and have no data in electronic format. Thus, management must a determination whether a PIA is needed then takes steps to ensure that controls deployed throughout the various systems are strong enough to protect against PII exploitation.

Criteria:

1. The National Institute of Standards and Technology (NIST) describes how an agency can identify Personally Identifiable Information (PII), enabling the agency to properly maintain an inventory of systems and what PII resides on each of those systems. The NIST guidance also provides guidance on how to perform a PIA. See **NIST 800-122** Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), **section 2.1:**

"Organizations should use a variety of methods to identify all PII residing within their organization or under the control of their organization through a third party (e.g., a system being developed and tested by a contractor). Privacy threshold analyses (PTAs), also referred to as initial privacy assessments (IPAs), are often used to identify PII. Some organizations require a PTA to be completed before the development or acquisition of a new information system and when a substantial change is made to an existing information system. PTAs are used to determine if a system contains PII, whether a Privacy Impact Assessment is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. PTAs should be submitted to an organization's privacy office for review and approval. PTAs are often comprised of simple questionnaires that are completed by the system owner. PTAs are useful in initiating the communication and collaboration for each system between the privacy officer, the information security officer, and the information officer. Other examples of methods to identify PII include reviewing system documentation, conducting interviews, conducting data calls, or checking with system owners."

2. NIST also describes the various elements making up PII. The elements below shall be considered when assessing the PII in systems maintained by the FMC, as noted in **NIST 800-122 section 2.1:**

"This publication uses the definition of PII from OMB Memorandum 07-16, which is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. To distinguish an individual is to identify an individual."

- Name, such as full name, maiden name, mother's maiden name, or alias;
- Personal identification number, such as SSN, passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number;
- Address information, such as street address or email address;
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people;
- Telephone numbers, including mobile, business, and personal numbers;
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry);
- Information identifying personally owned property, such as vehicle registration or identification number, and title numbers and related information; and
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, or employment, medical, education, or financial information).

3. The OMB has specific requirements regarding when and how a PIA should be conducted. This criteria states the instances when a PIA shall be performed as noted by **OMB Memorandum 03-22 section II.B.2:**

The E-Government Act of 2002 requires agencies to conduct a PIA. In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:

- Conversions - when converting paper-based records to electronic systems;
- Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
- Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;
- Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated;

- New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
- Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
- New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
- Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form;
- Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

Cause:

There is a lack of communication and coordination between the SAOP, PAO, CIO, and OIT Director, possibly leading to the absence of PIAs for some of the agency's systems.

Risk:

Without periodic communication and coordination between the OIT, CIO, and PAO, there may be PII vulnerable to exposure.

Recommendation(s):

1. The system owners/managers, CIO, OIT Director, SAOP, and PAO should hold annual meetings to discuss the various requirements for all FMC systems to determine the security requirements of protecting the PII residing within those systems. Those meetings should discuss the following:

- Complete inventory of systems and the type of data residing on those systems.
- The safeguarding of data on those systems.
- The management of the systems. For example, are the systems managed by a third party or managed in-house by the FMC?
- Electronic versus paper-based systems.
- The types of controls deployed and whether or not this is commensurate with the data residing on the systems.
- PIAs for each system.
- SORNs and routing uses for each system.

2. The system owners/managers, and as appropriate, system analyst or developer, should prepare privacy threshold analyses (PTAs) or initial privacy assessments (IPAs) to

identify PII in existing or proposed agency systems. Based on completed PTAs/IPAs, the SAOP and CIO should work with the PAO to determine if PIAs are needed for those systems that have not had a PIA completed. Furthermore, the Privacy/Freedom of Information Act (FOIA) Officer should ensure that completed PIAs transmitted to him/her from the SAOP and CIO is posted to the Commission's Internet website as appropriate.

02 System of Records Notices and Routine Use Review

The Privacy Act of 1974 places restrictions on the ability of Federal agencies to share a system of records with third parties, including other agencies. However, the Privacy Act does recognize the need of the government to share records in order to improve security, maintain accuracy and consolidate resources. This is often accomplished through matching programs which allow certain data elements in one system of records to be searched against records in another system in order to find any data matches. Such matches would link together the information from both systems.

The Privacy Act contains a "routine use" exception which allows the disclosure of information without the notice or consent of the individual. Routine use is defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected."

"A System of Records is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol or other identifying particular assigned to the individual."

A System of Records Notice (SORN) informs the public of the existence of a system of records and describes the type of information that an agency will be collecting, who will be collecting the information, how it will be safeguarded, the purpose for collecting such information, etc. It is an advanced notice to the public that must be given before an agency begins to collect, is given access to or can retrieve personal information for a new system of records and must be published in the Federal Register. As long as the SORN contains a listing of the routine uses of the information, an agency is considered compliant with the Privacy Act.

The following system of record notices has been published in the Federal Register:

1. FMC – 1 (Personnel Security File – paper based system)
2. FMC – 2 (Non-Attorney Practitioner File – paper and electronic system)
3. FMC – 7 (Licensed Ocean Transportation Intermediaries Files – paper and electronic system)
4. FMC – 8 (Official Personnel Folder – electronic system)
5. FMC – 9 (Training Program Records – electronic system)
6. FMC – 10 (Desk Audit File – paper based system)
7. FMC – 14 (Medical Examination File – electronic system)
8. FMC – 16 (Classification Appeals File – electronic system)
9. FMC – 18 (Travel Orders / Vouchers File – paper based system)
10. FMC – 19 (Financial Disclosure Reports and Other Ethics Program Records – electronic system)
11. FMC – 22 (Records Tracking System – paper and electronic system)

12. FMC – 24 (Informal Inquiries and Complaints Files – paper and electronic system)
13. FMC – 25 (Inspector General File – electronic system)
14. FMC – 26 (Administrative Grievance File – paper based system)
15. FMC – 28 (Equal Employment Opportunity Complaints Files – electronic system)
16. FMC – 29 (Employee Performance File System Records – electronic system)
17. FMC – 31 (Debt Collection Files – paper and electronic system)
18. FMC – 32 (Regulated Persons Index – electronic system)
19. FMC – 33 (Payroll/Personnel System – paper and electronic system)
20. FMC – 34 (Travel Charge Card Program – electronic system)
21. FMC – 35 (Transit Benefits File – electronic system)
22. FMC – 36 (SmartPay Purchase Charge Card Program – electronic system)

Agencies are also required to periodically review their systems and ensure the SORN listing maintained on the agency website is current. Agencies are also required to identify those systems without a SORN and assess if there are PII records within those systems that should have been communicated to the public via a SORN.

Condition:

3. "Routine Uses" are not described for the IT systems:

- GSS Network
- SERVCON
- FMCDB

4. Currently, there are 3 systems without a published SORN, even though it is a requirement that these systems should have an associated SORN that is published, thereby communicating to the public at large, regarding the data collected.

- GSS network
- SERVCON
- FMCDB

Criteria:

The OMB provides guidance regarding publishing of system records to ensure the public's trust, as stated in **OMB M-99-05,** Instructions on complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records", **section 4:**

"In passing the Privacy Act, the Congress made a strong policy statement that in order to ensure fairness, there shall be no record keeping systems, the very existence of which is secret. Therefore, each agency shall review its operations to identify any *de facto* systems of records for which no system of records notice has been published. If the agency identifies any such unpublished systems of records, then the agency should publish a system of records notice for the system promptly. Agencies shall implement appropriate measures (e.g., training) to ensure that system of records are not inadvertently established, but instead are established in accordance with the notice and other requirements of the Privacy Act."

1. Lastly, the OMB provides guidance on the periodic reviews of systems to ensure that unpublished records are complete and accurate, as stated in **OMB M-99-05, attachment B**:

"The Privacy Act of 1974 (5 U.S.C. § 552a, the Act) requires agencies to inform the public of the existence of systems of records containing personal information, to give individuals access to records about themselves in a system of records, and to manage those records in a way to ensure fairness to individuals in agency programs.

For the Privacy Act to work effectively, it is imperative that each agency properly maintain its systems of records and ensure that the public is adequately informed about the systems of records the agency maintains and the uses that are being made of the records in those systems. Therefore, agencies must periodically review their systems of records and the published notices that describe them to ensure that they are accurate and complete. OMB Circular A-130, "Management of Federal Information Resources," (61 Fed. Reg. 6428, Feb. 20, 1996) requires agencies to conduct periodic reviews, in accordance with the schedule in Appendix I of the Circular."

2. Each agency shall conduct a thorough review of its systems of records, system of records notices, and routine uses in accordance with the criteria and guidance below, as described by **OMB M-99-05, section 2:**

"Non-statutory disclosures created by administrative mechanisms should only be made when appropriate. Therefore, each agency shall review its "routine uses" to identify any routine uses that are no longer justified, or which are no longer compatible with the purpose for which the information was collected. The Privacy Act requires agencies to include in their systems of records notices a description of the routine uses for which information in a system of records may be disclosed. 5 U.S.C. § 552a(e)(4)(D)."

Cause:

OIT was not fully aware of its requirements and responsibilities with regard to SORNs and Routine Use review.

Risk:

Currently, the public is being misinformed regarding the listing of systems on the FMC website because the system listing is incomplete. The FMC is responsible to ensure that systems have published SORNs so that the public may be adequately informed of the systems that are in the agency's inventory and the PII contained within those systems. Without knowing if there are any unpublished systems, the public at large will be misinformed with regard to the complete listing of systems presented by the FMC. Also, documenting the "Routine Uses" enables IT to adequately protect the PII residing on systems. Without a full understanding of "Routine Uses," the data may not be adequately protected.

Recommendation(s):

3. The OIT should review all routine uses for the GSS Network, SERVCON, and the FMCDB. If any of those routine uses are no longer appropriate, the OIT should work with the PAO to delete those routine uses from the SORN and update accordingly on the agency's website.

4. As the system manager/owner, the OIT, and as appropriate, system analyst or developer, should prepare privacy threshold analyses (PTAs) and/or PIAs for the GSS Network, SERVCON, and FMCDB to determine if any of these systems contain records of individuals covered by the Privacy Act (i.e., contain PII). For each of these systems where PII is identified and after SAOP/CIO review, the OIT should prepare for publication, appropriate SORNs.

03 Privacy Impact Assessments

A Privacy Impact Assessment (PIA) is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Condition:

5. PIAs are required to be updated every 3 years (or earlier if the system had a significant change). PIAs are also required for new systems. A PIA has not been performed on one system and the PIA is outdated for two additional systems. See below for details:

- GSS Network – PIA last completed in 2008.
- SERVCON – PIA last completed in 2008.
- FMCDB – no PIA completed.

Criteria:

1. The OMB has specific requirements regarding when and how a PIA should be conducted. This criteria states the instances when a PIA shall be performed as noted by **OMB Memorandum 03-22 section II.B.2:**

The E-Government Act of 2002 requires agencies to conduct a PIA. In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:

- Conversions - when converting paper-based records to electronic systems;

- Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
- Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;
- Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated;
- New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
- Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
- New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
- Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form;
- Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

Cause:

The OIT has not made updating the two PIAs (GSS Network and SERVCON) and completing a new PIA (FMCDB) a priority because of competing demands on resources for.

Risk:

With outdated PIAs for some of the OIT systems, FMC may not be deploying security controls that are commensurate with the PII that resides on those systems.

Recommendation(s):

5. The OIT should update the PIA for the GSS Network and SERVCON systems, and complete a new PIA for the FMCDB. The PIAs should be approved and reviewed by the SAOP.

Prior Year Recommendations

#	POA&M	Report	Open / Closed
1	Develop and implement policies and procedures to require privacy impact assessments (PIA) to be completed for each applicable information system. **This was rolled into recommendation #7 on Report A12-02.**	Report A11-01A	**Open**
2	Remove the FMC-18 (Form-18) PIA from the publicly accessible web that incorrectly states, "A risk assessment has been conducted and the appropriate controls have been implemented" as no authorization (formerly Certification & Accreditation (C&A)) package was created for this system. **This was closed prior to the FISMA 2011 testing.**	Report A11-01A	Closed
3	Create a planning document for multifactor authentication that correlates with the IT capital planning and investment control process. Utilize multifactor authentication for remote authentication for FMC systems to authenticate users' identifies for Level 3 and 4 users in accordance with National Institute of Standards and Technology (NIST) 800-63. **This was rolled into recommendation #6 - Report A12-02.**	Report A11-01A	**Open**
4	Create policies and/or procedures to log, verify and reassess data extracts from database holding sensitive information after 90 days. **Policies are now in place that addresses this POA&M.**	Report A11-01A	Closed

Form **FMC-2** UNITED STATES GOVERNMENT FEDERAL MARITIME COMMISSION
(Rev. 07-89)

Memorandum

TO : Inspector General **DATE:** November 29, 2012

FROM : Senior Agency Official for Privacy (SAOP)

Privacy Act Officer (PAO)

SUBJECT : Joint Response on Evaluation of the FMC's FY 2012 Privacy and Data Protection

We have reviewed the recommendations in the subject Privacy and Data Protection Evaluation, and provide our responses below. Our responses assume adequate FY 2013 agency funding and resources.

Finding #1: SAOP, CIO, OIT Director, and PAO Coordination

Recommendation #1: The system owners/managers, CIO, OIT Director, SAOP, and PAO should hold annual meetings to discuss the various requirements for all FMC systems to determine the security requirements of protecting the PII residing within those systems. Those meetings should discuss the following:

a. Complete inventory of systems and the type of data residing on those systems.
b. The safeguarding of data on those systems.
c. The management of the systems. For example, are the systems managed by a third party or managed in-house by the FMC?
d. Electronic versus paper-based systems.
e. The types of controls deployed and whether or not this is commensurate with the data residing on the systems.
f. PIAs for each system.
g. SORNs and routing uses for each system.

Response: We concur in the recommendation. During FY 2013 the PAO (coordinating with the SAOP, CIO, and the OIT Director) will kick off a project to conduct an agency-wide System of Record (SOR) review on existing FMC systems and any proposed systems for compliance

with the Privacy Act. System owners/managers will be engaged in developing and providing input for systems under their control/responsibility. Appropriate Federal Register Notices will be drafted and published. Thereafter, the system owners/managers, CIO, SAOP, OIT Director, and PAO will meet annually to discuss any changes to existing systems and anticipated new systems, and security requirements for protecting PII residing in agency systems.

Recommendation #2: The system owners/managers, and as appropriate, system analyst or developer, should prepare privacy threshold analyses (PTAs) or initial privacy assessments (IPAs) to identify PII in existing or proposed agency systems. Base on completed PTAs/IPAs, the SAOP and CIO should work with the PAO to determine if PIAs are needed for those systems that have not had a PIA completed. Furthermore, the Privacy/FOIA Act Officer should ensure that completed PIAs transmitted to him/her from the SAOP and CIO, are posted to the Commission's Internet website as appropriate.

Response: We concur in the recommendation. In connection with the agency-wide SORN review coordinated by the PAO noted in response to Recommendation #1, the SAOP/CIO will oversee completion of PTAs for agency systems and proposed systems. Based on completed PTAs, the SAOP and CIO will meet with the PAO to determine if PIAs are needed for agency systems. The Privacy/FOIA Act Officer will ensure that completed PIAs transmitted to him/her from the SAOP/CIO, are posted to the Commission's Internet website as appropriate.

Finding #2: System of Records Notices and Routine Use Review

Recommendation #3: The OIT should review all routine uses for the GSS Network, SERVCON, and the FMCDB. If any of those routine uses are no longer appropriate, the OIT should work with the PAO to delete those routine uses from the SORN and update accordingly on the agency's website.

Response: We concur in the recommendation. During FY 2013 an agency-wide project to review agency System of Records, including the GSS Network, SERVCON, and FMCDB will be conducted, with any necessary updates or publication of systems completed. (See Response to Recommendation Number #1 above).

Recommendation #4: As the system manager/owner, the OIT, and as appropriate, system analyst or developer, should prepare privacy threshold analyses (PTAs) and/or PIAs for the GSS Network, SERVCON, and FMCDB to determine if any of these systems contain records of individuals covered by the Privacy Act (i.e., contain PII). For each of these systems where PII is identified and after SAOP/CIO review, the OIT should prepare for publication, appropriate SORNs.

Response: We concur in the recommendation and note that this recommendation will be handled as part of our response to Recommendation Numbers 1 and 2 above.

Finding #3: Privacy Impact Assessments

Recommendation #5: The OIT should update the PIA for the GSS Network and SERVCON systems, and complete a new PIA for the FMCDB. The PIAs should be approved and reviewed by the SAOP/CIO.

Response: We concur in the recommendation and note that this recommendation will be handled as part of our response to Recommendation Number 2 above.

/Austin L. Schmitt/	/Karen V. Gregory/
Senior Agency Official for Privacy	Privacy Act Officer

cc: Chief Information Officer
Director, Office of Information Technology