

Office of Inspector General

**Evaluation of the FMC's FY 2014
Privacy and Data Protection**

A15-03



November 2014

FEDERAL MARITIME COMMISSION



FEDERAL MARITIME COMMISSION
Washington, DC 20573

November 14, 2014

Office of Inspector General

Dear Chairman Cordero and Commissioners:

The Office of Inspector General (OIG) performed an evaluation 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 the agency's use of personally identifiable information (PII) and of its privacy and data protection policies and procedures. This evaluation satisfies the required privacy review. 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. Protecting the privacy rights and PII of FMC employees, stakeholders and other interested parties is a responsibility of the agency.

The agency has significantly improved its privacy program since our last evaluation in 2012. Specifically, all five of the outstanding recommendations from the 2012 evaluation have been implemented. In addition, there are no new findings as a result of this year's 2014 privacy evaluation.

The OIG wishes to thank the FMC staff, particularly the Privacy Act Officer and the Senior Agency Official for Privacy, for their assistance. I am available at your convenience to discuss the results of the evaluation.

Respectfully submitted,

Jon Hatfield
Inspector General

Attachment

cc: Vern W. Hill, Managing Director and Senior Agency Official for Privacy
Karen V. Gregory, Secretary and Privacy Act Officer
Tyler J. Wood, Deputy General Counsel
Anthony Haywood, Chief Information Officer
Anthony Wheat, Director, Office of Information Technology
Gregory S. Francis, Information Systems Security Officer

FEDERAL MARITIME COMMISSION
OFFICE OF INSPECTOR GENERAL



Evaluation of the FMC's FY 2014
Privacy and Data Protection

TABLE OF CONTENTS

BACKGROUND	1
EXECUTIVE SUMMARY	2
OBJECTIVES AND SCOPE.....	2
RESULTS	2
PRIOR YEAR RECOMMENDATIONS	3
ATTACHMENT	
MANAGEMENT'S RESPONSE.....	5

BACKGROUND

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, 5 U.S.C. § 552a, as amended, and Office of Management and Budget (OMB) Memorandum M-06-15, Safeguarding Personally Identifiable Information¹, requires agencies to collect only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order of the President. Agencies are required to protect this information from any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the information is maintained, and must not disclose this information except under certain circumstances. The information collected is considered a record under the Privacy Act if it is an item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

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 Privacy Act requires that a public notice, commonly referred to as a System of Records Notice (SORN), be published in the Federal Register that describes the existence and character of the system of records.

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.

¹ The term “personally identifiable information” refers to 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.

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 memoranda, Consolidated Appropriations Act of 2005, etc.). The Consolidated Appropriations Act of 2005, as amended, requires agencies to assign a Chief Privacy Officer (CPO) who is responsible for identifying and safeguarding personally identifiable information (PII) and requires a periodic independent third-party review of agency use of PII and of its privacy and data protection policies and procedures.

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.
- Assessed the agency's progress toward implementing corrective actions in prior evaluation reports.

RESULTS

The agency has improved its privacy program since our last review in 2012. It was determined through our evaluation procedures that there were no new findings. In our previous Privacy evaluation, we noted three new findings. FMC has made tremendous strides in closing those findings since our last evaluation. For example, FMC took a full inventory count of all systems. Those systems were reviewed to identify any PII, and then controls commensurate with the privacy risks were deployed to ensure that the security posture is sufficient. Privacy Impact Assessments (PIAs) were developed for all systems, where it was required in accordance with Privacy laws and regulations. Additionally, routine uses were reviewed for all systems as well as all SORNs. All necessary updates were made to the Federal Register, and updates were made to the FMC website, where the public at large can review the PIAs, privacy concerns, and more. As a result of our evaluation this year, all privacy findings that were identified in the last evaluation, are now closed.

PRIOR YEAR RECOMMENDATIONS

	Recommendations	Report	Open / Closed
1.	<p>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:</p> <ul style="list-style-type: none"> • 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 routine uses for each system. 	Report FY 2012	Closed
2.	<p>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.</p>	Report FY 2012	Closed
3.	<p>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.</p>	Report FY 2012	Closed
4.	<p>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.</p>	Report FY 2012	Closed

	Recommendations	Report	Open / Closed
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.	Report FY 2012	Closed

Memorandum

TO : Inspector General

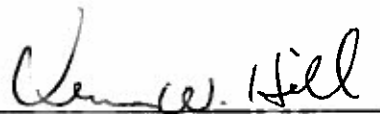
DATE: November 12, 2014

FROM : Senior Agency Official for Privacy (SAOP)
Privacy Act Officer (PAO)

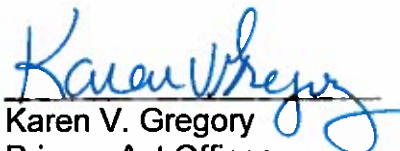
SUBJECT : Evaluation of the FMC's FY 2014 Privacy and Data
Protection – Management's Response

All actions to address the Inspector General's (IG's) findings and recommendations contained in the *A13-02, Evaluation of the FMC's FY 2012 Privacy and Data Protection* were completed and documented by management on September 30, 2013, and provided to the IG on same date. The subject 2014 Evaluation noted the agency actions taken to address the previous privacy findings and recommendations and determined that ". . . all privacy findings that were identified in the last evaluation [FY 2012], are now closed." The subject 2014 Evaluation did not identify any new findings requiring agency action, therefore management considers the previous matters closed and has no further comment.

We appreciate the IG's and its auditor's review and acknowledgment of the agency actions taken to address and close all past privacy findings and recommendations and to significantly improve the Commission's Privacy Program.



Vern W. Hill
Senior Agency Official for Privacy



Karen V. Gregory
Privacy Act Officer

cc: Chief Information Officer
Director, Office of Information Technology