Office of Inspector General

Evaluation of the FMC's Compliance with the Federal Information Security Management Act FY 2013

A14-02

December 2013

FEDERAL MARITIME COMMISSION

FEDERAL MARITIME COMMISSION
Washington, DC 20573

January 3, 2014

Office of Inspector General

Dear Chairman Cordero and Commissioners:

The Office of Inspector General (OIG) submits its report on the status of information security at the Federal Maritime Commission (FMC) for fiscal year (FY) 2013. The OIG relied on the expertise of information security evaluators from *Your Internal Controls LLC,* for assistance on this mandated review.

The objectives of this independent evaluation of the FMC's information security program were to evaluate its security posture by assessing compliance with the Federal Information Security Management Act (FISMA) and related information security policies, procedures, standards, and guidelines. The scope of this evaluation focused on the FMC General Support Systems (GSS) and Major Applications. The OIG also performed a network scan to identify potential system vulnerabilities and assessed management actions to implement prior-year recommendations.

The OIG is pleased to report the evaluators did not find any new deficiencies in this year's FISMA evaluation. Further, the agency continues to make progress addressing outstanding deficiencies from prior year FISMA evaluations.

The OIG would like to thank FMC staff, especially the Office of Information Technology (OIT), for their assistance in helping the OIG meet our evaluation objectives.

Respectfully submitted,

Jon Hatfield
Interim Inspector General

TABLE OF CONTENTS

PURPOSE

Your Internal Controls (contractor), on behalf of the Federal Maritime Commission (FMC), Office of Inspector General (OIG), conducted an independent evaluation of the quality and compliance of the FMC's information security program with applicable federal computer security laws and regulations. Your Internal Controls' evaluation focused on FMC's information security program as required by the Federal Information Security Management Act (FISMA). This report was prepared by the contractor with guidance by the Office of Inspector General.

BACKGROUND

On December 17, 2002, the President signed into law H.R. 2458, the E-Government Act of 2002 (Public Law 107-347). Title III of the E-Government Act of 2002, commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency. This program includes providing security for information systems provided or managed by another agency, contractor or other source. FISMA assigns specific responsibilities to agency heads and Inspectors General (IGs). FISMA is supported by security policy promulgated through the Office of Management and Budget (OMB), and risk-based standards and guidelines published in the National Institute of Standards and Technology (NIST), Special Publication (SP) series.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems. FISMA requires agencies to have an annual independent evaluation performed on their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG. Implementing adequate information security controls is essential to ensuring an organization can effectively meet its mission.

SCOPE AND METHODOLOGY

The scope of our testing focused on the FMC General Support Systems (GSS) and Major Applications. We conducted our testing through inquiry of FMC personnel, observation of activities, inspection of relevant documentation, and the performance of technical security testing. More specifically, our testing covered a sample of controls as listed in NIST 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 4. For example, testing covered system security plans, access controls, risk assessments, configuration management, contingency planning, security awareness and auditing. Our scope also included a Vulnerability Assessment for the overall network and workstations that connect to the network.

Our testing was for the period October 1, 2012 through September 30, 2013 (fiscal year 2013). From the recommendations noted in the table below, there are several issues that FMC appears to have made significant progress correcting during FY 2013. Specifically, recommendations 10, 11, 12, 13, and 14 all relate to certification and accreditation (C&A) matters. These recommendations could not be tested during this year's evaluation because supporting documents were provided to the evaluators on September 30, 2013, the last day of fieldwork. Therefore, ample time was not available to review the documents and make a final determination on whether to close the recommendations. However, the issue will be reviewed for compliance during the next FISMA cycle.

FMC provided us with information and documentation regarding monthly reviews of audit logs that had been performed by FMC, starting in the latter part of the review period. Recommendation 2 involves a process in which audit logs are reviewed monthly and necessary actions are taken to respond to those audit events generated as a result of adverse actions. Because the deficiency was corrected during the latter part of the review period, we have decided to report this issue as open until we can determine the process is being consistently performed over a longer period of time. This issue will be reviewed during the next FISMA cycle and we are hopeful the issue will be closed.

CURRENT YEAR FINDINGS

During our FY 2013 evaluation, we noted that FMC has taken steps to improve the information security program and to remediate some prior year deficiencies. For example, the FMC has deployed complexity settings on the servers supporting the major applications. The OIG did not find any new deficiencies in this year's FISMA evaluation. It shall also be noted that there were no new findings. Although there were no new findings, the FMC continues to rely on the OIG to run vulnerability scans on an annual basis. It has been suggested that the agency should run its own scans by purchasing the necessary software to do so. The estimated costs to purchase such software would be minimal and this software can be run as many times as necessary (e.g. monthly, quarterly, etc.). This software would assist in identifying vulnerabilities, outdated patches and virus definitions, and more. It is strongly recommended by the OIG, that the OIT purchase such software to better enable the agency to manage and respond to risks.

PRIOR YEAR RECOMMENDATIONS

The following table details 16 prior year recommendations identified during our FISMA evaluations that were open at the commencement of the FY 2013 FISMA evaluation.

We've determined that recommendation Nos. 2, 4, and 10 (from the chart below) are the most critical and should be remediated as soon as possible.

# 2 – Audit Settings - addresses the review of audit logs. Without reviewing the logs, there may be negative actions taken against the agency without awareness on the part of OIT. The audit logs must be reviewed timely and corrective actions (e.g. investigating failed logon attempts) must be taken as a result of those reviews.

# 4 – Contingency Plan - addresses the Contingency Plan. Without a final and signed Contingency Plan, the agency lacks basic assurances that the agency's critical functions could proceed during a catastrophic event without loss or compromise of its data.

# 10 – Certification and Accreditation - identifies C&A package shortcomings for the network and the SERVCON application. C&A packages document the various security controls, as identified from a security categorization (FIPS-199). The controls are then tested, and evaluated

to ascertain if there are any risks that would preclude the system from being placed in a live environment. Without finalized C&A packages, data may not be adequately protected with commensurate security controls.

During the FY 2013 review of FMC's information security, FMC has made strides in remediating prior year deficiencies. The FMC has remediated 4 of the 16 recommendations. Specifically, the agency is in the process of deploying Pretty Good Privacy (PGP) Symantec encryption on workstations and on mobile devices. The FMC has also made advances in clarifying the system inventory and determining those systems with Personally Identifiable Information (PII), as well as which of those systems need a privacy impact assessment (PIA). Lastly, the FMC has recently signed the GSS and SERVCON C&A packages as final. These accomplishments will be tested during the FY 2014 FISMA evaluation.

STATUS OF PRIOR YEAR RECOMMENDATIONS

	POA&M	Report	Open / Closed
1	Evaluate FMC mobile needs and implement FIPS 140-2 encryption on mobile computers and portable devices carrying agency data. *(OIG estimates the required level of effort for this recommendation to be 20 hours).*	Report A2010-02 (#3)	Open
2	Ensure that audit logs are reviewed monthly and necessary actions are taken to respond to those audit events generated as a result of adverse actions. *(OIG estimates the required level of effort for this recommendation to be 5 hours per month).*	Report A2012-02 (#2)	Open
3	Ensure only IT personnel and others with a job-related need have access to the Data Center by reviewing non-OIT personnel access badges and disabling as appropriate.	Report A2012-02 (#4)	Closed
4	Ensure that the Contingency Plan has been reviewed and signed off as final. Also, ensure that OIT performs a contingency test, training, and exercise in accordance with NIST 800-34. *(The estimated level of effort for this recommendation is 40 hours).*	Report A2012-02 (#5)	Open
5	Ensure that IT personnel are properly trained with regard to incident response prevention, detection, and correction.	Report A2012-02 (#6)	Closed
6	Implement HSPD-12 in accordance with laws and regulations. (OIG estimates the required level of effort for this recommendation to be 40 hours).	Report A2012-02 (#8)	Open

STATUS OF PRIOR YEAR RECOMMENDATIONS

	POA&M	Report	Open / Closed
7	A system inventory should be maintained and from this listing, the following should be performed: • identify which of those systems have PII and Information in Identifiable Form (IIF). • identify which of those systems need a PIA. • identify which of those PIAs need to be posted on the FMC website. • identify information that needs to be redacted prior to posting of the PIA on the FMC website. *(OIG estimates the required level of effort for this recommendation to be 20 hours).*	Report A2012-02 (#9)	Open
8	Ensure that IT incorporates the agency's checkout process for terminated employees into its access procedures and updates access permissions for those employees who are promoted or move (i.e., change assignments) within the agency. This will ensure that IT changes the user access settings appropriately. IT should also review access rights on a quarterly basis and with other Commission bureaus and offices to identify and assess non-FMC personnel access needs for other users such as those users that are external to the agency.	Report A2012-02 (#10)	Closed
9	Ensure that password complexity is set to "enable" and applies to all personnel within the FMC agency.	Report A2012-02 (#12)	Closed
10	The Network GSS C&A and the SERVCON C&A should be signed and finalized. *(OIG estimates the level of effort for this recommendation at 40 hours).*	Report A2012-02 (#13)	Open

STATUS OF PRIOR YEAR RECOMMENDATIONS

	POA&M	Report	Open / Closed
11	All controls in the System Security Plans (SSPs) should be reviewed to ensure their implementation status is correct. *(OIG estimates the level of effort for this recommendation at 40 hours).*	Report A2012-02 (#16)	Open
12	Any weaknesses as a result of Security Test and Evaluations (STEs) should be corrected immediately. *(OIG estimates the level of effort for this recommendation at 20 hours).*	Report A2012-02 (#17)	Open
13	The FMC Database (FMCDB) should be carved out into a separate C&A package. *(OIG estimates the level of effort for this recommendation at 40 hours).*	Report A2012-02 (#18)	Open
14	The SERVCON system should have an e-Authentication assessment conducted. *(OIG estimates the level of effort for this recommendation at 2 hours).*	Report A2012-02 (#19)	Open
15	Identify which patches are missing and assess which of those can be deployed without harming the network. Once complete, deploy the patches to ensure the network is protected.	Report A13-03 (#1)	Open
16	Disable all services running on the hosts that are not being used. If the services are being used, then deploy the latest versions, which will provide the latest security protection. Also, if FTP is to be deployed on servers, ensure that anonymous access is prohibited and secure transmission is required.	Report A13-03 (#2)	Open

UNITED STATES GOVERNMENT

FEDERAL MARITIME COMMISSION

Memorandum

TO : Inspector General

DATE: December 30, 2013

FROM : Managing Director

SUBJECT : Evaluation of the FMC's Compliance with the Federal Information Security Management Act, FY 2013

Management has reviewed the above-captioned audit, and notes that the auditor found no new deficiencies and makes no new recommendations. While the auditor indicates that the FMC has remediated 4 of 16 recommendations outstanding from prior years, it is management's position that 9 of those 16 recommendations have been resolved. The remaining open recommendations will be addressed and should be resolved during FY 2014. The results of this activity should be reflected in the OIG's next FISMA evaluation. Management provides the following comments with respect to the recommendations reported as outstanding from prior years:

► **Audit 2010-02, *FY 2009 Implementation of FISMA***

Recommendation #3: Evaluate FMC mobile needs and implement FIPS 140-2 encryption on mobile computers and portable devices carrying agency data.

Comment: As recognized by the OIG's FY 2013 FISMA review, the FMC provided evidence of purchasing Symantec PGP encryption. Staff is in the process of deploying PGP on the agency's mobile computers. This item will be completed during FY 2014.

► **Audit 12-02, *FMC's FY 2011 Implementation of FISMA***

Recommendation #2: Ensure that audit logs are reviewed monthly and necessary actions are taken to respond to those audit events generated as a result of adverse actions.

Comment: As recognized by the OIG's FY 2013 FISMA review, the FMC provided evidence of addressing this recommendation. In FY 2013, ManageEngine EventLog Analyzer software was purchased and implemented, allowing the FMC to automate the process of collecting, analyzing, searching, reporting, and archiving of all of the agencies servers from one central location. This software helps to mitigate internal threats, monitor file integrity, conduct log forensics analysis, monitor privileged users and comply to different compliance regulatory bodies by intelligently analyzing FMC's server logs and instantly generating a variety of reports like user activity reports, and regulatory compliance reports that are reviewed monthly.

Recommendation #5: Ensure that the Contingency Plan has been reviewed and signed off as final. Also, ensure that OIT performs a contingency test, training, and exercise in accordance with NIST 800-34.

Comment: Management is aware of this requirement and will accept the risk. Necessary documentation will be completed to acknowledge this risk acceptance. Management, however, is aware of the need for a finalized Contingency Plan and will make efforts to effectuate such a plan as resources are made available.

Recommendation #8: Implement HSPD-12 in accordance with laws and regulations.

Comment: The FMC is currently in the process of implementing HSPD-12 requirements. Currently 35% of the agency's desktop systems require two-factor authentication. It is intended that this remediation will be completed during FY 2014.

Recommendation #9: A system inventory should be maintained and from this listing, the following should be performed: identify which of those systems have PII and IIF; identify which of those systems need a PIA; identify which of those PIAs need to be posted on the FMC website; and identify information that needs to be redacted prior to posting of the PIA on the FMC website.

Comment: As recognized by the OIG's FY 2013 FISMA review, "The FMC has also made advances in clarifying the system inventory and determining those systems with Personally Identifiable Information (PII), as well as which of those systems need a privacy impact assessment (PIA)." The FMC has identified which of those PIAs need to be posted on the FMC website, and identified information to be redacted prior to posting on the FMC website. This item has been addressed and will be subject to verification in FY 2014.

Recommendation #13: The Network GSS C&A and the SERVCON C&A should be signed and finalized.

Comment: As recognized by the OIG's FY 2013 FISMA review, "the FMC has recently signed the GSS and SERVCON C&A packages as final. These accomplishments will be tested during the FY 2014 FISMA evaluation." Management believes that this item has been remediated.

Recommendation #16: All controls in the System Security Plans (SSPs) should be reviewed to ensure their implementation status is correct.

Comment: The FMC has conducted a C & A on the FMCGSS and FMCSERVCON systems. FMC is in the process of completing a C & A on the FMCDB system. As part of the C & A process, all controls in the System Security Plans (SSPs) have been reviewed to ensure that their implementation status is correct. Management is confident that this item has been remediated.

Recommendation #17: Any weaknesses as a result of Security Test and Evaluations (STEs) should be corrected immediately.

Comment: Management concurs with this recommendation, and any weaknesses found will be corrected as soon as possible. STEs for both FMCGSS and FMCSERVCON systems were completed as part of the C & As for each system. An STE will be completed as part of the C & A for the FMCDB system during FY 2014.

Recommendation #18: The FMC Database (FMCDB) should be carved out into a separate C&A package.

Comment: The FMCDB was carved out into a separate system, and a C & A will be completed during FY 2014.

Recommendation #19: The SERVCON system should have an e-Authentication assessment conducted.

Comment: The FMC has initiated an e-authentication assessment for the SERVCON system, which will be subject to verification in FY 2014.

► **Audit 13-03,** ***Evaluation of the FMC's Compliance with FISMA FY 2012***

Recommendation #1: Identify which patches are missing and assess which of those can be deployed without harming the network. Once complete, deploy the patches to ensure the network is protected.

Comment: The FMC is in the process of identifying a patch management solution that will allow the agency to identify which patches are missing, assess which patches can be deployed without harming the network, and once identified and deemed safe, allow the FMC to deploy the patches to ensure the network is protected. Management is confident that this item will be remediated during FY 2014.

Recommendation #2: Disable all services running on the hosts that are not being used. If the services are being used, then deploy the latest versions, which will provide the latest security protection. Also, if FTP is to be deployed on servers, ensure that anonymous access is prohibited and secure transmission is required.

Comment: The unused services identified in the auditor's vulnerability assessment scan have been disabled. As funds become available, the FMC will purchase the Nessus vulnerability scanning tool to run regular scans and better enable the agency to manage and respond to risks on a timely basis. It is management's intent that this item will be remediated during FY 2014.

W. Hill

Vern W. Hill
Managing Director

cc: Office of Information Technology
Office of the Chairman