Office of Inspector General

Evaluation of the FMC's Compliance with the Federal Information Security Management Act FY 2014

A15-02

November 2014

FEDERAL MARITIME COMMISSION

FEDERAL MARITIME COMMISSION
Washington, DC 20573

November 14, 2014

Office of Inspector General

Dear Chairman Cordero and Commissioners:

I am pleased to provide the attached Office of Inspector General's (OIG) report on the status of information security at the Federal Maritime Commission (FMC) for fiscal year (FY) 2014. The OIG relied on the expertise of an information security evaluator 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 agency continues to make progress addressing outstanding deficiencies from prior year FISMA evaluations. Specifically, eight of the 12 outstanding recommendations reported in last year's FISMA report have been implemented by the agency; another recommendation from last year was merged with a current year recommendation. This year's report includes five new recommendations to address three findings.

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
Inspector General

Attachment

cc: Vern W. Hill, Managing Director
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 Compliance with the Federal Information Security Management Act FY 2014

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, personnel security, contingency planning, identification / authentication and auditing. Our testing was for the period October 1, 2013 through September 30, 2014 (fiscal year 2014).

CURRENT YEAR FINDINGS

01 Continuous Monitoring / Security Plans

Condition:

Your Internal Controls reviewed the System Security Plans (SSPs) and Security Controls Assessments (SCAs) for all systems in scope (Servcon, FMCDB, and the GSS) and noted the following:

- Each of the SSPs have documentation to addresses the NIST 800-53 Revision 4 controls (e.g. account management, vulnerability scanning, and authenticator management), however, not all of the control objectives for each control are addressed. For example, AC-2 (account management), control objective (f) was not addressed in enough detail as it relates to "creates, enables, modifies, disables, and removes" user access rights. Also, RA-5 (vulnerability scanning) did not address specifics on how vulnerabilities are to be remediated in a timely manner with regards to the type of vulnerability that arose (e.g. low, moderate, or high risks). Lastly, IA-5 (authenticator management) didn't address how initial authenticators are established and the procedures to be followed in the event of a lost or stolen credential.
- Each of the SCAs contain testing for the systems under scope, however, this testing occurs infrequently or not at all for some of the controls. For example, the agency uses a software application to aid in the testing of controls, however, this software application only addresses the more technical controls, such as account management, vulnerability scanning, and authentication. There is no testing performed on controls that are not addressed as part of the software application deployed (for use in continuous monitoring)[1]. For example, the software does not address controls in Security Planning (PL) and Risk Assessment (RA), specifically as it relates to reviewing and updating the security categorization worksheets, and all other required FISMA documentation. These require OIT personnel to review and update specific documentation such as the Privacy Impact Assessment, System Security Plan, Information System Contingency Plan, boundary documents, and plan of action & milestones (POA&M) documentation. Lastly, the software does not address the review of access rights on an annual basis for regular users and semi-annually for administrators, as well as the evidence of audit reviews and corrective actions as a result of those audit reviews.

[1] The Office of Management and Budget (OMB) issued OMB Memorandum 14-03 on November 18, 2013, titled: "Enhancing the Security of Federal Information and Information Systems," which addressed Continuous Monitoring requirements for Federal agencies. As this requirement was issued during this fiscal year's FISMA evaluation, the FMC had not fully implemented the requirements set forth by the OMB.

Criteria:

NIST 800-53 Revision 4, PL-2 states:
"Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions."

NIST 800-53 Revision 4, CA-2 states:
"Assesses the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements."

Cause:

The cause is primarily because of a lack of personnel, budget, or time constraints to adequately document and/or assess all of the controls in NIST 800-53.

Risk:

Without appropriately documenting each of the control objectives, it will be unclear how specific controls are deployed. Without that clarity, controls may be deployed in a manner that are not commensurate with the risks of the system, which may expose the agency to vulnerabilities and exploitation attempts.

Without testing all of the controls, and on a continuous basis, there is a high likelihood that exploitation may occur as the controls are not deployed with the latest protective measures.

Recommendation(s):

1. Review all SSPs and ensure the documentation is clear and addresses each of the controls and all of their respective control objectives.
2. All controls within NIST 800-53 Revision 4 for the systems' categorization should be used as a starting point for determining the assessments and implementation of a continuous monitoring program. Then, management should determine which of those controls are critical. Those critical controls should be assessed every year. The remainder of the controls should then be divided by three and then assessed over a three-year period, whereby 1/3 of the remaining controls are assessed each year. Ideally, the controls to be assessed each year should then be done on a quarterly basis by taking the annual set of controls and assessing 1/4 each quarter.

Management Response:

FMC will review the system SSP's to ensure that each of the controls and all of their respective control objectives are addressed. Additionally, FMC will implement the continuous monitoring process described in the IG recommendation that will allow the FMC to monitor the controls that cannot be assessed by way of the Xacta continuous monitoring suite, but require OIT personnel to review and update. The implementation for this process will begin immediately and the success of this implementation will be determined during the 2015 RMF review period.

Condition:

Your Internal Controls requested evidence that background investigations or screening occurred in a timely manner for both employees and contractors and noted the following:

- No evidence was obtained that contractors are receiving background investigations or screening prior to being given access to data and systems.
- A sample of 12 employees was selected to ascertain if background investigations were performed and documented. The evidence received were as follows:
  - 4 employees lacked sufficient documentary evidence on the outcome of a background investigation.
  - 8 employees had evidence of an investigation having been performed by the Office of Personnel Management (OPM) or other sources within the Federal government.

Criteria:

NIST 800-53 Revision 4, PS-3 states:
"Screens individuals prior to authorizing access to the information system."

Cause:

The cause is primarily because of a lack of detailed knowledge surrounding the requirements in NIST 800-53 Revision 4, as it relates to contractors. Furthermore, the FMC's certifying official responsible for monitoring, certifying and documenting the results of employee background investigations separated from the agency in the latter part of the fiscal year.

Risk:

Without appropriately screening personnel and contractors prior to granting them access to the data and systems, this increases the risk that there are people with access to agency data and systems that should clearly not have been given such access due to an adverse event that has taken place in their past.

Recommendation(s):

3. Ensure all contractors undergo an appropriate investigation or screening prior to being granted access to any data and/or systems. Furthermore, ensure that all contractors undergo appropriate periodic reinvestigations or screening once the initial investigation is deemed to be successful.
4. Ensure a sufficient number of certifying officials are properly authorized and trained on the responsibilities associated with monitoring, certifying and documenting the results of employee background investigations, and reinvestigations, when warranted.

Management Response:

The FMC utilizes the Office of Personnel Management (OPM) to conduct background checks and manage documentation for FMC employee background checks. In the past several years, OPM has converted its records keeping to an online system, granting access to appropriate Commission staff to view records. Due to internal employee turnover, the FMC was unable to timely provide full employee background check records from the OPM system for audit purposes. The FMC has currently provided completed employee background check documentation for all requested employees to OIG. The Commission has taken steps to ensure that future access to background investigations and screenings records will remain constant by requesting multiple Commission employees be given access and adequate training. The FMC will continue to assess and implement improved recordkeeping processes for employee and contractor screening in FY 2015; and will address each of the above recommendations for compliance with the requirements.

Condition:

Your Internal Controls interviewed key IT personnel and noted the following:

- Although data is being backed up regularly, the backups are not taken off-site as they are maintained at the same premises as the agency. An external vendor has been contracted to pick up the backup tapes weekly, however, the tapes have not been delivered to the external vendor for approximately one year.

Criteria:

NIST 800-53 Revision 4, CP-9 states:
"Protects the confidentiality, integrity, and availability of backup information at storage locations."

Cause:

The cause is primarily because of a congressional hold on providing tapes to external contractors. The cause is also due to a lack of understanding because the congressional hold should not prevent the agency from protecting its data via the backup and storage at an off-site location.

Risk:

Without appropriately maintaining backup data at an external site, the FMC runs the risk that if the primary site has an adverse effect (fire, flood, earthquake, theft, etc.) whereby the data is destroyed, the FMC will likely not be able to restore the data.

Recommendation(s):

5. Take appropriate action to restart providing backup tapes to the external contractor and also test those backups by restoring from tape to ensure the data is available when needed.

Management Response:

FMC has now implemented a new backup architecture that no longer requires tape backups and restores. With this new architecture, all FMC backups will be replicated off-site to a disaster recovery location. The replication takes place in near real time as the backups are completed. OIT expects the off-site replication will be competed in the first quarter of fiscal year 2015. OIT will continue to test restoral capability from on-site backups, and in addition, will institute policies and procedures to test restoral capabilities from the off-site location.

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.	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.	Report A2012-02 (#2)	Closed
3	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.	Report A2012-02 (#5)	Open
4	Implement HSPD-12 in accordance with laws and regulations.	Report A2012-02 (#8)	Open
5	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.	Report A2012-02 (#9)	Closed
6	The Network GSS C&A and the SERVCON C&A should be signed and finalized.	Report A2012-02 (#13)	Closed
7	All controls in the System Security Plans (SSPs) should be reviewed to ensure their implementation status is correct.	Report A2012-02 (#16)	Merged with current year report A15-02 (#1), see page

	POA&M	Report	Open / Closed
8	Any weaknesses as a result of Security Test and Evaluations (STEs) should be corrected immediately.	Report A2012-02 (#17)	Closed
9	The FMC Database (FMCDB) should be carved out into a separate C&A package.	Report A2012-02 (#18)	Closed
10	The SERVCON system should have an e-Authentication assessment conducted.	Report A13-03 (#1)	Closed
11	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)	Closed
12	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)	Closed