Office of Inspector General

Evaluation of the FMC's Compliance with the Federal Information Security Management Act FY 2012

A13-03

December 2012

FEDERAL MARITIME COMMISSION

FEDERAL MARITIME COMMISSION
Washington, DC 20573

December 21, 2012

Office of Inspector General

Dear Chairman Lidinsky and Commissioners:

The Office of Inspector General (OIG) submits its report on the status of information security at the Federal Maritime Commission (FMC) for FY 2012. The OIG relied on the expertise of information security evaluators from *Your Internal Controls LLC,* for assistance on this mandated review.

The objectives of the 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 task included the FMC Network, and applications housing service contracts (SERVCON) tariff location filings (Form-1) and FMC license applications (Form-18). The OIG also performed a network scan to identify potential system vulnerabilities and assessed management actions to implement prior-year recommendations.

The FY 2012 report contains two new subject matter findings and two recommendations for corrective action. Scan results were provided to Office of Information Technology (OIT) network staff as soon as results were know to enable them to make needed adjustments. I am glad to report that no serious vulnerabilities were found.

The OIG thanks FMC staff, especially the OIT, for its assistance in helping us to meet our report objectives.

Respectfully Submitted,

/Adam R. Trzeciak/
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). It 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 (MA). 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 National Institute of Standards and Technology (NIST) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3. 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.

CURRENT YEAR FINDINGS

During our FY 2012 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 increased the size of audit logs and modified the audit log setting to automatically move them to another storage medium in the event that the audit logs become full. Security awareness training has been rolled out satisfactorily and this prior year deficiency is now closed. The FMC also re-categorized one system to comply with Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. Lastly, the agency has finalized Memorandums of Understanding (MOU) between the FMC and external agencies that communicate with FMC systems to ensure that security between them is meeting or exceeding FMC security requirements.

The OIG also found areas where improvement is possible. We identified two deficiencies which we identified in a network scan that pertain to weak server configuration settings and services running on the network that are not secure.

Based on this review, the OIG closed seven (7) recommendations and clarified to management what actions it needs to take to close remaining recommendations. The status of all open recommendations as of the close of fieldwork is identified in Appendix I.

MANAGEMENT RESPONSES AND PRIOR YEAR FOLLOW UP

We have included management's response to the OIG recommendation(s) at the end of the report. The contractor also reviewed the implementation status of 21 prior year(s) unimplemented recommendations. Management has taken steps to close seven (7) of the 21 recommendations, which the OIG verified as completed. The OIG was unable to close the remaining 14 recommendations, due to management's assertion that correct action had not yet occurred.

SYS-01 VULNERABILITY ASSESSMENT RESULTS

Condition:

The contractor performed a Vulnerability Assessment utilizing Nessus, a commercial software tool. This software deployed recent plug-ins, which allowed for the scan to identify the latest vulnerabilities on both the network (servers, routers, firewalls, etc.) and a sample of desktops connected to the network. The last vulnerability scan was conducted in 2009. The results of this scan were as follows:

1. The servers and workstations were not configured with the latest security patches.
2. The network and servers were not configured securely. There were agents and outdated services running that can be exploited.

Criteria:

1. **NIST 800-40 Procedures for Handling Security Patches, section 2.1 states** "We recommend creating a "Patch and Vulnerability Group" (PVG). The size of the PVG will vary depending on the size and complexity of the organization. The PVG may consist of full-or part-time personnel. The personnel involved should have broad knowledge of patches, systems administration, and computer vulnerabilities. In addition, it is helpful to have specialists in particular operating systems, applications, and servers. Personnel who already provide system or network administration functions, perform vulnerability scanning or who operate intrusion detection systems are likely candidates for this group. The duties of the PVG will be to support local administrators in finding and fixing vulnerabilities in the organization's software. The PVG will generally not patch vulnerabilities themselves; rather they will work with a local administrator to apply and test patches. Generally speaking, the main function of the PVG groups should be to ensure consistency across an organization."

2. **NIST 800-123 Guide to General Server Security, section 3.3 states** "Organizations should develop standardized secure configurations for widely used Operating Systems (OS) and server software. This will provide recommendations to server and network administrators on how to configure their systems securely and ensure consistency and compliance with the organizational security policy. Because it only takes one insecurely configured host to compromise a network, organizations with a significant number of hosts are especially encouraged to apply this recommendation." **Section 4.1 states** "Once an OS is installed, applying needed patches or upgrades to correct for known vulnerabilities is essential. Any known vulnerabilities an OS has should be corrected before using it to host a server or otherwise exposing it to untrusted users. To adequately detect and correct these vulnerabilities, server administrators should do the following:

- Create, document, and implement a patching process.
- Identify vulnerabilities and applicable patches.
- Mitigate vulnerabilities temporarily if needed and if feasible (until patches are available, tested, and installed).
- Install permanent fixes (patches, upgrades, etc.)

3. **NIST 800-123 Guide to General Server Security, section 4.2.2 states** "The default configuration of the OS often includes guest accounts (with and without passwords), administrator or root level accounts, and accounts associated with local and network services. The names and passwords for those accounts are well known. Remove (whenever possible) or disable unnecessary accounts to eliminate their use by attackers, including guest accounts on computers containing sensitive information. For default accounts that need to be retained, including guest accounts, severely restrict access to the accounts, including changing the names (where possible and particularly for administrator or root level accounts) and passwords to be consistent with the organizational password policy. Default account names and passwords are commonly known in the attacker community."

4. **NIST 800-123 Guide to General Server Security, section 4.2.2 states** "Enabling authentication by the host computer involves configuring parts of the OS, firmware, and applications on the server, such as the software that implements a network service. In special situations, such as high-value/high-risk servers, organizations may also use authentication hardware, such as tokens or one-time password devices. Use of authentication mechanisms where authentication information is reusable (e.g., passwords) and transmitted in the clear over an untrusted network is strongly discouraged because the information can be intercepted and used by an attacker to masquerade as an authorized user."

Cause:

The FMC network has undergone recent upgrades and there were time constraints placed on limited personnel to identify the latest patches and other vulnerability weaknesses.

Risk:

1. Without updated patches on systems, there is the potential for remote code execution through exploitation of buffer overflows, and other vulnerabilities. Patches are deployed to close those areas subject to exploitation. Without the latest patches being deployed, identified vulnerabilities may be exploited through known attack venues.

2. Hosts (and web servers) running outdated versions may result in a denial of service or other exploitative attacks on the network. Servers and other technologies are built with standard default user IDs and passwords so that administrators can configure them. Attackers know the default user IDs and passwords; as this is common knowledge. It is

therefore, crucial that those default IDs and passwords be changed to prevent exploitation of weak authentication credentials.

Recommendation(s):

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.

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.

PRIOR YEAR RECOMMENDATIONS

The following table details all prior year deficiencies identified during our FISMA evaluation. There are a total of 21 deficiencies identified in the table. Of those 21 deficiencies, seven (7) have been closed in the current audit period. While all of the deficiencies listed below are important, some are clearly a priority and should take precedence with regard to remediation. We've determined that deficiency Nos. 3, 6, 13, and 14 are the most critical and should be remediated as soon as possible.

Deficiency # 3 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.

Deficiency # 6 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.

Deficiency # 13 addresses password complexity. The current password requirements are not appropriate and they should adhere to complexity requirements.

Deficiency # 14 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.

#	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	From the report generated via the Numara software product, identify which patches and service packs can be deployed without harming the network. Further, upon completion, review the configuration settings of the servers to ensure security settings have not changed. (*OIG estimates the required level of effort for this recommendation to be 40 hours).*	Report A2012-02 (#1)	Closed during the FY 2012 FISMA engagement
3	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**
4	Set the audit logs to a size that can sustain the logs being generated. Also, as the logs fill up, they should be moved to another storage medium so that current logs are maintained.	Report A2012-02 (#3)	Closed
5	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)	**Open**
6	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**
7	Ensure that IT personnel are properly trained with regard to incident response prevention, detection, and correction.	Report A2012-02 (#6)	**Open**

#	POA&M	Report	Open / Closed
	(*The estimated level of effort for this recommendation is 40 hours per year for each OIT employee with incident response responsibilities).*		
8	The FMC should implement formal incident response procedures so that in the event of an incident, the appropriate responses could be taken to minimize any adverse impact to the agency. *(OIG estimates the required level of effort for this recommendation to be 20 hours).*	Report A2012-02 (#7)	Closed during the FY 2012 FISMA engagement
9	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**
10	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. • 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**
11	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)	**Open**

#	POA&M	Report	Open / Closed
	(*OIG estimates the required level of effort for this recommendation to be 10 hours).*		
12	Ensure that all agency personnel take Security Awareness Training every year in accordance with NIST 800-50 and comply with IT Security for Personnel MD 2011-4.	Report A2012-02 (#11)	Closed during the FY 2012 FISMA engagement
13	Ensure that password complexity is set to "enable" and applies to all personnel within the FMC agency. *(OIG estimates the level of effort for this recommendation at 4 hours).*	Report A2012-02 (#12)	**Open**
14	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**
15	The Network GSS and SERVCON System Security Plans (SSP) should be signed and finalized. *(OIG estimates the level of effort for this recommendation at 4 hours).*	Report A2012-02 (#14)	Closed during the FY 2012 FISMA engagement
16	The SERVCON FIPS-199 Security Categorization should be a "Moderate" categorization.	Report A2012-02 (#15)	Closed during the FY 2012 FISMA engagement
17	All controls in the 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**
18	Any weaknesses as a result of STEs should be corrected immediately. (*OIG estimates the level of effort for this recommendation at 20 hours).*	Report A2012-02 (#17)	**Open**
19	The 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**

#	POA&M	Report	Open / Closed
20	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**
21	Develop an MOU for all agencies where external personnel access the FMC data.	Report A2012-02 (#20)	Closed during the FY 2012 FISMA engagement

UNITED STATES GOVERNMENT FEDERAL MARITIME COMMISSION

Memorandum

TO : Office of the Inspector General **DATE:** December 7, 2012

FROM : Chief Information Officer

THROUGH: /Managing Director/

SUBJECT : Evaluation of the FMC's Compliance with the Federal Information Security Management Act (FISMA) FY 2012

This is in response to your recently provided FISMA audit draft report.

Recommendation 1. The OIG recommends that OIT 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.

Response: OIT agrees with the findings of the Inspector general and will follow the recommendations set forth in the FY 2012 Evaluation of the FMC's Compliance with the Federal Information System Management Act (FISMA). This is a new finding resulting from OIT not being able to use the Patch Manager software that has worked so well in the past. OIT is currently in the process of identifying a new server patch deployment technology which will be in place by the end of the second quarter of FY 2013.

Recommendation 2. The OIG recommends that OIT 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.

Response: OIT is in the process of identifying all unnecessary services running on the FMC servers and disabling them. Part of this process will be the installation of all of the FMC servers into the Xacta IA Manager continuous monitoring suite that employs the following standards USGCB/SCAP, FIPS 199, NIST 800-37 (Risk Management Framework), NIST 800-53/53A (Security Controls for Federal IS), NIST 800-60 (Guide for Mapping Information Systems to Security Categories) which will be completed by the end of the second quarter of FY 2013.

/Anthony Haywood/