

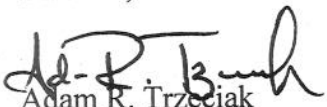


FEDERAL MARITIME COMMISSION
800 North Capitol Street, N.W.
Washington, DC 20573

Memorandum

DATE: January 19, 2007

TO : Stephanie Y. Burwell
Director, Office of Information Technology

FROM : 
Adam R. Trzeciak
Inspector General

SUBJECT: FY 2006 FISMA Follow-up (OR07-01)

The Office of Inspector General has completed its review of (i) the accuracy of the agency's December 1, 2006, Plan of Action & Milestones (POA&M) report to the Office of Management and Budget and (ii) its progress in correcting information security weaknesses identified on the POA&M. Attached for your information and comment is the OIG report communicating our results.

Please provide your written comments to the OIG on or before February 1, 2007. We will attach these comments to the report prior to final issuance. Written comments are optional..

The OIG would like to thank you and your staff for the cooperation we have received during this review. If you have any questions please contact Bridgette Hicks at 523-5863.

cc: Acting Director of Administration
Acting Deputy Director of Administration

Review of FY 2007 POA&M Summary Report and the Status of Corrective Actions

Introduction

The Plan of Action and Milestones (POA&M) is the authoritative and comprehensive agency management mechanism used to prioritize, track and manage all agency efforts to close security performance gaps. In addition to identifying tasks that need to be accomplished, it also details resources required to accomplish the elements of the plan, significant milestones associated with implementing the corrective actions and scheduled completion dates for the milestones. The POA&M is used, in part, as a basis for the Office of Management and Budget's (OMB) assessment of agency information technology (IT) security status as part of the President's Management Agenda Scorecard under the e-Government score.

On December 12, 2006, the Office of Inspector General (OIG) met with Office of Administration (OA) and Office of Information Technology (OIT) staff to (i) evaluate the accuracy of the Federal Maritime Commission's (FMC) December 1, 2006, POA&M submission to OMB and (ii) review OIT's progress in implementing corrective actions to address the vulnerabilities identified on the POA&M.

POA&M Evaluation

The OIG found that the FMC is accurately reporting its POA&M results to OMB. The table below displays the information the agency submitted in its December report to OMB.

Table 1. Agency Report to OMB: POA&M Summary – 1st Quarter of FY 2007

POA&M Summary Table					
	Total number of weaknesses identified at the start of the quarter.	Number of weaknesses for which corrective action was completed (including testing) by the end of the quarter.	Number of weaknesses for which corrective action is ongoing and is on track to be completed as originally scheduled.	Number of weaknesses for which corrective action has been delayed including a brief explanation for the delay.	Number of new weaknesses discovered following the last POA&M update and a brief description of how they were identified (e.g., agency review, IG evaluation, etc.).
FMC Submission	1	0	0	1	10

In our FY 2006 FISMA Report (A06-04, October 2, 2006), the OIG found that the FMC was inaccurately reporting to OMB the results of its POA&M process. Based on this operational review, it appears that the agency has made the necessary changes in its processes to ensure accurate reporting.

POA&M Status

In this section, the OIG summarizes the status of the 11 weaknesses tracked on the POA&M, as identified in Table 1. The OIG identifies the weaknesses, OIG-recommended actions to address the weaknesses, the status of corrective actions and the estimated completion dates. The OIG also validates weaknesses that have been "closed" by OIT to ensure that (i) agreed upon actions were taken and (ii) those actions effectively mitigated the weakness.

The OIG believes that the agency has made substantial progress in prioritizing, tracking, and managing weaknesses and corrective actions. A comprehensive review of FMC's POA&M activities for the first quarter of FY 2007 is presented below.

I. Weakness Identified at the start of the Quarter

Weakness 1. The FORM-1 System needs to be rewritten.

OIG-Recommended Actions in A-11-02:

- *Develop a new version of FORM-1.*

Status: Ongoing – Development of the new FORM-1 system was initiated in December 2006.

Estimated Completion Date: February 28, 2007

Validation: N/A

II. New Weakness Identified Following the Last POA&M Submission

Weakness 1. FMC applications are not certified and accredited.

OIG-Recommended Actions in A06-04:

- *Conduct and document system certifications and accreditations in accordance with NIST SP 800-37.*
- *Develop system security plans in accordance with SP 800-18.*

- *Develop risk assessments in accordance with NIST SP 800-30.*
- *Conduct self-assessments in accordance with NIST SP 800-26.*
- *Categorize systems in accordance with FIPS 199 and NIST SP 800-60.*

Status: Ongoing - OIT reported that the certifications and accreditation (C&A) packages will be conducted internally. The director of OIT informed the OIG that the agency is still on track to complete the required C&A's by March 30, 2007.

Estimated Completion Date: March 30, 2007

Validation: N/A

Weakness 2. FMC lacks documented computer security policies to guide its computer security program.

OIG-Recommended Actions in A06-04:

- *Use the POA&M to schedule completion dates for missing policies.*

Status: Ongoing - OIT reported that as of November 8, 2006, six policies were reviewed and approved by the FMC CIO. These policies address purpose, scope and authority, and contain additional sections to present and clarify the new policies. For example, the policies include information on responsibilities, procedures, exceptions, effective dates and references to relevant guidance. The completed policies are:

- Password Policy OIT-P01
- PDA Policy OIT-P02
- Incident Response OIT-P03
- Inactive Accounts Policy OIT-P04
- File Server Storage Policy OIT-P05
- Electronic Mail Policy OIT-P06

OIT staff told the OIG that additional policies will be completed and finalized by the June 29, 2007, deadline. During the review of OIT's policies the OIG noted that the *Inactive Accounts Policy* did not specify the number of days an account can be inactive before inquiries are made to determine if it should be disabled. This needs to be addressed in the policy.

Estimated Completion Date: June 29, 2007

Validation: N/A

Weakness 3. FMC is not tracking and reporting IT vulnerabilities and corrective actions in accordance with OMB guidance.

OIG-Recommended Actions in A06-04:

- *Complete and maintain the Plan of Action and Milestones (POA&M) in accordance with M-04-25 and M-06-20.*

Status: Completed - OIT reported that the POA&M has been completed and updated in accordance with OMB Memorandums M-04-25 and M-06-20. OIT provided a copy of the POA&M that more closely follows OMB guidance. Review of the POA&M confirmed that:

- Weaknesses are prioritized. Significant deficiencies and reportable conditions are listed ahead of less critical weaknesses.
- Point(s) of Contact were identified for each weakness.
- Each weakness has a scheduled completion date.
- Milestones with completion dates were identified.
- Source of the Finding was identified.
- Action taken is completed when appropriate.
- Status of the effort is reported.

Estimated Completion Date: Completed November 16, 2006.

Validation: The OIG reviewed the POA&M and verified that the identified corrective actions were implemented. Review of the two weaknesses that were addressed indicated that OIT implemented corrective actions on September 27 and November 16, 2006. The OIG and OIT will continue to work together to fine tune the POA&M process.

Weakness 4. FMC contingency plan may be incomplete and needs to be consolidated and tested.

OIG-Recommended Actions in A06-04:

- *Consolidate all documents relevant to the contingency plan in one place. This information should include but not be limited to:*
 - *Contact information for key personnel;*
 - *Contact information for vendors;*
 - *Maintenance agreements;*
 - *Contact information for emergency services;*
 - *System architecture;*
 - *Plans for specific incidents like power outages, hardware failure, fire, and water leakage; and*
 - *Document and test tape restoration procedures.*

- *Test the plan and make adjustments accordingly.*
- *Maintain copies of the contingency plan at the alternate sites.*

Status: Ongoing - OIT plans to issue a proposal to develop the contingency plan by early January, 2007. OIT also reported that it plans to meet the July 31, 2007, completion date for developing and implementing the contingency plan.

Estimated Completion Date: July 31, 2007

Validation: N/A

Weakness 5. FMC backup servers may not be secure.

OIG-Recommended Actions in A06-04:

- *Establish documented scan and patch management policies.*
- *Scan and patch systems at least quarterly.*
- *Establish a MOU/SLA with the vendor to identify roles and responsibilities.*

Status: Ongoing – This recommendation remains ongoing due to an MOU/SLA that has not been finalized between FMC and the vendor housing the back-up server. However, the OIT completed the corrective actions for establishing documented scan and patch management policies and purchasing the patch management software on September 27, 2006. The FMC has also begun conducting scans and applying patches quarterly.

Estimated Completion Date: September 27, 2007

Validation: OIT provided a QualysGuard scan reports from August 8, 2006, and December 27, 2006. OIT also provided a copy of the executive summary patch report.

Weakness 6. Personnel, operational and technical control deficiencies exist that could affect the security of SERVCON and the FMC Network.

OIG-Recommended Actions in A06-04:

- *Require FMC employees and contractors to sign rules of behavior and nondisclosure statements.*
- *Evaluate the cost/benefit of implementing an IDS to monitor network activity and alert appropriate OIT personnel of suspicious activity.*
- *Procure scanning software and run scans at least semi-annually.*

Status: Ongoing – QualysGuard scan software was purchased on August 3, 2006, and scans are now run quarterly. OIT is currently working on obtaining signed rules of behavior and nondisclosure statements from staff.

Estimated Completion Date: OIT reported that it expects to meet the September 30, 2007, completion date. Corrective actions for this weakness require Commission approval.

Validation: N/A

Weakness 7. Access control policies are not documented and technical access controls are not always implemented.

OIG-Recommended Actions in A06-04:

- *Document and finalize policies and procedures that address password development guidelines, remote access requests, audit logging, wireless, and other related areas.*
- *Develop a formal sanctions process for personnel failing to comply with established information security policies and procedures.*
- *Implement password protection for Blackberries.*
- *Evaluate the cost-effectiveness of purchasing and implementing Internet tracking software.*

Status: Ongoing - Responsibility for these corrective actions lies with OIT, but policies must be approved by the Commission. Notwithstanding, OIT anticipates meeting the proposed September 30 completion date.

Password protection for “BlackBerries” was implemented on January 8, 2007.

Estimated Completion Date: September 30, 2007

Validation: N/A

Weakness 8. FMC’s security awareness training course should be updated.

OIG-Recommended Actions in A06-04:

- *Update the online security awareness training course to address new security topics.*
- *Update training to include additional guidance to make passwords more secure.*
- *Implement password controls in the system that will enforce good password structure to include upper/lower case letters, numbers, special characters, and specific length.*
- *Develop sanctions for not taking training. For example, accounts of personnel who do not take training should be locked until training has been completed.*

Status: Ongoing - The Information Security Officer is currently working on the content of the IT Security Awareness course. OIT anticipates no delays or changes to the scheduled completion date at this time.

Estimated Completion Date: September 30, 2007

Validation: N/A

Weakness 9. The roles and responsibilities of Senior Agency Officials for Privacy are not clearly defined.

OIG-Recommended Actions in A06-04:

- *Update Commission Order 89 to document privacy responsibilities for senior privacy officials.*

Status: Ongoing – Currently, the FMC does not have an appointed Chairman. Further, other key positions, to include the Director of Administration, the Deputy Director of Administration and the Chief Information Officer, are occupied by temporarily-assigned staff. Documenting the responsibilities of the Senior Agency Official for Privacy will not be addressed until the permanent replacements are made for these positions. OIT does not anticipate changes to the completion date at this time.

Estimated Completion Date: March 30, 2007

Validation: N/A

Weakness 10. COOP site breach.

OIG-Recommended Actions in A06-04:

- *Develop SLA between FMC and the vendor and replace COOP e-mail system.*

Status: Ongoing - OIT was able to address and complete action on repairing the security breach. FMC is currently working with the vendor on developing a Service Level Agreement (SLA). Completion of task is dependent on the actions of the vendor.

Estimated Completion Date: To be determined

Validation: N/A