



FEDERAL MARITIME COMMISSION

800 North Capitol Street, N.W.
Washington, DC 20573

October 2, 2006

Office of Inspector General

Chairman Blust;

The Office of Inspector General has completed its independent evaluation of information security pursuant to requirements contained in the Federal Information Security Management Act (FISMA) of 2002. This is the fourth annual evaluation completed by the OIG in the area of information and computer security.

This year's review objectives were to assess compliance with FISMA and related information security policies, procedures, standards and guidelines, and to test their effectiveness on a representative subset of the agency's information systems. Specifically, this review (i) evaluated the implementation of the Federal Maritime Commission's (FMC) information security program; (ii) assessed agency progress towards correcting weaknesses addressed in the FY 2006 Plan of Actions & Milestones (POA&M); (iii) verified and tested information security and access controls for the FMC network and wireless tools; and (iv) scanned the internal network for security weaknesses.

The FMC continues to make progress in developing its information security program and has implemented or addressed past security vulnerabilities identified by the OIG. FMC has taken a number of steps to secure its systems and personnel. The organization established physical security controls that restrict access to FMC controlled areas including the Data Center. FMC established safe rooms throughout its facility to protect personnel from various security incidents. The agency has documented backup procedures and stores backups at various offsite locations. FMC has also established a "hot site" that should keep critical systems functioning in the event that the primary Data Center is destroyed or damaged. Finally, FMC implemented an online security awareness training program to promote security awareness among FMC personnel.

The FMC has also taken steps to ensure privacy and protection of personally identifiable information. The FMC appointed a Privacy Officer and has posted its privacy policy on its website. Recently the agency completed a thorough review of employee-initiated forms to identify and revise outdated forms that request employee Social Security Numbers even though it is not needed to process the transaction.

Although progress has been made, the OIG identified areas where some improvements are needed. The agency lacks documented information security policies. These form the backbone of any risk-based security program. The Certification and Accreditation (C&A) packages do not contain sufficient detail for the CIO or system owner to make valid, risk-based decisions on whether to place FMC systems into production. Complete C&A packages provide sufficient information to evaluate the vulnerabilities, safeguards, and risks associated with operating the systems in a production environment. Finally, the agency is not adequately

tracking its IT vulnerabilities to ensure that they are properly addressed and closed. These and other IT security-related findings are fully discussed in the attached report.

Changing security needs and requirements present challenges to most IT operations. Budgets for information security must compete with operations (new equipment, faster servers, larger storage, etc.) and often take a back seat. Operational needs are much more visible and tangibly impact all employees daily. Unfortunately, as we've witnessed recent breaches at many federal agencies, few events are more disruptive and more costly than computer security incidents that put the public we serve at some risk.

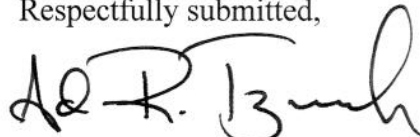
The OIG has identified areas where the agency fails to meet federally mandated standards. Vulnerabilities cannot be addressed if they are not identified. We have noted areas where more must be done to identify our risks and vulnerabilities. Then we must prioritize and track progress toward addressing them. We are not suggesting that we tackle everything at once. Rather, we should identify what is important and focus our energies on those areas initially. If more resources are required to address our vulnerabilities, then this needs to be identified as well.

Given our size and resources, the Office of Information Technology (OIT) has implemented baseline controls to ensure the security of our information systems. One could argue that the FMC is a low risk for intrusion. Therefore basic security, given competing demands on shrinking budgets, is the most effective use of our resources. However, given recent breaches at our "hot site," this view is less supportable.

The bottom line is that all federal agencies have some vulnerabilities. OMB recognizes this and is asking agencies to implement a security program that identifies them and lays out a plan to address (reduce, eliminate or accept) them based on acceptable levels of risk. The OIG believes that the best security program recognizes that risks are out there and lays out a plan to identify and address them. A good program is not one that says, "we have no problems."

The OIG performed this evaluation from May 25, 2006 through August 15, 2006, and followed National Institute of Science and Technology guidance for information systems, OMB Memorandum M-06-20, *Reporting Instructions for the Federal Information Security Management Act* (July 17, 2006) and best practices used in the industry. The OIG thanks OIT management and staff for its help and cooperation during our review.

Respectfully submitted,



Adam R. Trzeciak
Inspector General

* Note: The FY 2006 FISMA report is available in its entirety by emailing the OIG at OIG@FMC.GOV. An electronic copy will be forwarded to you.