

Semiannual Report To the Congress

**Covering the Period
April 1, 2006 to September 30, 2006**





FEDERAL MARITIME COMMISSION
Office of the Inspector General
Washington, DC 20573-0001

Office of Inspector General

Tel.: (202) 523-5863
Fax: (202) 566-0043
E-mail: oig@fmc.gov

Honorable Steven R. Blust
Chairman
Federal Maritime Commission
Washington, DC 20573

Chairman Blust:

The attached report is submitted in accordance with Section 5 of the Inspector General Act of 1978, as amended by the Inspector General Act amendments of 1988. It summarizes the activities of the Office for the period April 1, 2006 to September 30, 2006. The Act requires that you transmit the report to the appropriate committees of the Congress within 30 days of receipt. Your transmittal should also include any comments you consider appropriate and other statistical tables and reports required by law.

During this period the OIG issued four reports to the Commission and/or senior staff and one IT network scan which was provided, for security purposes, directly to the Chief Information Officer (CIO) and the information security officer. The office also began fieldwork on the Commission's annual financial statement audit.

Also during the period, the OIG received one hotline complaint from a member of the shipping industry and two referrals from FMC management regarding misconduct. The OIG opened three investigations into the allegations and closed two of them by the end of the period. One investigation was still ongoing as of the end of the reporting period.

OIG staff was also involved in other OIG mission-related activities during the period. The inspector general co-lead a symposium on IG information security reviews under the Federal Information Security Management Act attended by representatives of the CIO Council and small agency IG's. The purpose of this symposium was to assist both groups to perform more meaningful and helpful evaluations of their respective information security programs. We provided written and oral comments to a draft OMB circular on financial statement audits, redesigned the OIG web page to make it more useful and easier for the public and FMC staff to navigate and began preparations for a peer review, by a sister OIG, of our quality control program.

Inspector General's Semiannual Report to Congress

As in the past, management has been responsive in attempting to implement all OIG recommendations. I appreciate management's support and I look forward to working with you in our ongoing efforts to promote economy and efficiency in agency programs.



Adam R. Trzeciak
Inspector General

October 25, 2006

TABLE OF CONTENTS

Transmittal Letter	
Executive Summary	1
Background	1
Audits/Evaluations	3
Audit of Payroll Processing Transactions	3
Review of Privacy Data on Leave Request Forms	4
Review of FMC's Implementation of the Federal Information Security Management Act for FY 2006	5
FISMA Independent Evaluation and Privacy Act Implementation: OMB Submission	6
Investigative Activities	6
Other OIG Activities	7
Summary of Inspector General's Reporting Requirements	11
Table I. IG Issued Reports with Questioned Costs	12
Table II. IG Issued Reports with Recommendations That Funds Put to Better Use	13

EXECUTIVE SUMMARY

This Semiannual Report to the Congress summarizes the activities and accomplishments of the Federal Maritime Commission (FMC or Commission), Office of Inspector General (OIG) for the period April 1, 2006 through September 30, 2006. During this period we issued four reports to the Commission and one IT network scan which was provided, for security purposes, directly to the Chief Information Officer (CIO) and the information security officer. The office also began fieldwork on the Commission's annual financial statement audit. During the period, the OIG opened three investigations and co-lead a symposium on IG information security reviews under the Federal Information Security Management Act (FISMA) attended by representatives of the CIO Council and small agency IG's. Finally, we provided written and oral comments to a proposed Office of Management and Budget (OMB) circular on financial statement audits and redesigned the OIG web page to make it more useful and easier for the public and FMC staff to navigate. Details on these and other activities are provided below.

BACKGROUND

The FMC is an independent agency responsible for the regulation of oceanborne transportation in the foreign commerce of the United States. The principal statutes or statutory provisions administered by the Commission are the Shipping Act of 1984, as amended by the Ocean Shipping Reform Act of 1998; the Foreign Shipping Practices Act of 1988; and Section 19 of the Merchant Marine Act of 1920.

The FMC is headed by five Commissioners nominated by the President and confirmed by the Senate, each serving five-year terms. The President designates one of the Commissioners to serve as the Chairman. The Chairman is the chief executive and administrative officer of the Commission.

In Fiscal Year (FY) 2006, the Commission was authorized a total of 126 full-time equivalent positions with a total appropriation of \$20,294,010. Although the majority of the Commission's personnel are located in Washington, DC., the Commission also maintains a presence in Los Angeles, South Florida, Seattle/Tacoma, New York and New Orleans through area representatives who serve the major ports and transportation centers within their respective geographic areas. In addition, two at-large area representatives operate out of Washington, DC.

The FMC's Office of Inspector General (OIG) was established in 1989 as required by the Inspector General Act Amendments of 1988 (5 U.S.C. app.). The OIG is an independent audit and investigative unit headed by an Inspector General (IG) who reports directly to the Chairman of the FMC.

The OIG is responsible for conducting audits and investigations relating to the programs and operations of the FMC. Audits are conducted for the purpose of finding and preventing fraud, waste and abuse and to promote economy, efficiency and effectiveness within the agency. OIG investigations seek out facts related to allegations of wrongdoing on the part of FMC employees and individuals or entities having contracts with or obtaining benefits from the agency. The Inspector General Act provides that the OIG shall have access to all agency records and may subpoena records from entities outside of the agency in connection with an audit or investigation.

The OIG is required by law to prepare a semiannual report summarizing its audits and investigations during the immediately preceding six-month period. The report is sent to the FMC Chairman, the President of the Senate, the Speaker of the House and FMC's appropriating and authorizing committees. This dual reporting requirement facilitates and ensures the independence of the Office.

AUDITS/EVALUATIONS

During this semiannual period, the OIG issued an audit of the controls in place to ensure the accuracy of employee annual and sick leave balances and the efficiency, effectiveness and security of key time and attendance processes. We also issued an operational review (OR) of the agency's collection of social security numbers and our annual security evaluation of the agency's implementation of the Federal Information Security Management Act.

Completed Audits

<u>Audit Report Number</u>	<u>Subject of Audit</u>
A06-02	Audit of Payroll Processing Transactions
OR06-01	Review of Privacy Data on Leave Request Forms
A06-04	Review of FMC's Implementation of the Federal Information Security Management Act for FY 2006
A06-04A	FISMA Independent Evaluation and Privacy Act Implementation: OMB Submission

Summary of Audits Issued During the Current Period

In A06-02, *Audit of Payroll Processing Transactions*, the objective was to assess controls in place to ensure the accuracy of employee sick and annual leave balances and to assess procedures to protect select employee privacy data. This audit followed up on payroll-related findings developed in the OIG's FY 2005 Financial Statement Audit. Specifically, the OIG found several reconciliation errors between employee *Leave and Earnings Statements* generated by the National Finance Center (NFC) and FMC internal systems. Payroll-related errors can impact either employee or agency finances, depending on the direction and magnitude of the errors. While controls are in place, we found instances of noncompliance which permitted leave balance

errors to occur and persist. Further, actions taken by management to address leave balance inaccuracies were ineffective. For example, errors persist even after guidance to correct these errors was issued by management months earlier. The OIG believes that additional steps need to be taken to correct reporting errors and to strengthen controls to ensure that future errors are minimized and are identified timely.

We also noted several inconsistencies among timekeepers regarding the recording of payroll data, the extent to which documentation is maintained and secured and whether FMC policies and procedures are followed and/or enforced. To correct most of the deficiencies, the OIG believes that management should provide specific/targeted training to timekeepers that addresses the noted deficiencies. Management should also proactively ensure the accuracy of leave balances by running error reports which identify discrepancies in leave balances.

Management agreed with the OIG recommendations and has taken steps to correct the observed deficiencies.

In OR06-03, *Review of Privacy Data on Leave Request Forms*, the objective was to identify instances where employee social security numbers (SSN) were requested on government-wide or agency-specific forms but were not used or needed to process the transaction. For example, 64 percent of leave slips we sampled contained the employee's SSN even though it was not used by timekeepers to record the leave. The form, *Request for Leave and Approved Absence* (OPM Form 71), was last revised in June, 2001. While this information may be necessary at some larger Federal agencies to process leave requests, FMC timekeepers told the OIG it was unnecessary at our agency. This practice needlessly exposed FMC employees to identity theft (should this information fall into the wrong hands).

The OIG believes that employees provided information requested because they believed it to be required. The OIG recommended that the leave slips, which are completed on line and available on the agency's intranet, be revised to block out the request for SSN's. We also recommended

that the agency review all other forms used by the agency (e.g., training forms, travel documents, etc.) to identify instances where SSN's are collected but not used to process the specific transaction.

The agency took immediate steps to address this vulnerability. Within two weeks, it completed its review of all agency forms requiring an SSN and determined that seven forms in all were needlessly collecting the employee's SSN. All forms were amended to exclude this information and staff were alerted to this change.

In A06-04, *Review of FMC's Implementation of the Federal Information Security Management Act for FY 2006*, the 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 FMC's 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. The FMC has taken a number of steps to secure its systems and personnel. The agency established physical security controls that restrict access to FMC-controlled areas including the Data Center. The FMC established safe rooms throughout its office space 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 posted its privacy policy on its website. As stated above, the agency completed a thorough review of employee-initiated forms to identify and revise outdated forms that request an employee's SSN even though it is not needed to process the transaction.

Although progress has been made, the OIG identified areas where 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.

The OIG also identified some technical vulnerabilities on servers inside the FMC network. These findings were presented to the agency's information security officer in a separate report. Most were addressed within days of the OIG's internal scan.

In A06-04A, *FISMA Independent Evaluation and Privacy Act Implementation: OMB Submission*, the OIG responded to OMB requirements to report on select performance measures concerning the FMC's information security program and to validate select agency self-reported responses to information security metrics. The OIG reported no discrepancies between the OIG submission and that of the agency's CIO.

INVESTIGATIVE ACTIVITIES

The Inspector General Act of 1978, as amended, provides that the IG may receive and investigate complaints or information concerning the possible allegations of fraud, waste and abuse

occurring within FMC programs and operations. Matters of possible wrongdoing are referred to the OIG in the form of allegations or complaints from a variety of sources, including FMC employees, other government agencies and the general public.

During this reporting period, the OIG opened three preliminary investigations into possible wrongdoing or abuse of authority. Two of the complaints were made by FMC staff to the OIG and one was made by a member of the shipping industry. As of the end of the reporting period, two of these preliminary investigations were closed. The OIG is continuing to collect evidence on the remaining preliminary investigation to determine whether to open a formal investigation. The OIG also received other complaints that were more appropriately addressed by FMC enforcement staff or other sister agencies. Consequently, the OIG referred these complaints to these organizations for disposition.

The OIG referred no matters to prosecutorial authorities during the period.

OTHER OIG ACTIVITIES

Review of Legislation

As required by the Inspector General Act of 1978, as amended, the Office of Inspector General routinely reviews proposed legislation and regulations. The purpose of these reviews is to assess whether the proposed legislation or regulation (1) impacts on the economy and efficiency of FMC programs and operations, and (2) contains adequate internal controls to prevent and detect fraud and abuse.

During this period, a number of legislative proposals as well as Commission Orders/policy guidelines were reviewed by this Office. On one proposed regulation, OIG staff provided both verbal and written comments to an OMB circular update on audit requirements for federal financial statements.

Executive Council on Integrity and Efficiency Activities

The Executive Council on Integrity and Efficiency (ECIE) was established by Executive Order 12805 on May 11, 1992, to:

- address integrity, economy, and effectiveness issues that transcend individual government agencies, and
- enhance the professionalism and effectiveness of IG personnel throughout the government.

To accomplish its mission, the ECIE members participate in interagency and inter-entity audit, inspection and investigation projects to promote economy and efficiency in Federal programs and operations and address more effectively government-wide issues of fraud, waste, and abuse. The Council members also develop policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled IG workforce.

During the reporting period, the inspector general teamed with the CIO at the Federal Trade Commission to lead a discussion on “lessons learned” after five years of information security legislation. The symposium’s objective was to assist the information security and OIG communities to prepare for the annual Federal Information Security Management Act evaluation (for FY 2006) by discussing common weaknesses, problems and shortcomings of past evaluations and to move forward to provide agency heads, Congress, OMB and the public with meaningful and helpful assessments. Concerns regarding how OIG’s review information security programs and CIO implementation of OMB-required controls were discussed.

The inspector general and assistant inspector general continued to serve on the Executive Council on Integrity and Efficiency and Federal Audit Executive Council (FAEC). The ECIE serves as a forum for the exchange of views for the inspector general community and provides a base for the establishment of joint inspector general projects. The FAEC is comprised of senior audit staff who discuss and coordinate issues affecting the Federal audit community with special emphasis on audit policy and operations of common interest to FAEC members.

Peer Review Activities

Federal Offices of Inspector General are required by the IG Act to have a peer review performed on their organization once every three years. These reviews are to be performed only by Federal auditors. A committee of the ECIE schedules the review to ensure that resources are available to perform them and that OIG's do not conduct reciprocal reviews.

Against this background, the FMC/OIG is scheduled to be reviewed by the inspector general from the National Credit Union Association in October, 2006. The objectives of a peer review are to determine for the audit function whether an effective quality control system has been established in the office and if policies, procedures and applicable government auditing standards are being followed. The OIG is collecting the required documentation for the review and is responding to an ECIE questionnaire regarding quality assurance procedures in the office.

Significant Management Decisions

Section 5(a)(12) of the Inspector General Act requires that if the IG disagrees with any significant management decision, such disagreement must be reported in the semiannual report. Further, Section 5(a)(11) of the Act requires that any decision by management to change its response to a significant resolved audit finding must also be disclosed in the semiannual report. For this reporting period, there were no significant management decisions made on which the IG disagreed and management did not revise an earlier decision on an OIG audit recommendation.

Access to Information

The IG is to be provided with ready access to all agency records, information or assistance when conducting an investigation or audit. Section 6(b)(2) of the IG Act requires the IG to report to the agency head, without delay, if the IG believes that access to required information, records or assistance has been unreasonably refused, or otherwise has not been provided. A summary of each report submitted to the agency head in compliance with Section 6(b)(2) must be provided in the semiannual report in accordance with Section 5(a)(5) of the Act.

During the reporting period, the OIG did not encounter any difficulties in obtaining assistance or access to agency records. Consequently, no report was issued by the IG to the agency head in accordance with Section 6(b)(2) of the IG Act.

Audit Resolution

As of the end of this reporting period, all OIG audit recommendations for reports issued in prior periods have been resolved. That is, management and the OIG have reached agreement on what actions need to be taken.

Contacting the Office of Inspector General

Employees and the public are encouraged to contact the OIG regarding any incidents of possible waste, fraud or abuse occurring within FMC programs and operations. The OIG telephone number is **(202) 523-5863**. To report suspected wrongdoing, employees or the public may call the OIG Hotline on **(202) 523-5865**. A confidential or anonymous message can be left 24 hours a day. Complaints or allegations of fraud, waste or abuse can also be emailed to OIG@FMC.GOV.

SUMMARY OF INSPECTOR GENERAL'S REPORTING REQUIREMENTS

IG Act Reference	Reporting Requirement	Page(s)
Section 4(a)(2)	Review of legislation and regulations	7
Section 5(a)(1)	Significant problems, abuses and deficiencies	None
Section 5(a)(3)	Prior significant recommendations on which corrective actions have not been made	10
Section 5(a)(4)	Matters referred to prosecutive authorities	7
Section 5(a)(5)	Summary of instances where information was refused	9
Section 5(a)(6)	List of audit reports by subject matter, showing dollar value of questioned costs and funds put to better use	12-13
Section 5(a)(7)	Summary of each particularly significant report	3 - 6
Section 5(a)(8)	Statistical tables showing number of reports and dollar value of questioned costs	12
Section 5(a)(9)	Statistical tables showing number of reports and dollar value of recommendations that funds be put to better use	13
Section 5(a)(10)	Summary of each audit issued before this reporting period for which no management decision was made by the end of the reporting period	12-13
Section 5(a)(11)	Significant revised management decisions	9
Section 5(a)(12)	Significant management decisions with which the inspector general disagrees	9

TABLE I
INSPECTOR GENERAL ISSUED REPORTS
WITH QUESTIONED COSTS

	<u>Dollar Value</u>		
	<u>Number</u>	<u>Questioned Cost</u>	<u>Unsupported Costs</u>
A. For which no management decision has been made by the commencement of the reporting period	0	0	0
B. Which were issued during the reporting period?	0	0	0
Subtotal (A + B)	0	0	0
C. For which a management decision was made during the reporting period	0	0	0
(i) dollar value of disallowed costs	0	0	0
(ii) dollar value of costs not disallowed	0	0	0
D. For which no management decision has been made by the end of the reporting period	0	0	0
E. Reports for which no management decision was made within six months of issuance	0	0	0

TABLE II
INSPECTOR GENERAL ISSUED REPORTS
WITH RECOMMENDATIONS
THAT FUNDS BE PUT TO BETTER USE

	<u>Number</u>	<u>Dollar Value</u>
A. For which no management decision has been made by the commencement of the reporting period	0	0
B. Which were issued during the reporting period	0	0
Subtotal (A plus B)	0	0
C. For which a management decision was made during the reporting period	0	0
(i) dollar value of recommendations that were agreed to by management	0	0
(ii) dollar value of recommendations that were not agreed to by management	0	0
D. For which no management decision has been made by the end of the reporting period	0	0
Reports for which no management decision was made within six months of issuance	0	0

HOTLINE COMPLAINTS

The success of the OIG mission to prevent fraud, waste and abuse depends on the cooperation of FMC employees and the public.

A COMPLAINT CAN BE REPORTED BY CALLING OUR 24-HR DIRECT LINE

(202) 523-5865

E-MAIL ADDRESS:

oig@fmc.gov

TO PLACE A COMPLAINT IN WRITING PLEASE MAIL TO:

**Federal Maritime Commission
Office of Inspector General
Room 1054
800 North Capitol Street, NW
Washington, DC 20573**

To Be Opened By the IG Only

THE INFORMATION YOU PROVIDE IS CONFIDENTIAL AND YOU CAN BE ANONYMOUS

**HOWEVER, EACH CALLER IS ENCOURAGED TO ASSIST THE INSPECTOR GENERAL BY
SUPPLYING INFORMATION AS TO HOW THEY MAY BE CONTACTED FOR ADDITIONAL INFORMATION**