FEDERAL TRADE COMMISSION

OFFICE OF INSPECTOR GENERAL

SEMIANNUAL REPORT TO CONGRESS

April 1, 2006 - September 30, 2006

Report #35

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of Inspector General

October 20, 2006

The Honorable Deborah Majoras
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Dear Chairman Majoras:

The attached report covers the Office of Inspector General's (OIG) activities for the second half of fiscal year 2006 and is submitted pursuant to Section 5 of the Inspector General Act of 1978, as amended.

During the six-month reporting period ending September 30, 2006, the OIG issued an audit of the FTC's Implementation of the Federal Information Security Act for FY 2006. The OIG also issued two management advisories.

In addition, the OIG processed 52 consumer inquiries and complaints/allegations of possible wrongdoing during the period, opened three new investigations into wrongdoing, and closed six investigations. The results of these closed investigations were reported to management for ultimate disposition.

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.

Sincerely,

Howard L. Sribnick
Inspector General

INTRODUCTION

The Federal Trade Commission (FTC) seeks to assure that the nation's markets are competitive, efficient and free from undue restrictions. The FTC also seeks to improve the operation of the marketplace by combating unfair and deceptive practices, with emphasis on those practices that might unreasonably restrict the free exercise of informed choice by consumers. The FTC relies on economic analysis to support its law enforcement efforts and to contribute to the economic policy deliberations of Congress, the Executive Branch and the public.

To aid the FTC in accomplishing its consumer protection and antitrust missions, the Office of Inspector General (OIG) was provided five work years and a budget of $917,500 for fiscal year 2006.

AUDITS

AR-06-73 Review of FTC Implementation of the Federal Information Security Management Act (FISMA)

The OIG completed a review of Federal Trade Commission Implementation of the Federal Information Security Management Act during fiscal year 2006.[1]

The OIG found that FTC's Office of Information and Technology Management (ITM) continues to make progress in developing a mature information security program and has implemented or addressed OIG-identified security vulnerabilities discussed in previous independent evaluation reports and other security reviews.

Notwithstanding the progress made by the FTC, the OIG identified weaknesses and vulnerabilities that merit management's attention. The more important findings include:

- FTC's Disaster Recovery Plan (DRP) needs further development. The identified alternate sites at 601 New Jersey Avenue and the East Central Regional Office (ECRO) do not have sufficient space, power, or HVAC capability to function as a backup site for the FTC, if the main data centers were disabled. Additionally, there was no evidence that memoranda of understanding (MOU), service level agreements (SLA), or agreements with the General Services Agency (GSA) are in place to provide the extra resources needed at ECRO.

[1] As part of its review the OIG conducted an internal scan of the FTC network environment. The results of the scan were reported to the agency under a separate non-public document.

- FTC has contracted with ICF Consulting (ICF) for the use of Commentworks[SM] software to receive and process comments from the public on proposed regulatory action. The FISMA review found that FTC managers responsible for CommentWorks[SM] are not notified when FTC employees leave the organization or are transferred within the organization and no longer need access to the system. Additionally, the review discovered that there is no contingency plan for ICF or CommentWorks[SM] in the event of a discontinuance of service.

- Policies, procedures and related security documentation for the FTC's Internet Lab either do not exist or are not documented.[2] There are no documented policies, procedures or forms for requesting, approving or creating/removing user accounts for the Internet Lab. OIG was also advised that user ID's and passwords are not required for users to log onto and access Internet Lab workstations. There are no documented maintenance procedures. Backups are not conducted at this time; however, raw data is archived.

- The East Central Regional Office may take longer to recover from an incident since they do not have a contingency plan. All regional offices rely on Headquarters for contingency planning and disaster recovery. The FTC DRP and Continuity of Government kit do not address recovery of regional offices.

MANAGEMENT ADVISORIES

MA-06-12 Vulnerabilities Pertaining to Oversight of Receiver

The OIG completed analysis of FTC's practices and procedures for recommending and monitoring receivers appointed in consumer fraud cases. The OIG found that there was no centralized repository for information regarding the qualifications of potential receivers, there was no procedure in place to assure that potential receivers had not in the past been disciplined in connection with the performance of their fiduciary obligations, and that monitoring of receivers' performance was left to the court (which, in many cases, did not enforce reporting requirements included in the order establishing the receivership). The OIG recommended that the agency centralize the maintenance of information gathered on potential receivers, require that potential receivers attest that they had not been the subject of prior disciplinary action, and implement procedures to allow the agency to more closely monitor the work of receivers. Management has agreed with the recommendations included in this advisory and is in the process of taking actions to complete implementation.

MA-06-14 Improved Oversight of FTC Travel Card Program

---

[2] The Internet Lab is an internal bank of computers that are not connected to the agency's network and whose gateway to the internet cannot be traced back to the FTC's IP address. The Lab is used by agency staff to conduct law enforcement investigations.

The OIG completed an examination of controls relating to FTC travel credit card program. The OIG found a number of areas of employee abuse of the travel credit card program including charging personal expenses not related to government travel, taking cash advances for personal use and not paying off the balance owed on the credit card in a timely manner. The OIG also found that the agency was usually unaware of employee misuse of travel credit cards until notified by the card issuer that the employee's charge privileges were about to be suspended or cancelled. The OIG recommended a number of improvements to management controls over this program. In response to these recommendations, management undertook action including: routine screening of employee charges on FTC issued travel credit cards; requiring that holders of travel credit cards sign a notice and attestation demonstrating that they are aware that charges may only be made for approved purchases while on official travel and that balances owed must be paid in a timely manner and the hiring of a new manager to monitor the program. In the view of the OIG, these actions will significantly improve the integrity of this program.

PLANNED AUDITS AND REVIEWS

Audit of the FTC's Financial Statements for Fiscal Year 2006

The purpose of the audit is to express an opinion on the financial statements of the Federal Trade Commission for the fiscal year ending September 30, 2006. The principal statements to be audited include the (a) Balance Sheet; (b) Statement of Net Cost; (c) Statement of Changes in Net Position; (d) Statement of Budgetary Resources; (e) Statement of Financing; (f) Statement of Custodial Activity and notes to the financial statements. The OIG will also test the internal controls associated with the movement of transactions through the FTC's financial system and assess compliance with selected laws and regulations.

The OIG is using guidance contained in OMB Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements*, in performing this audit. The audited financial statements are required to be included in the financial section of the agency's Performance and Accountability Report to be issued on or before November 15, 2006.

Review of the Federal Trade Commission Purchase Card Program

The objective of this audit will be to assess internal controls over the government purchase card program. Specific audit objectives will be to (i) document controls; (ii) determine the functioning of processes and procedures; and (iii) assess areas that could be strengthened to better ensure that the goals of the program are achieved.

Audit of the Operations of the Redress Office of the Bureau of Consumer Protection

The scope of the audit includes how the program is managed, how well tracking and reporting responsibility is performed, the status of implementation of OIG recommendations regarding the appointment of receivers and tests of internal controls.

Review of the Consumer Response Center

The scope of the review includes how CRC classifies complaints and inquiries for assistance, how responsive the CRC is to meeting consumer complaints including the accuracy of recording information into the database , how "user friendly" is the CRC reporting system and how well personally identifiable information is protected.

INVESTIGATIVE ACTIVITIES

The Inspector General is authorized by the IG Act to receive and investigate allegations of fraud, waste and abuse occurring within FTC 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 FTC employees, other government agencies and the general public.

Reported incidents of possible fraud, waste and abuse can give rise to administrative, civil or criminal investigations. OIG investigations are also initiated when there is an indication that firms or individuals are involved in activities intended to improperly affect the outcome of particular agency enforcement actions. Because this kind of wrongdoing strikes at the integrity of the FTC's consumer protection and antitrust law enforcement missions, the OIG places a high priority on these investigations.

In conducting criminal investigations during the past several years, the OIG has sought assistance from, and worked jointly with, other law enforcement agencies, including other OIG's, the Federal Bureau of Investigation, U.S. Postal Inspection Service, U.S. Secret Service, U.S. Marshal's Service, Internal Revenue Service, Capitol Police, Federal Protective Service as well as state agencies and local police departments.

Investigative Summary

During this reporting period, the OIG received 52 consumer and other inquiries and reports of possible wrongdoing. Of the 52 complaints, 21 involved issues that fall under the jurisdiction of FTC program components (identity theft, credit repair, etc.). Consequently, the OIG referred these matters to the appropriate FTC component for disposition.

Of the remaining complaints, the OIG opened 3 new investigations. The OIG offered some assistance to other OIG's or law enforcement organizations in conducting ongoing investigations respecting 3 inquiries. Another five complaints remained ongoing at the end of the reporting period. Finally, the OIG closed the 20 remaining complaints without any further action.

Following is a summary of the OIG's investigative activities for the six-month period ending March 31, 2006:

Cases pending as of 3/31/06	**3**
PLUS: New cases	**3**
LESS: Cases closed	**(6)**
Cases pending as of 9/30/06	**0**

Investigations Closed

The OIG closed the following six investigations during this reporting period:

The OIG closed a file, opened during a prior reporting period, involving misuse of a Government-issued travel card. The investigation stemmed from the agency's ongoing monitoring of employee use of Government-issued credit cards, as previously reported. The investigative referral to agency management detailed personal travel card transactions totaling thousands of dollars and spanning more than a year. The matter was referred to management and disciplinary action is pending.

The OIG continued investigative work on two computer misuse matters opened during a prior reporting period and opened a new computer misuse investigation. Investigative work on all three matters was completed during this reporting period and the investigative files were closed.

The first computer misuse investigation arose from the agency's ongoing monitoring of employee usage of the internet. The referral alleged that an employee in the agency's information technology program office allegedly installed a software program from an internet website that enables users to downloaded illegal software license keys (*i.e.*, numerical codes that allow use of software applications without proper authorization from the software manufacturers). Forensic analysis revealed that the employee had previously installed this unauthorized program from an internet website and downloaded illegal software license keys onto his computer. Additional unauthorized software programs were found on his Government computer. We referred the investigative findings to management and disciplinary action is currently pending.

The second computer misuse investigation involved allegations that an agency attorney had downloaded pornographic images in violation of agency policy. Management referred the matter to this office because the downloaded images may have been in violation of criminal statute. The attorney had been the subject of a prior OIG investigation in 2004 and management was alerted that the problem may be ongoing when the employee allegedly used the agency's computer printer to print a pornographic image. Management authorized a forensic analysis of the employee's computer that revealed the presence of additional pornographic images that were not present on his computer when it was analyzed as part of the earlier OIG investigation. Disciplinary action is currently pending.

The third computer misuse investigation focused on allegations that an agency attorney was misusing Government computers to view pornographic images. Because management obtained evidence that criminal statutes could be implicated, the OIG was advised concerning the matter. Our investigation revealed that the employee had a history of the alleged misuse and that he was using computers that were not specifically assigned to him to view graphic images in violation of agency policy. There was also evidence that he left the office during scheduled work hours to meet individuals with whom his initial contact was made online. During the pendency of the OIG investigation, the employee voluntarily retired from federal service.

Another investigation was in response to the theft of a government laptop from a locked vehicle while the attorney responsible for the laptop was on official travel. The laptop contained personally identifiable information (*i.e.*, g names, addresses, Social Security numbers, dates of birth, drivers license numbers, voter registration information and in some instances financial account numbers) gathered in law enforcement investigations for approximately 110 individuals. These individuals were defendants in FTC cases, relatives of FTC defendants, individuals associated with FTC defendants or individuals whose names are similar to FTC defendants. The agency promptly notified the affected individuals that their personal information was compromised and provided information on the steps that the individuals should consider taking to limit their risk of identity theft. The agency also offered each affected individual one year of free credit monitoring. The OIG investigation into the theft revealed that the attorney responsible for the laptop failed to adhere to her supervisor's explicit instruction to remove all personally identifiable information from her laptop prior to business travel, which left the personally identifiable information contained on the stolen laptop vulnerable to unauthorized disclosure.

The FTC has no reason to believe the information on the laptops, as opposed to the laptops themselves, was the target of the theft. Our investigation also revealed that the attorney's organization failed to follow agency procedures regarding the disposition of the employee's old computer that had been replaced. The OIG referred the matter to management for further action.

The sixth investigation closed during this reporting period involved an allegation that an agency employee physically accosted and behaved in an unprofessional manner toward an individual who attended an FTC-sponsored industry conference. The employee, an agency investigator, attended the conference and had been assigned many logistical and organizational responsibilities relating to the conference. The complaint to the OIG alleged that, on two occasions, the employee physically restrained an individual representing an industry consumer advocacy group that has been critical of the FTC's enforcement of regulations governing the industry. The agency employee also allegedly informed the conference attendee that he would have to leave the conference because he had not preregistered for the event. The OIG obtained statements from three separate eyewitnesses to the alleged incidents and presented the employee with the evidence. The employee denied that any of the alleged incidents occurred as described by the eyewitnesses and complainant. We referred our conclusion that the employee had mistreated the conference attendee to management for appropriate action.

Matters Referred for Prosecution

During this reporting period the OIG referred no new cases to the Department of Justice for prosecution.

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 final management decisions made on which the IG disagreed and management did not revise any 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 this reporting period, the OIG did not encounter any problems 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. In addition, management has taken action to implement most of OIG's outstanding recommendations. The OIG is awaiting final action by the Redress Administration Office of the Bureau of Consumer Protections regarding automated tracking of redress contractor performance and the centralization of information regarding potential receivers.

Review of Legislation

Section 4(a)(2) of the IG Act authorizes the IG to review and comment on proposed legislation or regulations relating to the agency or, upon request, affecting the operations of the OIG. During this reporting period, the OIG reviewed no legislation.

Contacting the Office of Inspector General

Employees and the public are encouraged to contact the OIG regarding any incidents of possible fraud, waste, or abuse occurring within FTC programs and operations. The OIG telephone number is **(202) 326-2800**. To report suspected wrongdoing, employees may also call the OIG's investigator directly on **(202) 326-2618**. A confidential or anonymous message can be left 24 hours a day. Complaints or allegations of fraud, waste or abuse can also be emailed directly to chogue@ftc.gov. OIG mail should be addressed to:

Federal Trade Commission
Office of Inspector General
Room NJ-1110
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

OIG reports can be obtained directly from the internet at: www.ftc.gov/oig. A visitor to the OIG home page can download recent OIG semiannual reports to Congress, the FY 1998 - 2005 financial statement audits, and other program and performance audits issued beginning in FY 1999. A list of audit reports issued prior to FY 1999 can also be ordered via an e-mail link to the OIG. In addition to this information resource about the OIG, visitors are also provided a link to other federal organizations and Office of Inspectors General.

Internet Access

The OIG can be accessed via the world wide web at: http://www.ftc.gov/oig. A visitor to the OIG home page can download recent OIG semiannual reports to Congress, the FY 1998 - 2005 financial statement audits and other program and performance audits issued beginning in FY 1999. A list of audit reports issued prior to FY 1999 can also be ordered via an e-mail link to the OIG. In addition to this information resource about the OIG, visitors are also provided a link to other federal organizations and office of inspectors general.

TABLE I

SUMMARY OF INSPECTOR GENERAL REPORTING REQUIREMENTS

IG Act Reference	Reporting Requirement	Page(s)
Section 4(a)(2)	Review of legislation and regulations	7
Section 5(a)(l)	Significant problems, abuses and deficiencies	1 - 3
Section 5(a)(2)	Recommendations with respect to significant problems, abuses and deficiencies	1 - 3
Section 5(a)(3)	Prior significant recommendations on which corrective actions have not been made	7
Section 5(a)(4)	Matters referred to prosecutive authorities	7
Section 5(a)(5)	Summary of instances where information was refused	7
Section 5(a)(6)	List of audit reports by subject matter, showing dollar value of questioned costs and funds put to better use	11
Section 5(a)(7)	Summary of each particularly significant report	1 - 3
Section 5(a)(8)	Statistical tables showing number of reports and dollar value of questioned costs	10
Section 5(a)(9)	Statistical tables showing number of reports and dollar value of recommendations that funds be put to better use	10
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	7
Section 5(a)(11)	Significant revised management decisions	7
Section 5(a)(12)	Significant management decisions with which the inspector general disagrees	7

TABLE II

INSPECTOR GENERAL ISSUED REPORTS
WITH QUESTIONED COSTS

		Number	Dollar Value	
			Questioned Costs	Unsupported Costs
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]
	Subtotals (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 cost not disallowed	0	0	(0]
D.	For which no management decision was made by the end of the reporting period	0	0	(0]
	Reports for which no management decision was made within six months of issuance	0	0	(0]

TABLE III

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

		Number	Dollar Value
A.	For which no management decision has been made by the commencement of the reporting period	0	0
B	Which were issued during this reporting period	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
	- based on proposed management action	0	0
	- based on proposed legislative action	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