# *Finance Center*
# *Computer Security and Controls*

## *U. S. Coast Guard*

***Report Number: FI-2001-088***
***Date Issued: September 6, 2001***

# Memorandum

**U.S. Department of Transportation**
Office of the Secretary of Transportation
Office of Inspector General

Subject: **ACTION:** Report on Finance Center Computer Security and Controls U.S. Coast Guard FI-2001-088

Date: September 6, 2001

From: Alexis M. Stefani
Assistant Inspector General for Auditing

Reply To Attn Of: Meche:x6 4196

To: Chief of Staff
U.S. Coast Guard

This report provides the results of the computer security and controls audit at the U.S. Coast Guard Finance Center (FINCEN), Chesapeake, Virginia. The audit was performed by KPMG LLP under contract with the Office of Inspector General (OIG). The objective of the audit was to determine whether FINCEN computer operations are adequately secured to ensure integrity, confidentiality, and availability of Coast Guard major financial systems in support of the Department of Transportation (DOT) Fiscal Year (FY) 2001 Consolidated Financial Statements.

## SCOPE AND METHODOLOGY

KPMG conducted an audit of computer security and controls for six major financial systems at FINCEN, in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States and the General Accounting Office's Federal Information System Control Audit Manual. OIG and KPMG met to discuss the project scope and objectives. After reviewing previous audit reports and information about FINCEN provided by OIG, KPMG prepared an audit plan, which was reviewed and approved by OIG. KPMG then conducted field work in accordance with the plan, including interviews, reviews of documentation, observation of procedures, and testing of control features.

In addition to KPMG's work, OIG independently reviewed and evaluated the results of an automated security scan of FINCEN's network performed by Coast Guard's Telecommunication and Information Systems Command on July 18, 2001. This OIG work is not included in the KPMG report, but is summarized in this report.

## RESULTS

FINCEN is responsible for payment processing and financial reporting. KPMG concluded that computer security and controls at FINCEN are effective to ensure secure operations of its financial systems. However, KPMG identified four areas for improvement.

- Certification and Accreditation of Financial Systems

  DOT, Coast Guard, and the Office of Management and Budget (OMB) all issued requirements that major information systems be periodically reviewed for security certification. Only one of six major FINCEN financial systems had the security review and was certified as adequately secured for operations. The FINCEN data center itself also did not have a security review. This certification process provides better assurance that the integrity, confidentiality, and availability of financial systems is protected.

- Continuity of Operations

  OMB Circular A-130 requires planning for the continuity of operations for all information systems to be prepared for potential disruptions of agency functions. KPMG found that the plan for continuity of operations at FINCEN does not represent a viable plan in the event of a disaster. During the audit, FINCEN took corrective action to produce backup tapes for all of its systems. However, FINCEN has no alternative processing arrangement or facility. KPMG also found that the current offsite storage facility for backup tapes is within 300 yards of the FINCEN facility and not sufficiently distant as recommended by DOT policy to prevent both facilities from being affected by the same disaster. A comprehensive continuity of operations plan would ensure that FINCEN would be able to continue operations following a disaster.

- Access Controls

  KPMG found that controls over FINCEN password files could be improved. The password files could be read and copied by an unauthorized user without the knowledge of systems administrators. This could allow unauthorized users to access data in the name of authorized users. KPMG also found that there are no established procedures for periodic review of user access accounts. As a result, users may retain access to financial systems that they no longer need to do their jobs.

- Software Change Tracking

  FINCEN does not have a formal process for reviewing, approving, and tracking software change requests. A formal process could decrease the risk that unauthorized software change requests are made.

OIG also reviewed the vulnerabilities identified as a result of Coast Guard network scanning. We found that the vulnerabilities identified by Coast Guard did not represent a major security risk to its financial systems. FINCEN has taken corrective actions to eliminate the vulnerabilities identified. Therefore, we are not making any recommendations on this issue.

## RECOMMENDATIONS

We recommend that the Coast Guard Chief Financial Officer in coordination with the Chief Information Officer:

1. Develop and implement a plan and schedule to certify financial systems and the data center in accordance with OMB Circular A-130.

2. Direct FINCEN to develop and periodically test a comprehensive continuity of operations plan as required by OMB Circular A-130. This plan should include alternative processing arrangements or facilities and an offsite storage facility for backup tapes at a sufficient distance from the data center.

3. Direct FINCEN to improve security over password files, and establish procedures for periodic review of users' need to access financial systems.

4. Direct FINCEN to document and follow formal procedures for reviewing, approving, and tracking software change requests.

## MANAGEMENT RESPONSE

A draft of this report was provided to the Coast Guard Chief Financial Officer and the FINCEN Director on August 21, 2001. The FINCEN Director agreed with the findings, but expressed concerns about the cost and benefits of implementing a comprehensive continuity of operations plan.

## OFFICE OF INSPECTOR GENERAL COMMENTS

We agree that FINCEN should perform a cost-benefits analysis for implementing a comprehensive continuity of operations plan. In its analysis, FINCEN should consider making alternative processing arrangements with other Coast Guard data

centers. For example, the Coast Guard Operations Systems Center at Martinsburg, West Virginia, has similar technical setup and network connections as FINCEN. It could be cost-beneficial to Coast Guard, as a whole, if these two centers use each other as an alternative processing site.

The KPMG final report was provided to the Coast Guard Chief Financial Officer and the FINCEN Director on August 31, 2001. The KPMG report is available upon request.

**ACTION REQUIRED**

In accordance with DOT Order 8000.1C, we would appreciate receiving your written comments within 30 days. If you concur with the findings and recommendations, please state specific actions taken or planned for each recommendation and provide target dates for completion. If you do not concur, please provide your rationale. You may provide alternative courses of action that you believe would resolve the issues presented in this report.

We appreciate the courtesies and cooperation of Coast Guard representatives. If you have questions concerning this report, please call me at (202) 366-1964 or John Meche at (202) 366-1496.

-#-