Evaluation Report

OIG-CA-08-010

INFORMATION TECHNOLOGY: Treasury Successfully Demonstrated its TCS Disaster Recovery Capability (**REDACTED VERSION**)

August 12, 2008

Office of Inspector General

Department of the Treasury

Appendices

Abbreviations

DRE	Disaster Recovery Exercise
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
SBU	Sensitive But Unclassified
TCS	Treasury Communications System
TCS-POF	TCS Primary Operating Facility
TCS-AOF	TCS Alternate Operating Facility
TNet	Treasury Network

This page intentionally left blank.

OIG **Evaluation Report**

The Department of the Treasury
Office of Inspector General

August 12, 2008

Michael Duffy
Chief Information Officer
Department of the Treasury

Our overall objective for this evaluation was to determine if the Department of the Treasury could successfully demonstrate its Treasury Communications System (TCS) disaster recovery capability. In addition, we followed up on findings from the previous disaster recovery exercise (DRE). To accomplish this objective, we observed the DRE held at the TCS Alternate Operating Facility (TCS-AOF) from January 19 to January 20, 2008, and reviewed disaster recovery documentation for the exercise.

A more detailed description of our objectives, scope, and methodology is provided in appendix 1.

Results In Brief

Treasury successfully demonstrated its TCS disaster recovery capability in January 2008 by meeting the established exercise objectives. In addition, we found that Treasury had addressed the finding in the 2007 report on a previous TCS DRE and implemented two of three corresponding recommendations.[1] However, our prior recommendation on **[REDACTED – FOIA EXEMPTION 2, 5 U.S.C.**

[1] *Information Technology: Treasury Successfully Demonstrated its TCS Disaster Recovery Capability*, OIG-07-041 (June 25, 2007).

§552(b)(2)] Consequently, we are making two recommendations to address this issue.

Background

TCS is one of the largest private secure government networks. It serves more than 1,500 locations within and outside of the United States. The TCS mission is to provide best-cost, secure, robust, and reliable telecommunications services to Treasury and its bureaus and business partners to support their missions of promoting a stable U.S. and global economy through active governance of the financial infrastructure of the U.S. government. TCS delivers reliable, scalable, integrated, secure telecommunications services to Treasury and other federal agencies.[2]

TCS is configured in a distributed architecture with two main facilities. The TCS primary operating facility (TCS-POF) and TCS-AOF operate concurrently, and either facility can manage all traffic in the event the other fails. The disaster recovery capability of this system is required to be tested annually. We observed the January 2008 DRE performed at the TCS-AOF facility, which involved an anthrax scenario that rendered the TCS-POF operable but uninhabitable. Communications service continued to be provided from both facilities, but all management, operations, and support activities were performed from TCS-AOF. The test was conducted over a 2-day period and did not affect Treasury communications.

[2] TCS Continuity of Operations Plan Version 3.1, p. 1.

Finding and Recommendations

Finding TCS Successfully Demonstrated Disaster Recovery Capability but [REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]

We determined that Treasury successfully demonstrated its TCS disaster recovery capability by transferring management of TCS services and personnel to the alternate facility and remotely managing the primary facility. TCS personnel tested a valid scenario, participated in training sessions, and verified operation of systems at both facilities. In addition, Treasury addressed the finding identified in our prior audit and implemented two of three corresponding recommendations. The implemented recommendations were as follows:

1. Ensure that all workstations have an automatic lockout for use when unattended and that all staff understand the need to lock unattended workstations.
2. Work with the Internal Revenue Service to improve security at TCS-AOF and ensure that laptops are checked on exit to prevent unauthorized removal of equipment.

Treasury decided not to implement our third recommendation on **[REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]**

Recommendations

The Treasury Chief Information Officer should do the following:

1. **[REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]**
2. **[REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]**

Management Response

[REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]

OIG Comment

The actions planned by the Chief Information Officer satisfy the intent of our recommendations.

* * * * * *

I would like to extend my appreciation to TCS and the Office of the Chief Information Officer for the cooperation and courtesies extended to my staff during the review. If you have any questions, please contact me at (202) 927-5171 or Gerald Steere, Information Technology Specialist, Office of Information Technology Audits, at (202) 927-6351. Major contributors to this report are listed in appendix 3.

/s/

Tram J. Dang
Director, Office of Information Technology Audits

Our overall objective for this evaluation was to determine if Treasury could successfully demonstrate its Treasury Communications System (TCS) disaster recovery capability.[3] We accomplished this objective by (1) observing the disaster recovery exercise from January 19 to January 20, 2008, at TCS-AOF; (2) interviewing appropriate information technology personnel; and (3) reviewing and analyzing TCS's pre- and post-exercise documentation.

As criteria to assess the results of the exercise, we used National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems"; Office of Management and Budget Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"; Office of Management and Budget Memorandum M-06-16, "Protection of Sensitive Agency Information"; and Treasury CIO Memorandum TCIO-M-06-04, "Testing of Contingency Plans." We performed our fieldwork at the TCS-AOF facility from January 19 to January 20, 2008. We conducted our work in accordance with the President's Council on Integrity and Efficiency and Executive Council on Integrity and Efficiency's Quality Standards for Inspections. We are redacting certain information that we consider sensitive but unclassified (SBU) from the public distribution of our report to avoid any potential compromises of Treasury information security.

[3] This evaluation was included in the Treasury Office of Inspector General *Fiscal Year 2008 Annual Plan* (December 2007), p. 30.

Appendix 2
Management Comments

[REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]

[REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]

Office of Information Technology Audits

Tram J. Dang, Director, Office of Information Technology Audit
Louis C. King, Former Director
Gerald J. Steere, Information Technology Specialist
Leslye K. Burgess, Referencer

Department of the Treasury

Office of Accounting and Internal Control
Office of Strategic Planning and Performance Management
Office of the Chief Information Officer

Office of Management and Budget

Office of Inspector General Budget Examiner