



Audit Report



OIG-07-041

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

June 25, 2007

Office of
Inspector General

Department of the Treasury

Audit Report.....3

Results In Brief 3

Background..... 4

Finding and Recommendations 4

TCS Demonstrated Disaster Recovery Capability but Some Improvements Are Needed..... 4

Recommendations..... 6

Other Observations 7

Appendices

Appendix 1: Objective, Scope, and Methodology8

Appendix 2: Management Comments9

Appendix 3: Major Contributors 14

Appendix 4: Report Distribution 15

Abbreviations

- DRE Disaster Recovery Exercise
- OIG Office of Inspector General
- TCS Treasury Communications System
- [REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]
- [REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]

This page intentionally left blank.

*The Department of the Treasury
Office of Inspector General*

June 25, 2007

Edward Roback
Acting Chief Information Officer
Department of the Treasury

Our overall objective for this audit was to determine if 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 (1) observed the DRE held at the [REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)] , from January 20 to January 22, 2007, and (2) reviewed disaster recovery policies and procedures.

We performed our work in accordance with generally accepted government auditing standards. 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 addition, we found that Treasury had resolved both findings identified in our 2005 report on a previous TCS DRE and implemented all five corresponding recommendations.¹

Although the January 2007 DRE was successful, we found that (1) physical security at the [REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)] facility should be improved; and (2) [REDACTED]

¹ *Information Technology: The TCS Disaster Recovery Exercise Was Not Successful*, OIG-06-001 (Oct 4, 2005).

– **FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)**] We are making three recommendations to address these issues.

Background

TCS is one of the largest private secure government networks serving over 1,500 locations both within and outside of the United States. The TCS mission is to provide best-cost, secure, robust, and reliable telecommunications services to the Department of the 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 United States government. TCS delivers reliable, scalable, integrated, secure telecommunications services to Treasury and to other federal government agencies.²

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

The disaster recovery capability of this system is required to be tested annually. We observed the January 2007 DRE performed at the [REDACTED – **FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)**], which consisted of deactivating the primary routers at the [REDACTED – **FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)**] The test was conducted over a 3-day period to allow time for transition, troubleshooting, and operation over a full business day.

Finding and Recommendations

Finding **TCS Demonstrated Disaster Recovery Capability but Some Improvements Are Needed**

We determined that Treasury successfully demonstrated its TCS disaster recovery capability by transferring and sustaining the processing of TCS services at the backup facility for all of the

² TCS Continuity of Operations Plan Version 3.1, pg. 1

Treasury bureaus and related component agencies during the test period. In addition, Treasury resolved both findings identified in our prior audit and implemented all five corresponding recommendations. The recommendations pertained to

1. determination and correction of failures from a previous DRE,
2. conducting a DRE during a peak utilization period that includes all TCS components,
3. establishing a prioritization plan for shutting down low priority bureaus or systems,
4. identifying critical bureau systems, and
5. establishing a policy for the management of network traffic during a long-term outage.

However, we noted two new issues pertaining to physical security and [REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)] and observed several instances where physical security should be improved. Specifically, we noted weaknesses in security of workstations and building exit procedures. For example, we observed the following: (1) workstations in use at [REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)] that were not physically locked to a stationary object when left unattended, (2) some computers whose screensavers did not automatically lock after more than 30 minutes of being unattended, (3) bags that were not X-rayed or checked upon exiting the building, and (4) personnel who were not checked although they set off metal detectors while exiting the building.

Treasury Department Publication 85-01 (TD P 85-01), "Treasury Information Technology Security Program," requires that all workstations be logged off or locked or use a password-protected screensaver when unattended. Additionally, TD P 85-01 requires that controls be based on the level of risk and sufficient to safeguard assets against possible loss, theft, destruction, accidental damage, and malicious actions. Not complying with these requirements could lead to unauthorized access of sensitive information, removal of sensitive information, or theft of laptops from [REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]

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

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

Recommendations

The Treasury Chief Information Officer should do the following:

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 [REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)] and ensure that laptops are checked on exit to prevent unauthorized removal of equipment.
3. [REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]

Management Response

The Treasury CIO concurred with the three recommendations. The TCS Program Management Office will provide additional training in the use of the issued laptop cable lock systems, work with IRS to improve security at [REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)], and follow the established plan to meet the [REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]

OIG Comment

The actions proposed by the TCS Program Management Office satisfy the intent of our recommendations.

Other Observations

While reviewing documentation related to communications policy and TCS disaster recovery plans, we identified two areas for potential improvement. First, an outdated version of the Treasury Information Technology Manual (TD P 81-01) is published on the TreasNet Intranet page for the Office of the Chief Information Officer. The version on the intranet site is dated June 7, 2002. The current version of TDP 81-01, dated July 17, 2006, contains policies important to the management of communications during emergencies. Second, sections of the TCS Continuity of Operations Plan were out of date and did not contain the most current information available on the TCS intranet. This information includes diagrams of TCS customer networks. Both of these issues could lead to the use of outdated or incorrect information during a true emergency.

* * * * *

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) 927-5774 or Richard Kernozek, Information Technology Audit Manager, Office of Information Technology Audits, at (202) 927-7135. Major contributors to this report are listed in appendix 3.

/s/

Louis C. King, Director
Office of Information Technology Audits

SENSITIVE BUT UNCLASSIFIED

Appendix 1
Objective, Scope, and Methodology

Our overall objective for this audit was to determine if the 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 20 to January 22, 2007, at **[REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]**; (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 Federal Preparedness Circular 65, “Continuity of Operations”; National Institute of Standards and Technology Special Publication 800-34, “Contingency Planning Guide for Information Technology Systems”; Office of Management and Budget Circular 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 **[REDACTED – FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]**, from January 20 to January 22, 2007. We conducted our work in accordance with generally accepted government auditing standards. As permitted by those standards, we are omitting certain information (i.e., locations of key facilities and a sensitive finding) from the public distribution of our report to avoid any potential compromises of Treasury information security.

³ This audit was included in the Treasury Office of Inspector General *Fiscal Year 2007 Annual Plan* (December 2006), p 32.

SENSITIVE BUT UNCLASSIFIED

Appendix 2
Management Comments

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

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

Appendix 2
Management Comments

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

SENSITIVE BUT UNCLASSIFIED

Appendix 2
Management Comments

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

[SBU]

SENSITIVE BUT UNCLASSIFIED

Appendix 2
Management Comments

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

SENSITIVE BUT UNCLASSIFIED

Appendix 2
Management Comments

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

Appendix 3
Major Contributors

Office of Information Technology Audits

Louis C. King, Director
Richard G. Kernozek, Information Technology Audit Manager
Gerald J. Steere, Information Technology Specialist
Abdirahman M. Salah, Information Technology Specialist
Jeffrey Dye, Referencer

Appendix 4
Report Distribution

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