



Audit Report



OIG-06-001

INFORMATION TECHNOLOGY: The TCS Disaster Recovery Exercise Was Not Successful

October 4, 2005

Office of
Inspector General

Department of the Treasury

Contents

Audit Report	3
Results In Brief.....	3
Background	4
Findings and Recommendations	6
TCS’ Disaster Recovery Process Was Not Successful.....	6
Recommendations.....	7
Processing Prioritization Scheme Not In Place.....	7
Recommendations.....	9
Other Issues For Consideration	10

Appendices

Appendix 1: Objective, Scope, and Methodology	11
Appendix 2: TCS’ Actions Addressing Prior Audit Recommendations	12
Appendix 3: Management Comments	15
Appendix 4: Major Contributors.....	19
Appendix 5: Report Distribution.....	20

Abbreviations

OIG	Office of Inspector General
TCE	Treasury Communications Enterprise
TCS	Treasury Communications System
TCS-MCC	TCS Backup Facility in Martinsburg, West Virginia
TCS-W2	TCS McLean, Virginia
TEOAF	Treasury Executive Office for Asset Forfeiture
Treasury	Department of the Treasury
WAN	Wide Area Network

This Page Intentionally Left Blank.

*The Department of the Treasury
Office of Inspector General*

October 4, 2005

Ira L. Hobbs
Chief Information Officer
Department of the Treasury

Our overall objective for this audit was to determine if the Department of the Treasury (Treasury) could successfully perform its disaster recovery capability for its telecommunication systems (TCS) operations. To accomplish this objective, we observed the most recent disaster recovery exercise (DRE) to determine if deficiencies identified in prior reports¹ were corrected.²

The disaster recovery test was performed at the backup facility in Martinsburg, West Virginia (TCS-MCC) on August 17 and 18, 2005. A more detailed description of our objectives, scope, and methodology is provided in Appendix 1.

Results In Brief

Treasury was unable to successfully transfer and sustain the processing of TCS services at the backup facility for all of the Treasury bureaus and the related component agencies. Of the five recommendations identified in our prior report, Treasury attempted to address the following two:

- Conduct a disaster recovery exercise during a peak utilization period that includes all TCS components

¹ *Audit of Treasury Communications System Automated Information System Security Program*, dated February 1999 (OIG-99-039)

Lack of Bureau Connectivity Remains A Weakness In Treasury's Communications System's Disaster Recovery Capability, dated April 2003 (OIG-03-079)

INFORMATION TECHNOLOGY: The Treasury Communications System's Disaster Recovery Capability Has Improved, dated May 2005 (OIG-05-038)

² See Appendix 2 of this report for a detailed description of the previous OIG report finding, recommendations, management's response to the recommendations, and actions taken during this disaster recovery exercise to implement the recommendations.

requiring connection to TCS in the event of a service disruption and

- Establish a prioritization plan that provides guidance for shutting down low priority bureaus or systems.

In addition, because Treasury Executive Office for Asset Forfeiture (TEOAF) systems are linked to the DO LAN, the following recommendation is no longer relevant:

- Ensure that TEOAF has established a backup connection to TCC-MCC and is tested in a disaster recovery test.

In our previous report, we identified other issues that warranted consideration for TCS' disaster recovery capability. These issues did not have an impact on prior or current disaster recovery exercises. However, one of the areas remains a concern: the future plans to replace current TCS architecture with the Treasury Communications Enterprise (TCE).

Background

TCS is a nationwide data network whose mission is to provide best-cost, secure, robust, and reliable telecommunications services to the Treasury and its associated bureaus and business partners. This supports the mission of promoting a stable United States and global economy through active governance of the financial infrastructure of the United States Government. TCS offers a complete range of information technology services through its service providers. In February 1999, the OIG issued an audit report citing TCS' lack of a backup facility as a material weakness. In response, Treasury developed a remediation plan to assist in establishing a disaster recovery site to support TCS' Continuity of Operations Plan. The remediation plan was implemented in three phases beginning in January 2002. An acceptance test was conducted at the end of the first two phases to evaluate whether disaster recovery capabilities and critical system functionalities were working as designed.

In May and October 2002, we observed the acceptance testing for phases one and two conducted at the primary site in Mclean,

Virginia (TCS-W2) and TCS-MCC.³ We found that TCS management had taken actions to remedy the material weakness by establishing a backup facility at TCS-MCC. In addition, TCS management succeeded in recovering critical systems during acceptance testing. Although disaster recovery capabilities existed for TCS, we identified a number of weakness that needed to be addressed:

- Bureaus had not established connectivity to TCS-MCC to ensure networking services would not be interrupted in the event of a disaster.
- Performance testing was not conducted for systems at TCS-MCC.
- Disaster recovery exercises were not conducted, and disaster recovery standard operating procedures were not documented.
- Access to the Network Operating Center at TCS-MCC was not restricted.

TCS management concurred with all OIG findings and recommendations and commenced efforts to implement our recommendations. In addition, we stated that Treasury may consider downgrading the material weakness associated with the lack of TCS' backup facility when (1) all bureaus have established connectivity to TCS-MCC, and (2) disaster recovery exercises are successfully conducted.

In June 2004, we observed the TCS disaster recovery exercise at TCS-MCC.⁴ Although significant progress was made, the following findings were identified:

- A lack of full bureau participation,
- A processing prioritization scheme was not established, and
- TEOAF has no backup connection to TCS.

³ *Lack of Bureau Connectivity Remains A Weakness In Treasury Communications System's Disaster Recovery Capability*, dated April 2003 (OIG-03-079).

⁴ *INFORMATION TECHNOLOGY: The Treasury Communications System's Disaster Recovery Capability Has Improved*, dated May 2005 (OIG-05-038)

Findings and Recommendations

Finding 1 **TCS' Disaster Recovery Exercise Was Not Successful**

The disaster recovery exercise, which officially began on Wednesday, August 17, 2005,⁵ was aborted on August 18, 2005 because of the inability to establish and maintain connectivity and provide the services to the Treasury's bureaus and components from the backup facility. On August 18, 2005, TCS personnel informed us that the test was aborted at 5:00 a.m. due to a system failure that occurred overnight. In addition, although diagnostic equipment showed no anomalies, some bureaus reported disruptions in internet and email services. For example, a number of emails sent after 4:00 PM on August 17, 2005 did not arrive to their destinations in a timely manner. In some instances, these emails arrived to their destinations three days after sending as a result of the direct intervention of system administrators.

The exercise was conducted to comply with the Federal Preparedness Circular 65 which requires the annual testing of the Federal Executive Branch's continuity of operations to ensure readiness. The TCS' disaster recovery exercise was conducted as part of this annual assessment.

⁵ Some of the bureaus/components were switched to TCS-MCC prior to this date due to workload considerations.

Recommendations

The Treasury CIO should:

1. Determine the cause(s) of the inability to complete the disaster recovery exercise and implement necessary corrections or upgrades to ensure that the backup facility will operate adequately during future DREs or during actual disasters.
2. After the cause(s) is (are) identified and corrected, conduct a DRE during a peak utilization period that includes all TCS components requiring connection to TCS in the event of a service disruption.

Management Response Management agreed with the recommendations. The TCS contractor provided management with a final After Action report which identified the root causes of the disaster recovery exercise service disruption. The report provided specific remediation maintenance actions that have been completed to prevent outages of this nature in the future. After all of the findings in this audit report, the After Action report, and the TCS internal assessment have been completed, a full disaster recovery exercise will be conducted. The exercise will be completed no later than September 30, 2006.

OIG Comment The actions taken and planned by the Office of Information Systems are responsive to the intent of our recommendations.

Finding 2 Processing Prioritization Scheme Not In Place⁶

A component prioritization scheme was not established in the event that a processing overload occurs at TCS-MCC. TCS does not currently have a finalized prioritization plan that would provide guidance for shutting down low priority bureaus or systems. In addition, bureau level prioritization guidance has not been adopted to assist bureaus in prioritizing their systems for recovery in the event of a disaster. We were provided with a draft plan titled *Managing Electronic Communications During Emergencies* –

⁶ This was noted in the previous report. Since TCS has not fully addressed this issue and did not consider it part of this exercise, we are including it with updated information in this report.

MINIMIZE which was dated July 6, 2005. The draft plan establishes the purpose, policy, authority, and activation to implement the plan. The plan also includes the requirement that all Treasury Bureaus shall establish and maintain a prioritized list of critical systems and critical information flows. The draft plan is before the CIO Council for their review. However, no formal action has been taken on the plan.

In addition, there is no policy or process on how a network overload at TCS-MCC would be managed over longer periods of time (versus an immediate recovery). Currently, if this situation occurs, TCS management would provide network usage analysis to Treasury senior management exclusively for direction on handling bureau/system prioritization.

OMB Circular A-130, *“Management of Federal Information Resources”*, establishes policy for the management of federal information resources. Appendix III, *“Security of Federal Automated Information Resources”*, of this circular establishes a minimum set of controls to be included in federal automated information security programs. According to Appendix III, managers should plan for how they will perform their mission and/or recover from the loss of existing application support, and determine whether the loss is due to the inability of the application to function or a general support system failure. They should establish and periodically test the capability to continue providing services within a system based upon the needs and priorities of the participants of the system. Experience has demonstrated that testing a recovery plan significantly improves its viability. Untested plans, or plans not tested for a long period of time, may create a false sense of ability to recover in a timely manner.

Since TCS is the conduit for disseminating Treasury information and data, any major TCS service disruption can impede bureaus’ operations and missions. In the event of a disaster, inadequate recovery capabilities would cause mission critical operations to cease. Therefore, the cause of the system failure must be discovered and repaired to ensure an orderly transition of services in the event of a disaster.

Recommendations

The Treasury CIO should:

3. Establish a prioritization plan that provides guidance for shutting down low priority bureaus or systems.
4. Ensure that bureaus identify what systems are critical and what TCS needs to recover in the event of a disaster.
5. Establish a policy that identifies how a system overload at TCS-MCC would be managed over longer periods of time.

Management Response Management agreed with the recommendations. Corrective measures for recommendation three include developing and distributing guidelines for bureau development of prioritization of their circuits and applications. Once the guidelines are developed, an action plan will be developed for evaluating bureau responses; developing a comprehensive, overarching enterprise prioritization plan; and implementing it. The action plan will be developed through the Telecommunications Sub Council of the Treasury CIO Council. Corrective measures for recommendations four and five include revising the TCS Continuity of Operations Plan and Disaster Recovery plans to include (1) identification of systems that are critical to bureaus and a plan for recovering them in the event of a disaster and (2) include a policy on managing system overload over extended periods of time. This may entail monitoring traffic growth over TCS and working with bureaus on sizing.

OIG Comment Since the response did not specify that the bureaus would identify which systems are critical, it did not appear that the response for item four conformed to the recommendation. The CIO's office confirmed that the bureaus would be identifying which systems are critical. This will be accomplished through the Treasury Telecommunications Sub-Council, which is composed of representatives from the various bureaus. Therefore, the actions taken and planned by the Office of Information Systems are responsive to the intent of our recommendations.

Other Issues For Consideration

In our previous report, we identified other areas of consideration that, although did not directly impact the disaster recovery exercise or TCS' functionality, need to be considered as part of TCS' future operations. To date, there is still no the current plan to transition TCS operations to a new communications infrastructure.

TCS management planned to migrate its current TCS operations to the TCE communications environment. The contractor responsible for maintaining the functionality of TCS has approximately one month remaining on its current contract. An automatic 6-month extension can be granted on the contract; however, once the current contract expires, IRS will request a 12-month extension. Treasury is in the process of procuring TCE which will replace TCS. The objective of the TCE contract is to improve TCS services by enhancing or replacing current infrastructure, assets, and services. To ensure continuity of operations, it is essential that Treasury ensures a well planned transition to sustain the viability of TCS' day-to-day operations, as well as disaster recovery capability. The lack of a sound transition process could lead to a disruption in the service TCS provides to the bureaus.

* * * * *

I would like to extend my appreciation to TCS 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, IT Audit Manager, Office of Information Technology Audits, at (202) 927-7135. Major contributors to this report are listed in Appendix 5.

Louis C. King
Director, Office of Information Technology Audits

The objectives of this audit were to determine if the Department implemented our prior audit recommendations and to assess the Department's disaster recovery capabilities for the TCS Mclean facility⁷. These objectives were accomplished by (1) observing the disaster recovery exercise which took place from August 17^h to 18^h, 2005 at TCS-MCC; (2) interviewing appropriate IT personnel; (3) reviewing disaster recovery exercise reports provided by Treasury; (4) reviewing and analyzing Treasury's planning, results and post-exercise documentation; and (5) analyzing limited e-mail traffic during the disaster recovery exercise. Since the exercise was aborted, bureau locations within the Washington, D.C. area were not reviewed.

We used the Federal Preparedness Circular 65 and OMB Circular A-130 as criteria to assess the results of the exercise. Fieldwork was performed at TCS-MCC during August 2005. We conducted our work in accordance with Generally Accepted Government Auditing Standards.

⁷ This audit was included in the OIG's *Annual Plan Fiscal Year 2005* on page 28.

Appendix 2
TCS' Actions Addressing Prior Audit Recommendations

A backup facility at TCS-MCC has been established. In our May 16, 2005 report, we identified weaknesses in TCS' disaster recovery capabilities that would impact TCS and Treasury bureaus in the event of a disaster or unplanned disruption at TCS-W2. As a result, we provided five recommendations to the CIO. The recommendations, CIO management response, and action taken during this disaster recovery exercise are specifically identified below.

Recommendation 1: Conduct a disaster recovery exercise during a peak utilization period that includes all TCS components requiring connection to TCS in the event of a service disruption.
Management Response: Management agreed to conduct a full disaster recovery test once all of the bureaus were connected to the backup site.
Actions Taken Prior To And During The Exercise: The Director, Infrastructure Operations sent an e-mail to the bureaus and components apprising them of the disaster recovery exercise which was scheduled for August 17-19, 2005. The e-mail stated that this disaster recovery exercise would involve an almost total power-down of the TCS-W2 facility to more realistically reflect the disaster recovery procedures in the event of catastrophic damage to the primary facility. The e-mail further stated that the exercise would include a review of the "prioritization plan" to maintain minimum service levels in extraordinary circumstances. However, the information we obtained during the exercise in-brief stated that a review of this plan was not included in the exercise.

Appendix 2
TCS' Actions Addressing Prior Audit Recommendations

Recommendation 2: Establish a prioritization plan that provides guidance for shutting down low priority bureaus or systems.
Management Response: Management indicated that they would develop a Treasury prioritization plan and related directive to ensure bureaus and offices shut down low priority systems during times of emergency.
Actions Taken Prior To And During The Exercise: A draft plan, titled <i>Managing Electronic Communications during Emergencies – MINIMIZE</i> and dated July 6, 2005, has been forwarded to the CIO Council for comment. Documentation provided at the in-brief meeting indicated that inclusion of this recommendation was not part of the exercise.

Recommendation 3: Ensure that bureaus identify what systems are critical and what TCS needs to recover in the event of a disaster.
Management Response: Management stated that they would identify critical systems and provide the TCS program management office with a prioritized list.
Actions Taken Prior To And During The Exercise: Documentation provided at the in-brief meeting indicated that inclusion of this recommendation was not part of the exercise.

Recommendation 4: Establish a policy that identifies how a system overload at TCS-MCC would be managed over longer periods of time.
Management Response: Management agreed to monitor the growth of TCS traffic and work with the bureaus to ensure they adequately size their alternate communication paths.
Actions Taken Prior To And During The Exercise: Documentation provided at the in-brief meeting indicated that inclusion of this recommendation was not part of the exercise.

Appendix 2
TCS' Actions Addressing Prior Audit Recommendations

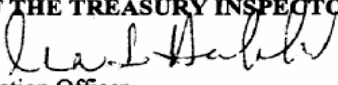
Recommendation 5: Ensure that TEOAF has established a backup connection to TCS-MCC and is tested in a disaster recovery test.
<u>Management Response:</u> Management informed the OIG that TEOAF was no longer connected directly to TCS for its primary WAN services. It receives its connectivity from IT Headquarters and the Departmental Offices local area network maintains disaster recovery connectivity.
<u>Actions Taken Prior To And During The Exercise:</u> No additional action necessary.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

SEP 29 2005

MEMORANDUM FOR: LOUIS C. KING
**DIRECTOR, INFORMATION TECHNOLOGY AUDITS
OFFICE OF THE TREASURY INSPECTOR GENERAL**

FROM: Ira L. Hobbs 
Chief Information Officer

SUBJECT: Draft Audit Report - "The TCS Disaster Recovery Exercise
Was Not Successful", (OIG-05-), dated August 31, 2005

Thank you for the complete out briefing and for the opportunity to review the draft report. Attached please find our response to the findings and recommendations, with which we concur.

The Office of the Chief Information Officer (OCIO) is committed to providing the highest level of information technology support in a manner that is consistent with Treasury and other Federal policies and practices.

I would like you to be aware that my office has received an After Action Report (AAR) from the TCS Contractor, Northrop Grumman Information Technology, and has performed an internal assessment of the disaster recovery exercise. We have synopsised these as they relate to your findings about the unsuccessful execution of the exercise and will provide full copies at your request. We intend, prior to the next disaster recovery exercise, to address and mitigate all the findings from these reports as well as those you have identified in the draft audit report.

If you or your staff have questions, please contact me on (202) 622-1200 or Ken Riccini, Associate CIO for Telecommunications Management, on (202) 622-2047.

Attachment

Management Response to Draft Audit Report – Draft Audit Report – “The TCS Disaster Recovery Exercise Was Not Successful”, (OIG-05-), dated August 31, 2005

FINDINGS

Finding 1: TCS’ Disaster Recovery Exercise was not successful

The DR exercise, which officially began on Wednesday, August 17, 2005, was aborted on August 18, 2005, because of the inability to establish and maintain connectivity and provide services to the Treasury’s bureaus and components from the backup facility. On August 18, 2005, the test was aborted at 0500 due to a system failure that occurred overnight.

Comments: We concur with the observation and would like you to be aware of the results of our analyses of the causes. During the exercise, all Treasury Bureaus and some non-Treasury customers successfully established and transferred wide area network communications from their primary locations to the Treasury Communication Systems’ (TCS) alternate operating facility in Martinsburg, WV. Near the end of the cutover phase, the wide area network load balancer system failed after the TCS contractor technical support team improperly executed a configuration change. This system prioritizes and balances traffic routing across the wide area network’s firewalls. The failure of this device resulted in a complete loss in Intranet, extranet and external email services. Subsequently, when returning services to the TCS primary operating facility in McLean, VA, the TCS contractor technical support team failed to reconfigure an email gateway. This oversight caused external email to be directed to the alternate operating facility in Martinsburg, WV, where services were inoperable. Once discovered, the affected external email was redirected to TCS primary operating facility and delivered accordingly. In both cases, the after action report identifies the TCS contractor technical support team’s failure to follow established SOPs when making configuration changes as the root cause of the failures.

Among other actions to remediate recurrences, TCS management is reviewing with the contractor existing disaster recovery standard operating procedures to ensure technical accuracy in their execution.

Finding 2: Processing Prioritization Scheme Not In Place

A component prioritization scheme was not established in the event of a processing overload occurs at TCS-MCC. TCS does not currently have a finalized prioritization plan that would provide guidance for shutting down low priority bureaus or systems. In addition, bureau level prioritization guidance has not been adopted to assist bureaus in prioritizing their systems for recovery in the event of a disaster. The OIG was provided with a draft plan titled *Managing Electronic Communications During Emergencies – MINIMIZE* which was dated July 6, 2005. The draft plan is before the CIO council for their review. However, no formal action has been taken on the plan.

In addition, there is no policy or process on how a network overload at TCS-MCC would be managed over longer periods of time (versus an immediate recovery). Currently, if this situation occurs, TCS management would provide network usage analysis to Treasury senior management exclusively for direction on handling bureau/system prioritization.

Comments: We concur with the observations.

RECOMMENDATIONS

Recommendation 1 - The Treasury CIO should:

Determine the cause(s) of the inability to complete the disaster recovery exercise and implement necessary corrections or upgrades to ensure that the backup facility will operate adequately during future DREs or during actual disasters.

OCIO Response: We have received a final After Action Report from the TCS contractor, Northrop Grumman Information Technology (NGIT), which identifies the root causes of the DRE service disruption. This report provided specific remediation maintenance actions that have been completed to prevent this type of outage in the future.

Accountable official: ACIO for Telecommunications

Target Completion Date: Completed September 2005

Recommendation 2 - The Treasury CIO should:

After the cause(s) is (are) identified and corrected, conduct a DRE during a peak utilization period that includes all TCS components requiring connection to TCS in the event of a service disruption.

OCIO Response: We will conduct a full Disaster Recovery Exercise during FY06 after all findings in this audit report, the After Action Report, and our internal assessment have been remediated.

Accountable Official: ACIO for Telecommunications

Target Completion Date: No later than September 30, 2006

Recommendation 3 - The Treasury CIO should:

Establish a prioritization plan that provides guidance for shutting down low priority bureaus or systems.

OCIO Response: We have developed and distributed guidelines for bureau development of prioritization of their circuits and applications as required by FPC 65. We will develop, through the Telecommunications Sub Council of the Treasury CIO Council, an action plan for evaluating bureau responses; developing a comprehensive, overarching enterprise prioritization plan; and implementing it.

Accountable Official: ACIO for Telecommunications

Target Completion Date: Plan developed March 30, 2006

Recommendation 4 - The Treasury CIO should:

Ensure that bureaus identify what systems are critical and what TCS needs to recover in the event of a disaster.

OCIO Response: We will revise the TCS COOP and DR plans to include identification of systems that are critical to bureaus and a plan for how they will be recovered in the event of a disaster.

Accountable Official: ACIO for Telecommunications

Target Completion Date: March 30, 2006

Recommendation 5 - The Treasury CIO should:

Establish a policy that identifies how a system overload at TCS-MCC would be managed over longer periods of time.

OCIO Response: We will revise the TCS COOP and DR plans to include a policy on managing system overload over longer periods of time. This may include monitoring the growth of traffic over TCS, and work with bureaus on sizing.

Accountable Official: ACIO for Telecommunications

Target Completion Date: March 30, 2005

Office of Information Technology Audits

Louis C. King, Director
Richard G. Kernozek, IT Audit Manager
Leslye K. Burgess, IT Audit Manager
Charles Dampare, IT Auditor
Catherine Yi, Referencer

The Department of the Treasury

Office of the Deputy Assistant Secretary for Information
Systems/Chief Information Officer
Office of Accounting and Internal Control
Enterprise Communications Program Management Office

Office of Management and Budget

Office of Inspector General Budget Examiner