Additional Disaster Recovery Planning, Testing, and Training Are Needed for Data Communications

April 2004

Reference Number: 2004-20-079

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

April 9, 2004

MEMORANDUM FOR CHIEF INFORMATION OFFICER

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Additional Disaster Recovery Planning, Testing, and Training Are Needed for Data Communications (Audit # 200320019)

This report presents the results of our review of the telecommunications disaster recovery strategy. The overall objective of this review was to determine whether the Internal Revenue Service (IRS) developed and tested an effective telecommunications disaster recovery strategy.

To allow users and taxpayers fast and efficient access to applications and services, the IRS must have a robust, responsive telecommunications infrastructure that provides high-speed, high-availability network connectivity. The IRS Enterprise Networks organization is responsible for managing the design and engineering of the telecommunications environment, which includes approximately 181,500 network devices and 1,200 network connection addresses.

In summary, the IRS has implemented several measures to create a robust and resilient network architecture to support continuous data communications. For example, it has made significant upgrades to its data communications network, including redundant connections and diverse data traffic routing for key facilities, and standardization and redundancy in network hardware. The IRS has also taken additional measures at its facilities to reduce the vulnerability of the network, including off-premises storage of network documentation, network system backups, installation of an uninterruptible power supply, and identification and reduction of single points of failure within the network. In addition, the Enterprise Networks organization has ongoing projects to evaluate its data communications network to improve and upgrade the infrastructure, while at the same time trying to reduce network operations costs. However, additional actions could further improve the disaster recovery strategy for data communications.

While each of the four facilities we visited prepared a disaster recovery plan for data communications and stored the plan at its off-premises location, the plans did not contain all of the required components and sufficient training had not been conducted for the disaster recovery teams. Inadequate disaster recovery plans and training for the disaster recovery personnel diminish the assurance that the IRS can rapidly recover data communications at a site in an emergency and that the disaster recovery activities can be conducted efficiently. In addition, the plans had not been comprehensively exercised. While the day-to-day operational measures taken by management and staff in response to daily data communications interruptions may diminish the need for testing system restoration, exercising the remaining plan elements, such as plan activation and team member notification and reporting procedures, would improve the site's ability to recover timely.

Presidential Decision Directive 63, *Critical Infrastructure Protection (CIP)*,[1] dated May 1998, requires that each Federal Government department and agency prepare a plan for protecting its own critical infrastructure. The infrastructure includes systems essential to the minimum operations of the economy and the Federal Government, such as telecommunications, banking and finance, energy, and transportation. As part of its CIP Program, the IRS identified 19 critical assets, which included the data communications network. The IRS also completed a vulnerability assessment in November 2000 for each of the critical assets. However, the IRS has not completed the disaster recovery planning and risk management activities for data communications, which could result in the inability of the IRS to timely restore critical data communications in the event of a disaster, potentially affecting the IRS' ability to accomplish its mission and serve taxpayers.

Lastly, the IRS engaged a vendor to assess the old network, propose a new network design, and provide cost estimates for a new network. The vendor concluded that the proposed design and configuration presented the least amount of complexity and cost while delivering the maximum level of capabilities and benefits, including alternate routing access and recovery. However, the IRS did not prepare a formal cost-benefit analysis which may have resulted in the IRS not selecting the most feasible or cost-effective data communications network design and recovery strategy that would support the needs of the business units. In addition, our site survey results showed that a bi-directional ring[2] connecting the Campus[3] and Territory Office[4] in Atlanta was not being used as advantageously as possible. For example, the Territory Office currently does not use the bi-directional ring for routing its data traffic; instead, the data are being sent over a separate circuit. By implementing a solution that would permit the Territory

---

[1] Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection,* issued December 17, 2003, superseded Presidential Decision Directive 63 and requires Federal agencies to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the disruption or destruction of information.

[2] A bi-directional ring topology reroutes traffic in the other direction if the circuit is cut.

[3] The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.

[4] Territory Offices serve taxpayers within a specified geographical area.

Office to shift its data traffic to the bi-directional ring, management could remove the circuit and realize potential cost savings of $315,000[5] over 5 years.

We recommended the Chief, Information Technology Services, ensure each site reviews the disaster recovery plan for completeness and accuracy quarterly or whenever significant changes occur to any plan element, periodically trains employees in their disaster recovery roles and responsibilities, and performs at least one exercise of each disaster recovery plan element annually. In addition, we recommended the Chief, Information Technology Services, complete the additional disaster recovery and risk management measures outlined in the IRS' CIP Program for the data communications network, ensure a cost-benefit analysis is prepared for projects redesigning the network architecture that result in a significant investment, and ensure the current IRS project tasked with optimizing the data communications network also assesses the use of the bi-directional rings.

Management's Response: IRS management agreed to the recommendations presented in the report. Planned corrective actions include performing quarterly reviews of the disaster recovery plans, conducting yearly training sessions and disaster recovery tests, and identifying critical points of failure within the local area networks. Enterprise Networks organization management will include the names, responsible program areas, and contact numbers in site-specific disaster recovery plans. All future risk assessments of the network(s) will be processed under the Treasury Communications Enterprise managed services contract. In addition, Enterprise Networks organization management will develop a suite of business case and alternative analysis processes for evaluating significant investment projects and will include an evaluation of bi-directional rings when optimizing the data communications network. Management's complete response to the draft report is included as Appendix VII.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

[5] The potential cost savings of $315,000 would be reduced by any additional costs to implement the solution.

Table of Contents

Additional Disaster Recovery Planning, Testing, and Training Are Needed for Data Communications

Background

One of the Internal Revenue Service's (IRS) major strategies contained in the *IRS Strategic Plan Fiscal Years 2000-2005* is to provide high-quality, efficient, and responsive information services. This strategy includes building a robust, responsive telecommunications infrastructure that provides high-speed, high-availability network connectivity to allow users and taxpayers fast and efficient access to authorized IRS applications and services. The IRS Enterprise Networks organization is responsible for managing the design and engineering of the telecommunications environment, which includes approximately 181,500 network devices and 1,200 network connection addresses.

To ensure network availability, controls should be implemented that are designed both to prevent interruptions and to promptly recover data communications service should unexpected events occur. Business continuity planning is the process of establishing, testing, and maintaining policies, procedures, and physical resources to effect the timely resumption of critical business processes in the event of a disaster. A key component of business continuity planning is disaster recovery planning, which is the advance planning and preparations from a technology aspect that are necessary to minimize loss and ensure continuity of the critical business functions.

In the *IRS-Wide Business Continuity Planning – Case for Action,* dated November 30, 2001, the IRS reported weaknesses in its ability to perform disaster recovery. For example, the IRS reported that many of its business continuity plans were not tested and updated on a regular basis. In December 2002, we reported that the IRS had made substantial progress in its business continuity program.[1] Activities initiated by the IRS included increasing the visibility and management oversight of business continuity issues, improving physical security at its offices, and developing plans to improve the recovery capability of its mainframe computers. However, the General Accounting Office (GAO) reported in May 2003

[1] *The Internal Revenue Service Has Made Substantial Progress in Its Business Continuity Program, but Continued Efforts Are Needed* (Reference Number 2003-20-026, dated December 2002).

that the IRS had not developed disaster recovery plans for certain key systems at some facilities and had not tested the plans at other facilities.[2] A disaster recovery plan defines the resources, actions, tasks, and data required to manage the restoration process for an application or system within the stated disaster recovery goals, thereby minimizing the effects of a major disruption.

This review was performed in the Enterprise Networks office at the IRS National Headquarters in New Carrollton, Maryland; the Tennessee Computing Center (TCC)[3] in Memphis, Tennessee; the Martinsburg Computing Center (MCC) in Martinsburg, West Virginia; and the IRS Campus[4] and Territory Office[5] in Atlanta, Georgia, during the period September through December 2003. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Several Measures Have Been Taken to Deliver Uninterrupted Data Communications

Maintaining uninterrupted data communications is critical to the IRS to accomplish its mission of providing top-quality service to taxpayers. As a result, the IRS has implemented several measures to create a robust and resilient network architecture to support continuous data communications. As reflected in the *Data Communications Utility (DCU) Network Border Router Configuration and Redundancy Design*, dated April 2000, and the *Infrastructure Architecture Modernization Assessment*, dated February 2002, the IRS has made significant upgrades to its network including:

[2] *Information Security: Progress Made, but Weaknesses at the Internal Revenue Service Continue to Pose Risks* (Reference Number GAO-03-44, dated May 2003).
[3] IRS computing centers support tax processing and information management through a data processing and telecommunications infrastructure.
[4] The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.
[5] Territory Offices serve taxpayers within a specified geographical area.

- Implementation of Asynchronous Transfer Mode (ATM)[6] as the backbone[7] transport.
- Redundant connections between IRS campuses and computing centers.
- The use of bi-directional ring topology[8] and microwave[9] to provide diverse and redundant data traffic routing for the computing centers.
- Standardization and redundancy in network hardware at each of the border router locations.

The results of our site visits to four IRS facilities also reflected that additional measures were being taken to reduce the vulnerability of the data communications network at those sites. Detailed information on our site visits is presented in Appendix V. These measures included off-premises storage of network documentation, network system backups, installation of an uninterruptible power supply, and identification and reduction of single points of failure within the network. In addition, the sites maintained some spare parts for network equipment and had service level agreements with vendors for repairs. The Enterprise Networks organization also has ongoing projects to evaluate its data communications network to improve and upgrade the infrastructure, while at the same time trying to reduce network operations costs.

Improved Site Disaster Recovery Plans and Increased Testing and Training Are Needed for Data Communications

Office of Management and Budget (OMB) Circular A-130, *Security of Federal Automated Information Resources*, requires that agency plans assure they can recover and provide sufficient service to meet the minimal user needs of the system in the event of a disaster. Disaster recovery is the ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions. The IRS Internal

[6] The ATM is a high-speed, cell-switching network technology that handles data, real-time video, and voice.
[7] A segment of the network used to connect smaller segments of the network.
[8] A bi-directional ring topology reroutes traffic in the other direction if the circuit is cut.
[9] Microwave is a point-to-point, free-space technology providing an alternative to a fiber-based network.

Revenue Manual (IRM) contains specific requirements for developing a disaster recovery plan for all mission critical systems at each facility. The IRS has also developed a disaster recovery plan template to assist site management in the development of their respective plans.

Major components of a site's disaster recovery plan for data communications should include an overview of the disaster recovery strategy, recovery team information, notification procedures, network/circuit diagrams, hardware and software inventory, system backup requirements, off-premises storage information, and a telephone listing of external contacts such as vendors and suppliers. The disaster recovery plan should also contain recovery priorities and step-by-step restoration procedures to prevent difficulty or confusion in an emergency. The IRM stipulates that each site store a complete copy of the plan in both magnetic media and hard copy at the off-premises storage facility for that site.

The IRM also contains requirements for maintaining and testing the disaster recovery plans to assure the system can be recovered in a timely manner. To be effective, the plan must be reviewed and updated regularly since frequent changes can occur with the names and contact information for team members and with system requirements and procedures as a result of shifting business needs and technology upgrades. Therefore, the IRM requires that the plan be reviewed quarterly, tested annually, and updated as needed to provide for the reasonable restoration of operations. According to the National Institute of Standards and Technology (NIST),[10] testing of the disaster recovery plan should include exercising each plan element to identify planning gaps and address plan deficiencies, thereby improving plan effectiveness and overall agency preparedness. The disaster recovery personnel should also be trained at least annually to prepare them to execute their respective recovery procedures during plan activation.

[10] The NIST is an organization within the United States Department of Commerce that is responsible for setting security standards for the nondefense side of the Federal Government.

As illustrated in Exhibit 1, a review of the disaster recovery plans and preparedness activities for data communications at four IRS facilities identified areas where improvements are needed. Detailed information on our review of the sites' disaster recovery plans is contained in Appendix VI.

Exhibit 1: Status of Disaster Recovery Activities for Data Communications

IRS Facility	Plan Prepared	Plan Complete	Plan Stored Offsite	Comprehensive Exercise of the Plan	Sufficient Training Conducted
MCC	Yes	No	Yes	No	Yes
TCC[11]	Yes	No	Yes	No	No
Atlanta Campus	Yes	No	Yes	No	Yes
Atlanta Territory Office	Yes	No	Yes	No	No

Source: The Treasury Inspector General for Tax Administration's review of site disaster recovery plans and discussions with management using requirements contained in NIST and IRS guidelines.

While each facility prepared a disaster recovery plan for data communications and stored it at its off-premises location, the plans did not contain all of the required components. In addition, the plans had not been comprehensively exercised and sufficient training had not been conducted for the disaster recovery teams.

The disaster recovery plans require additional information

The disaster recovery plans prepared by each site for data communications contained many of the required components. In general, the disaster recovery plans contained an overview of the recovery strategy, recovery team member names and telephone numbers, recovery team responsibilities, notification procedures, contact information for vendors and suppliers, network/circuit diagrams, system

[11] The TCC had recently prepared a Technical Contingency Planning Document, which was regarded as the site's disaster recovery plan for evaluative purposes since it contained many of the required components and was similar in format to a disaster recovery plan.

backup requirements, and off-premises storage information. However, most of the plans did not contain the following information required by NIST and IRS guidelines:

- Recovery priorities and step-by-step restoration procedures.
- An inventory of hardware and software.
- A listing of Internet Protocol (IP)[12] addresses and circuits.
- A record of updates to the plan.

While management at the sites we visited did maintain an inventory of hardware and a listing of IP addresses, and stored this information at their off-premises locations, they did not include this information as part of their disaster recovery plans. Inadequate disaster recovery plans diminish the assurance that the IRS can rapidly recover data communications at a site in an emergency and that the disaster recovery activities can be conducted efficiently. Management did not develop adequate disaster recovery plans because they were uncertain about exactly what information should have been included in the plans.

Additional testing of the plans and training of the disaster recovery personnel are needed

Each of the sites had not completed a comprehensive exercise of its disaster recovery plan for data communications. Management explained that the recovery of failed data communications devices is a day-to-day operational issue. While sites may not specifically document disaster recovery testing, they exercise their disaster recovery capabilities throughout the year in response to incidents, including the restoration of routers. Management also performs tests by annually powering off and restoring equipment and by participating in the disaster recovery exercises of other systems (e.g., mainframe computers). In addition, management attributed the absence of a formal disaster recovery test for data communications to their concern for disrupting operations.

[12] A Department of Defense standard protocol designed for use in interconnected systems of computer communications networks.

According to NIST guidelines, a disaster recovery test should include exercising each plan element, such as plan activation, team member notification and reporting procedures, and system restoration from backup media. While the day-to-day operational measures taken by management and staff in response to daily data communications interruptions may diminish the need for testing system restoration, exercising the remaining plan elements would improve the site's ability to recover timely. To obtain the most benefit from disaster recovery testing, the test plan should contain detailed information, including the scenario, test elements, evaluation criteria, and time periods. The results of the test should be documented and lessons learned identified to improve plan effectiveness.

Training was inadequate for the disaster recovery personnel because management was unsure what the training should entail for their disaster recovery teams. According to the NIST, recovery personnel should be trained at least annually on the following elements:

- Purpose of the plan.
- Cross-team coordination and communication.
- Reporting procedures and security requirements.
- Team-specific processes and individual responsibilities.

The goal of disaster recovery training should be to train the disaster recovery personnel to the extent that they are able to execute initial recovery procedures without aid of the actual document, since a paper or electronic version of the plan may be unavailable for the first few hours as a result of the disaster.

Recommendations

The Chief, Information Technology Services, should ensure each site:

1. Reviews the disaster recovery plan for completeness and accuracy quarterly or whenever significant changes occur to any plan element.

Management's Response: The MCC and TCC developed a process to perform quarterly reviews. The first review will

be completed by April 1, 2004. The Atlanta Territory Manager implemented a controlled response process to ensure the disaster recovery plan was reviewed. The responses are due March 31, June 30, September 30, and December 31 requiring verification that each team has met and their respective disaster recovery plans have been reviewed for accuracy. A *Plan Changes or Reviews* sheet has been added to the plans to document all changes to and reviews of the plans.

2. Periodically trains employees in their disaster recovery roles and responsibilities.

Management's Response: Both the MCC and TCC will conduct yearly training sessions beginning in September 2004 during the preplanning phase for this year's disaster recovery exercise. The Atlanta Territory Manager will ensure the Telecommunications organization conducts an independent biannual disaster recovery table exercise and documents it in the plan.

3. Performs at least one exercise of each disaster recovery plan element annually.

Management's Response: Testing at the MCC and TCC is conducted more frequently than on an annual basis. This includes participation in disaster recovery of other systems (e.g., mainframe disaster recovery exercise). Testing for this calendar year will be conducted by December 1, 2004. The Atlanta Campus and Atlanta Territory Manager will coordinate with the Mission Assurance Office to ensure annual disaster recovery testing is conducted.

The Data Communications Network Requires Additional Disaster Recovery and Risk Management Measures

Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection (CIP),*[13] dated May 1998, calls for a national effort to assure the security of the nation's critical infrastructure. The infrastructure includes systems essential to the minimum operations of the economy and Federal Government, such as telecommunications, banking and

[13] Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection,* issued December 17, 2003, superseded PDD 63 and requires Federal agencies to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the disruption or destruction of information.

finance, energy, and transportation. PDD 63 also requires that each Federal Government department and agency prepare a plan for protecting its own critical infrastructure. Executive Order 13231, *Critical Infrastructure Protection in the Information Age,* issued October 2001, reaffirms the need to continually take actions to secure information systems, emergency preparedness communications, and physical assets.

The Department of the Treasury Critical Infrastructure Protection Plan (TCIPP), dated August 30, 2002, stipulated that each departmental office and bureau is responsible for identifying the critical assets under its control, assessing the vulnerabilities of those assets, and assuring their availability, integrity, confidentiality, survivability, and adequacy. According to the TCIPP, critical infrastructure would include the physical and cyber assets that support critical missions. Physical assets include the facilities providing service to the public, while cyber assets include networks, computers, applications, data, and information. Each departmental office and bureau is also required to develop its own CIP Management Plan addressing governance, risk management, critical asset management, threat assessment, vulnerability/risk assessment, disaster recovery planning and management, incident reporting and handling, and training and awareness.

In February 2003, we reported that, while the IRS had not yet completed its CIP Management Plan, it had taken significant steps in protecting its critical assets.[14] Some of the required activities identified in the IRS' draft CIP Management Plan included:

- Critical asset identification.
- Vulnerability assessment.
- Disaster recovery planning.
- Risk management.

As part of its CIP Program, the IRS identified 19 critical assets, which included the data communications network.

[14] *Progress Has Been Made in Protecting Critical Assets* (Reference Number 2003-20-047, dated February 2003).

The IRS also completed a vulnerability assessment in November 2000 for each of the critical assets. However, the IRS has not completed the disaster recovery planning and risk management activities for data communications, which could result in the inability of the IRS to timely restore critical data communications in the event of a disaster, potentially affecting the IRS' ability to accomplish its mission and serve taxpayers.

According to the draft CIP Management Plan, critical asset owners shall ensure that disaster recovery plans cover their critical assets and that those plans appropriately prioritize actions with respect to those critical assets. For data communications, the disaster recovery plan should address the compromise or incapacitation of the critical asset as a result of physical or cyber attacks as well as natural disasters. Critical asset owners were also required to develop and maintain a risk management plan. Risk management encompasses those activities taken to identify, control, and reduce risks. The risk management plan should be reviewed and revised annually or more frequently in response to changes in the assessed risk.

IRS management explained that a disaster recovery plan and risk management plan were not developed for the data communications network because they were notified by the Department of the Treasury that critical assets were going to be reidentified by the National Critical Infrastructure Assurance Office. However, the IRS has not received any updated listing of its critical assets. The CIP Program efforts have also stalled to some extent since the stand-up of the Department of Homeland Security (DHS), which resulted in the former Department of the Treasury's Critical Infrastructure Protection Officer transferring to the DHS.

Recommendation

4. The Chief, Information Technology Services, should complete the additional disaster recovery and risk management measures outlined in the IRS' CIP Program for the data communications network.

Management's Response: The Enterprise Networks organization will partner with the End User Equipment and

Services organization to identify critical points of failure within the IRS' local area networks. The Enterprise Networks organization will also provide the names, responsible program areas, and contact number of its management team to be included in site-specific disaster recovery plans.

As the Treasury Communications System will soon be replaced with the Treasury Communications Enterprise (TCE) managed services contract, all future risk assessments of the wide or local area network(s) should be processed under the TCE umbrella. The Enterprise Networks organization will begin transitioning to the TCE in Fiscal Year 2005.

Significant Investments to Enhance Network Availability and Recovery Capability Should Require a Cost-Benefit Analysis

OMB Circular A-130 requires that agencies take cost-effective steps to manage any disruption of service in the event of a disaster. In addition, the Clinger-Cohen Act of 1996[15] (also referred to as the Information Technology Management Reform Act) requires each Federal Government agency to establish effective and efficient capital planning processes for selecting, managing, and evaluating the results of all its major investments in information systems.

According to the NIST, agencies should perform a cost-benefit analysis to identify the optimum recovery strategy. The cost-benefit analysis should include the following for each alternative considered:

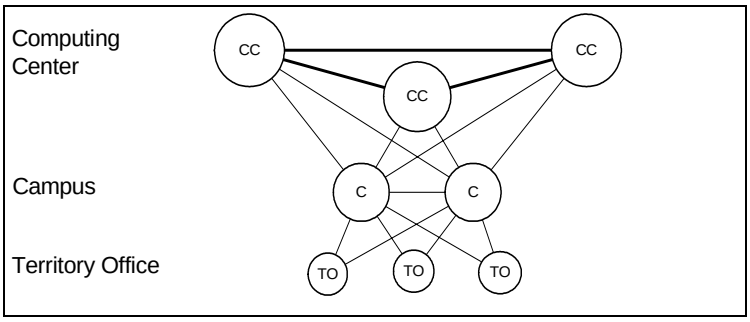
- Assumptions and constraints of the business need/problem.
- A description of the alternative being considered.
- The benefits and costs on a full life-cycle basis.
- A risk analysis that addresses both technical and organizational risk.

In April 2000, a team of IRS network engineers and contracted consultants prepared the proposal for the IRS'

[15] Pub. L. No. 104-106, 110 Stat. 642 (codified in scattered sections of 5 U.S.C., 5 U.S.C. app., 10 U.S.C., 15 U.S.C., 16 U.S.C., 18 U.S.C., 22 U.S.C., 28 U.S.C., 29 U.S.C., 31 U.S.C., 38 U.S.C., 40 U.S.C., 41 U.S.C., 42 U.S.C., 44 U.S.C., 49 U.S.C., 50 U.S.C.).

current ATM/Frame Relay[16] data communications network. The network topology in Exhibit 2 shows the hierarchal ATM network design for connections among the computing centers, campuses, and Territory Offices. The posts-of-duty have Frame Relay connectivity to the Territory Offices.

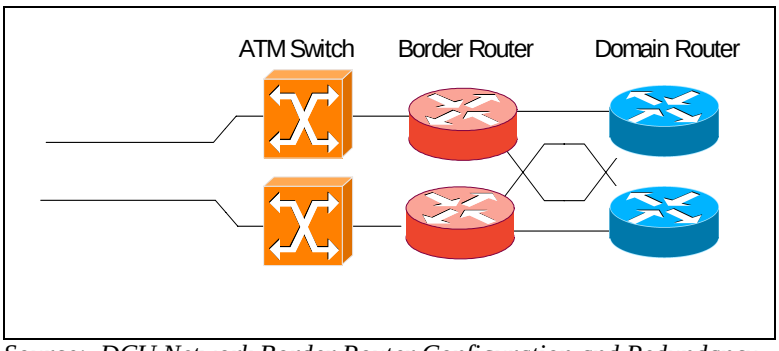
Exhibit 2: Network Topology



Source: DCU Network Border Router Configuration and Redundancy Design, dated April 20, 2000.

The goal was to design a consistent, highly available system architecture that could be scaled to meet the current and future requirements. As illustrated in Exhibit 3, the design provided for standardization of the border router configuration within the IRS network and redundancy at each of the border router locations. The switches are paired with the border routers to avoid single points of failure and to provide more than one access point into the ATM service provider.

Exhibit 3: Network Border Router Configuration



Source: DCU Network Border Router Configuration and Redundancy Design, dated April 20, 2000.

[16] Frame Relay is a high-speed protocol suited for data and image transfer.

The design provided for the capability that, in the event of a failure in the primary or secondary communication path, the unaffected path would provide alternate routing access and recovery. While the vendor concluded that the proposed design and configuration presented the least amount of complexity and cost while delivering the maximum level of capabilities and benefits, the IRS did not prepare a formal cost-benefit analysis. Instead, the IRS engaged the vendor to assess the old network, propose a new network design, and provide cost estimates for the new ATM/Frame Relay network.

The proposed ATM/Frame Relay data communications network was estimated to cost $4.9 million and was largely comprised of the vendor's products and equipment. Not conducting a formal cost-benefit analysis may have resulted in the IRS not selecting the most feasible or cost-effective data communications network design and recovery strategy that would support the needs of the business units. IRS management explained that an immediate and significant upgrade to the data communications network was necessary at the time and that the absence of a cost-benefit analysis occurred primarily because they did not consider the redesign of the network to be a separate information technology investment project.

IRS management recognizes that, while there is a strong argument in favor of ease of operations and management to use a single vendor environment, it hinders their ability to leverage the IRS' purchasing power. In fact, the Enterprise Networks organization is actively assessing its data communications network to implement improvements while reducing operational costs. For example, a current IRS project is tasked with optimizing the data communications network since it was based on the IRS' organizational structure prior to the reorganization, which has resulted in architectural inefficiencies and operational issues.

One of the effectiveness measures identified by the project is to identify potential cost savings opportunities (e.g., reduced hardware, circuits, etc.). This effort should also include assessing the use of the bi-directional rings that provide diverse traffic routing at some IRS locations. Our site survey results showed that a bi-directional ring

connecting the Campus and Territory Office in Atlanta was not being used as advantageously as possible. For example, the Territory Office currently does not use the bi-directional ring for routing its data traffic; instead, the data are being sent over a separate circuit. By implementing a solution that would permit the Territory Office to shift its data traffic to the bi-directional ring, management could remove the circuit and realize potential cost savings of $315,000[17] over 5 years.

Recommendations

The Chief, Information Technology Services, should ensure:

5. A cost-benefit analysis is prepared for projects redesigning the network architecture that result in a significant investment.

Management's Response: The Enterprise Networks organization will develop a suite of business case and alternative analysis processes for evaluating significant investment projects, which will be used as a critical decision factor in all recommendations and approvals.

6. The current IRS project tasked with optimizing the data communications network also assesses the use of the bi-directional rings.

Management's Response: The Engineering Branch of the Enterprise Networks organization will include the use and evaluation of bi-directional rings when optimizing the data communications network.

[17] The potential cost savings of $315,000 would be reduced by any additional costs to implement the solution.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service (IRS) developed and tested an effective telecommunications disaster recovery strategy. To accomplish this objective, we:

I. Reviewed the policies and procedures for completing a cost-benefit analysis during the development of a disaster recovery strategy to ensure redundancy and resiliency in the data communications architecture. We interviewed management and reviewed studies and analyses completed to establish the recommended disaster recovery strategy to determine whether a cost-benefit analysis was used to select the most efficient disaster recovery option. We also reviewed the IRS' network topology to determine if the selected strategy was incorporated into the current data communications architecture.

II. Reviewed the policies and procedures for developing and updating disaster recovery plans. We interviewed management at the visited sites about the preparation of a disaster recovery plan for telecommunications and about the effectiveness and efficiency of the current disaster recovery architecture. We also reviewed the disaster recovery plans at the visited sites to determine their adequacy and completeness for prompt recovery of data communications in the event of a disaster. In addition, we determined if measures were implemented to ensure uninterrupted telecommunications and reviewed the network topology to assess whether single points of failure had been sufficiently eliminated.

III. Reviewed the policies and procedures for conducting disaster recovery tests and evaluating test results. In addition, we reviewed the disaster recovery test plans, test results, and test schedule at each site to identify the extent to which the disaster recovery capabilities for telecommunications were tested and whether identified deficiencies have been adequately addressed. At each site, we also identified training provided to the telecommunications disaster recovery staff related to their disaster recovery responsibilities.

IV. Reviewed the policies and procedures for the Critical Infrastructure Protection (CIP)[1] Program to determine what additional actions the IRS requires for its critical assets. In addition, we interviewed management and reviewed documents prepared by the IRS to meet CIP Program requirements related to telecommunications.

[1] The CIP Program is a national effort to assure the security of the nation's critical infrastructure, which includes systems essential to the minimum operations of the economy and Federal Government, such as telecommunications, banking and finance, energy, and transportation.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Gary Hinkle, Director
Danny Verneuille, Audit Manager
Paul Mitchell, Senior Auditor
Van Warmke, Senior Auditor
Olivia Jasper, Auditor
Linda Screws, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief, Information Technology Services OS:CIO:I
Director, End User Equipment and Services OS:CIO:I:EU
Director, Enterprise Networks OS:CIO:I:EN
Acting Director, Portfolio Management OS:CIO:R:PM
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Management Controls OS:CFO:AR:M
Audit Liaisons:
- Chief, Information Technology Services OS:CIO:I
- Director, End User Equipment and Services OS:CIO:I:EU
- Director, Enterprise Networks OS:CIO:I:EN
- Manager, Program Oversight and Coordination OS:CIO:R:PM:PO

Appendix IV

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. This benefit will be incorporated into our Semiannual Report to the Congress.

Type and Value of Outcome Measure:

- Cost Savings, Funds Put to Better Use – Potential; $315,000 (see page 11).

Methodology Used to Measure the Reported Benefit:

We reviewed the use of the bi-directional ring[1] connecting the Campus[2] and Territory Office[3] in Atlanta, Georgia. We determined that by shifting the Territory Office's data traffic to the bi-directional ring, management could remove the current circuit for data traffic and realize potential cost savings of $315,000[4] over 5 years.

Description	Amount
Estimated average current monthly recurring charge of circuit used for data traffic at the Territory Office.	$5,700
Estimated monthly recurring charge for using the bi-directional ring.	<$450>
Estimated monthly savings by shifting the data traffic to the bi-directional ring.	$5,250
Estimated 5-year savings ($5,250 * 12 months * 5 years).	$315,000

[1] A bi-directional ring reroutes traffic in the other direction if the circuit is cut.
[2] The data processing arm of the Internal Revenue Service. The campuses process paper and electronic submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.
[3] Territory Offices serve taxpayers within a specified geographical area.
[4] The potential cost savings of $315,000 would be reduced by any additional costs to implement the solution.

Appendix V

Status of Additional Measures by Site to Ensure Uninterrupted Data Communications

Checks [✓] represent those measures implemented at the site.					
Measure	**Comments**	**Martinsburg Computing Center[1]**	**Tennessee Computing Center**	**Atlanta Campus[2]**	**Atlanta Territory Office[3]**
1. Risk Assessment	All sites had risk assessments completed on their networks within the last 3 years.	✓	✓	✓	✓
2. Backup Power Source	Each of the sites had an uninterruptible power supply device and generator.	✓	✓	✓	✓
3. Multiple Demarcation Points[4]	The Martinsburg Computing Center consisted of two buildings. Each building had a demarcation point, and there was a separate fiber cable connecting the two buildings to provide redundancy.	✓			
4. Spare Parts Inventory	All sites maintained some spare parts for repairs.	✓	✓	✓	✓
5. Service Level Agreements With Vendors	All sites had a service level agreement with vendors for repairs.	✓	✓	✓	✓
6. Redundant Circuits	All sites had redundant circuits for network connectivity.	✓	✓	✓	✓
7. Network Diversity	All sites used bi-directional ring topology[5] or microwave[6] to provide network diversity.	✓	✓	✓	✓

[1] Internal Revenue Service (IRS) computing centers support tax processing and information management through a data processing and telecommunications infrastructure.
[2] The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.
[3] Territory Offices serve taxpayers within a specified geographical area.
[4] The demarcation point is the interface location for telecommunications at the customer's premises.
[5] A bi-directional ring topology reroutes traffic in the other direction if the circuit is cut.
[6] Microwave is a point-to-point, free-space technology providing an alternative to a fiber-based network.

Checks [✓] represent those measures implemented at the site.					
Measure	**Comments**	**Martinsburg Computing Center**	**Tennessee Computing Center**	**Atlanta Campus**	**Atlanta Territory Office**
8. Multiple Carriers[7]	Except for the Martinsburg Computing Center,[8] all sites had only one local carrier for their data communications circuits.	✓			
9. System Backups	All sites were backing up critical files and storing them at their off-premises location.	✓	✓	✓	✓
10. Off-premises Storage of Documentation	All sites stored system recovery documentation at their off-premises location.	✓	✓	✓	✓

Source: The Treasury Inspector General for Tax Administration's review of Internal Revenue Service documents and management discussions.

[7] A carrier is a telecommunications company that provides communications transmission services to the public.
[8] The Martinsburg Computing Center had microwave in addition to wire circuits for data communications, which was provided by a different carrier.

Appendix VI

Status of Site Disaster Recovery Plans for Data Communications

Checks [✓] represent those items contained in the site's disaster recovery plan.				
Plan Requirement and Description	**Martinsburg Computing Center[1]**	**Tennessee Computing Center**	**Atlanta Campus[2]**	**Atlanta Territory Office[3]**
1. **Recovery Strategy Overview** – A description of the methods that provide recovery capability over the full spectrum of incidents.	✓	✓	✓	✓
2. **Recovery Team Information** – The name, role, and telephone number for the recovery team leaders and members.	✓	✓	✓	✓
3. **Notification Procedures** – A description of the methods used to notify recovery personnel during business and nonbusiness hours.	✓	✓	✓	✓
4. **Recovery Team Responsibilities** – An overview of team member roles and responsibilities in a contingency situation.	✓	✓	✓	✓
5. **Recovery Priorities** – A prioritized sequence of recovery activities based upon the business impact analysis.				✓
6. **Restoration Procedures** – Step-by-step procedures in sequential order to restore data communications.				
7. **Vendor and Supplier Information** – The name, address, and telephone number of telecommunications vendors and suppliers.	✓			✓
8. **Critical Telephone List** – The name and telephone number of other critical personnel that may be needed during the recovery process.	✓	✓	✓	✓
9. **Network/Circuit Diagrams** – High- and low-level topologies that depict the interconnectivity between networks.	✓			✓

[1] Internal Revenue Service (IRS) computing centers support tax processing and information management through a data processing and telecommunications infrastructure.
[2] The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.
[3] Territory Offices serve taxpayers within a specified geographical area.

Additional Disaster Recovery Planning, Testing, and Training Are Needed for Data Communications

Checks [✓] represent those items contained in the site's disaster recovery plan.				
Plan Requirement and Description	**Martinsburg Computing Center**	**Tennessee Computing Center**	**Atlanta Campus**	**Atlanta Territory Office**
10. **Hardware and Software Inventory** – A listing of physical hardware (i.e., circuits, routers, and switches) and computer software.				
11. **System Backup Requirements** – File backup frequency and rotation schedule for critical files stored at the off-premises facility.		✓		✓
12. **Listing of Internet Protocol (IP)**[4] **Addresses and Circuits** – A listing of the IP addresses and circuits for both the facility and other supported sites.	✓			
13. **Off-premises Storage Information** – The name, address, and telephone number of the off-premises storage facility.		✓		✓
14. **Record of Changes** – A record of plan modifications that includes the page number, change comment, and date of change.				

Source: The National Institute of Standards and Technology Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, the Internal Revenue Service's Internal Revenue Manual and Disaster Recovery Plan Template, and the Treasury Inspector General for Tax Administration's review of site disaster recovery plans.

[4] A Department of Defense standard protocol designed for use in interconnected systems of computer communications networks.

Appendix VII

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

RECEIVED
MAR 30 2004

March 30, 2004

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: W. Todd Grams WTG
Chief Information Officer

SUBJECT: Management Response to Draft Audit Report - Additional Disaster Recovery Planning, Testing, and Training Are Needed for Data Communications (Audit # 200320019)

The Internal Revenue Service's (IRS) Modernization and Information Technology Services (MITS) organization is committed to providing technology services that the IRS can depend on in its day-to-day operations. MITS places a high priority on ensuring that the IRS can rapidly recover its data communications network following a disaster.

As acknowledged in your report, the Enterprise Networks organization is responsible for managing the design and engineering of the telecommunications environment, which includes approximately 181,500 network devices and 1,200 network connection addresses. To maximize the recovery process and minimize lost production time of the data communications network, the Service must ensure that its disaster recovery (DR) plans for each site are complete, adequately tested, and have sufficiently trained employees.

The Service has taken several measures to reduce the vulnerability of the network. These include off-premises storage of network documentation, network system backups, installation of an uninterruptible power supply, and the identification of single points of failure within the network. Adequate circuit redundancy and diversity is available in the wide area network to support the as-built architecture.

IRS acknowledges the potential costs savings of $315,000 over five years. We address the report's six recommendations in our attached management response. We are advising that none of the material in the draft report warrants protection under the Freedom of Information Act or other applicable laws.

If you have questions, please call me at (202) 622-6800, or have your staff call Thomas C. Mulcahy of the Program Oversight Office, at (202) 283-6063.

Attachment

1

Management Response to Draft Audit Report – Additional Disaster Recovery Planning, Testing, and Training Are Needed for Data Communications (Audit # 200320019)

IDENTITY OF RECOMMENDATION #1:

The Associate Chief Information Officer for Information Technology Services should ensure that each site reviews the disaster recovery plan for completeness and accuracy quarterly or whenever significant changes occur to any plan element.

CORRECTIVE ACTION #1a:

The Martinsburg Computing Center (MCC) and Tennessee Computing Center (TCC) developed a process to perform quarterly reviews. The first review will be completed by April 1, 2004.

IMPLEMENTATION DATE:

COMPLETED February 27, 2004 PROPOSED _____

RESPONSIBLE OFFICIAL(S):

Chief Information Officer (CIO)
Associate CIO for Information Technology Services
Director, Enterprise Networks OS:CIO:I:EN

CORRECTIVE ACTION MONITORING PLAN #1a:

Local Enterprise Networks management at MCC and TCC will review the quarterly updates to the Disaster Recovery (DR) Plan to ensure appropriate action has been taken to correct the underlying deficiency. Local management will report on the progress quarterly until all deficiencies in the plan are removed. All reports will be forwarded to the Associate Chief Information Officer for Information Technology Services.

CORRECTIVE ACTION #1b:

The Atlanta Territory Manager implemented a controlled response process to ensure their DR Plan was reviewed. The responses are due March 31, June 30, September 30, and December 31 requiring verification that each team has met and their respective DR Plans have been reviewed for accuracy. We have added a *Plan Changes or Reviews* sheet to the plans for the purpose of documenting all changes and reviews to the plans.

IMPLEMENTATION DATE:

COMPLETED February 27, 2004 PROPOSED _____

RESPONSIBLE OFFICIAL(S):

Chief Information Officer (CIO)
Associate CIO for Information Technology Services
Director, End User Equipment and Services OS:CIO:I:EU

CORRECTIVE ACTION MONITORING PLAN #1b:

The monitoring plan is provided through the Atlanta Territory control box. The required action is directed from the Atlanta Territory Manager to Telecom A (campus) and Telecom B (Summit and PODs). The territory analyst monitors the controls daily and requires a response for all due actions. These actions have been placed in the control box and are due quarterly, March 31, June 30, September 30, and December 31.

IDENTITY OF RECOMMENDATION #2:

The Associate Chief Information Officer for Information Technology Services should ensure that each site periodically trains employees in their disaster recovery roles and responsibilities.

CORRECTIVE ACTION #2a:

While MCC is in compliance with this recommendation, both MCC and TCC will conduct yearly training sessions beginning in September 2004 during the pre-planning phase for this year's Disaster Recovery exercise.

IMPLEMENTATION DATE:

COMPLETED February 27, 2004 PROPOSED _____

RESPONSIBLE OFFICIAL(S):

Chief Information Officer (CIO)
Associate CIO for Information Technology Services
Director, Enterprise Networks OS:CIO:I:EN

CORRECTIVE ACTION MONITORING PLAN #2a:

Local Enterprise Networks management at MCC and TCC will ensure that the appropriate training measures are taken to correct the underlying deficiency. Local management will report on the progress in October 2004 once the annual training has been conducted. All reports will be forwarded to the Associate Chief Information Officer for Information Technology Services.

CORRECTIVE ACTION #2b:

The Atlanta Campus and Atlanta Territory Manager will coordinate with the Mission Assurance Office to ensure annual DR testing is conducted. The Atlanta Territory Manager will also ensure that Telecommunications conducts an independent biannual DR table exercise with documentation included in the plan. This will fall under the purview of the Territory Management Control.

IMPLEMENTATION DATE:

COMPLETED _____ PROPOSED October 1, 2004

RESPONSIBLE OFFICIAL(S):

Chief Information Officer (CIO)
Associate CIO for Information Technology Services
Director, End User Equipment and Services OS:CIO:I:EU

CORRECTIVE ACTION MONITORING PLAN #2b:

The monitoring plan is provided through the Atlanta Territory control box. The required action is directed from the Atlanta Territory Manager to Telecom A (campus) and Telecom B (Summit and PODs). The territory analyst monitors the controls daily and requires a response for all due actions. These actions have been placed in the control box and are due biannually, March 31 and September 30.

IDENTITY OF RECOMMENDATION #3:

The Associate Chief Information Officer for Information Technology Services should ensure that each site performs at least one exercise of each disaster recovery plan element annually.

CORRECTIVE ACTION #3a:

Testing at the Martinsburg Computing Center (MCC) and Tennessee Computing Center (TCC) is conducted more frequently than on an annual basis. This includes participation in disaster recovery of other systems (e.g. Mainframe DR exercise). Testing for this calendar year will be conducted by December 1, 2004.

IMPLEMENTATION DATE:

COMPLETED _____ PROPOSED December 1, 2004

RESPONSIBLE OFFICIAL(S):

Chief Information Officer (CIO)
Associate CIO for Information Technology Services
Director, Enterprise Networks OS:CIO:I:EN

CORRECTIVE ACTION MONITORING PLAN #3a:

Local Enterprise Networks management at MCC and TCC will ensure that the DR Plan continues to be tested on an annual basis. Local management will report on the progress in December 2004 after the annual exercise has been conducted. All reports will be forwarded to the Associate Chief Information Officer for Information Technology Services.

CORRECTIVE ACTION #3b:

The Atlanta Campus and Atlanta Territory Manager will coordinate with the Mission Assurance Office to ensure annual DR testing is conducted. The Atlanta Territory Manager will also ensure that Telecommunications conducts an independent biannual DR table exercise with documentation included in the plan. This will fall under the purview of the Territory Management Control.

IMPLEMENTATION DATE:

COMPLETED _____ PROPOSED October 1, 2004

RESPONSIBLE OFFICIAL(S):

Chief Information Officer (CIO)
Associate CIO for Information Technology Services
Director, End User Equipment and Services OS:CIO:I:EU

CORRECTIVE ACTION MONITORING PLAN #3b:

The monitoring plan is provided through the Atlanta Territory control box. The required action is directed from the Atlanta Territory Manager to Telecom A (campus) and Telecom B (Summit and PODs). The territory analyst monitors the controls daily and requires a response for all due actions. These actions have been placed in the control box and are due biannually, March 31 and September 30.

IDENTITY OF RECOMMENDATION #4:

The Associate Chief Information Officer for Information Technology Services should complete the additional disaster recovery and risk management measures outlined in the IRS' CIP program for the data communications network.

CORRECTIVE ACTION #4:

Enterprise Networks will partner with the End User and Equipment Services organization to identify critical points of failure within the IRS local area networks. Enterprise Networks will also provide the names, responsible program areas, and contact number of its management team to be included in site-specific disaster recovery plans.

Adequate circuit redundancy and diversity is available in the wide area network to support the as-built architecture. As the Treasury Communications System (TCS) will soon be replaced with the Treasury Communications Enterprise (TCE) managed services contract, all future risk assessments of the wide or local area network(s) should be processed under the TCE umbrella. Enterprise Networks will begin transitioning to TCE in FY05.

IMPLEMENTATION DATE:

COMPLETED _____ PROPOSED December 1, 2005

RESPONSIBLE OFFICIAL(S):

Chief Information Officer (CIO)
Associate CIO for Information Technology Services
Director, Enterprise Networks OS:CIO:I:EN

CORRECTIVE ACTION MONITORING PLAN #4:

The Director, Enterprise Networks will provide a bi-annual report to the CIO regarding the status of these actions.

IDENTITY OF RECOMMENDATION #5:

The Associate Chief Information Officer for Information Technology Services should ensure that a cost-benefit analysis is prepared for projects redesigning the network architecture that result in a significant investment.

CORRECTIVE ACTION #5:

The Enterprise Networks organization recognized the need for performance improvement in this area. Enterprise Networks retained a skilled contractor to develop a suite of business case and alternative analysis processes to be used in evaluating significant investment projects. The summary of requirements for this development process is the deliverable that must include the related requirements of the Internal Revenue Service Enterprise Life Cycle (ELC) LITE, as well as other significant information recommended by the Chief Financial Officer. The intended outcome is the required use of an automated process where, using size/cost/complexity guidelines, a pre-defined "spreadsheet" (small/medium/large) would be completed. The outcome (a business case/alternative analysis) would become a necessary part of all significant projects. It will be used as a critical decision factor in all recommendations and approvals.

IMPLEMENTATION DATE:

COMPLETED _____ PROPOSED February 1, 2005

RESPONSIBLE OFFICIAL(S):

Chief Information Officer (CIO)
Associate CIO for Information Technology Services
Director, Enterprise Networks OS:CIO:I:EN

CORRECTIVE ACTION MONITORING PLAN #5:

Not Applicable.

IDENTITY OF RECOMMENDATION #6:

The Associate Chief Information Officer for Information Technology Services should ensure that the current IRS project tasked with optimizing the data communications network also assesses the use of the bi-directional rings.

CORRECTIVE ACTION #6:

The Engineering Branch of the Enterprise Networks organization will include the use and evaluation of bi-directional rings when optimizing the data communications networks, when the use of such rings is an appropriate resolution of the problem. The evaluation of the ring solution, when it is a part of the evaluation, is included in the recommended approval process. (This will also be an outcome of implementing corrective active #5.)

IMPLEMENTATION DATE:

COMPLETED March 3, 2004 PROPOSED _____

RESPONSIBLE OFFICIAL(S):

Chief Information Officer (CIO)
Associate CIO for Information Technology Services
Director, Enterprise Networks OS:CIO:I:EN

CORRECTIVE ACTION MONITORING PLAN #6:

Not Applicable.