



*The Internal Revenue Service Adequately
Protected Sensitive Data and Restored
Computer Operations After the Flooding of
Its Headquarters Building*

January 26, 2007

Reference Number: 2007-20-023

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:

3(d) = Identifying Information - Other Identifying Information of an Individual or Individuals

Phone Number | 202-927-7037

Email Address | Bonnie.Heald@tigta.treas.gov

Web Site | <http://www.tigta.gov>



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

January 26, 2007

MEMORANDUM FOR CHIEF, AGENCY-WIDE SHARED SERVICES

FROM: *Michael R. Phillips*
Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building (Audit # 200620041)

This report presents the results of our review to evaluate the actions taken by the Internal Revenue Service (IRS) in response to the flooding of its Headquarters building. Specifically, we determined whether the IRS adequately protected data and computer operations and sufficiently recovered its computer systems and data damaged or disrupted by the flooding. The Senate Finance Committee requested that the Treasury Inspector General for Tax Administration determine the extent and nature of disruption to IRS operations and identify the functions and locations that have been most affected as a result of the flooding. This audit is one of three reviews that the Treasury Inspector General for Tax Administration initiated to answer the Senate Finance Committee's request.

Impact on the Taxpayer

The flooding disaster at the IRS Headquarters building in Washington, D.C., could have resulted in the loss of taxpayer data and disruption in computer operations. However, due to preparatory and responsive actions, the IRS adequately protected sensitive data in the aftermath of the flooding and restored computer operations for its Headquarters employees.

Synopsis

A rare tropical deluge over the Washington, D.C., metropolitan area on June 24 and 25, 2006, unleashed floods of water that swamped the Federal Triangle area of the nation's capital and forced an estimated 3 million gallons of water into the basement and subbasement of the IRS Headquarters building at 1111 Constitution Avenue, NW. Due to cleanup activities, health



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

concerns, and the lack of electricity and ventilation, the building was closed and could not be immediately reoccupied. The building reopened in December 2006. The Headquarters building houses more than 2,200 employees from various IRS business units, including many top-level management officials.

Perimeter security was always maintained at the Headquarters building, and entry was tightly controlled after the flooding occurred. As a result, taxpayer data stored in the entire building were adequately protected against the risk of unauthorized access. In addition, damaged equipment and destroyed taxpayer data stored in the basement were properly protected and disposed of.

A little more than 1 month after the flooding, the Agency-Wide Shared Services Division had completed workstation space arrangements for displaced employees in 15 different locations in the District of Columbia, Maryland, and Virginia. Within the same time period, the Modernization and Information Technology Services (MITS) organization had located unassigned computers for those employees without computers, configured the computers to fit each employee's needs, and provided technical support to allow employees to reconnect to the IRS network.

The MITS organization restored computer infrastructure operations that existed in the Headquarters building prior to the flooding. A Wage and Investment Division computer application system, the only mainframe application operating out of the Headquarters building, was reestablished at a mainframe computer in another site within 2 calendar days after the flooding. Other critical servers¹ were moved from the Headquarters building to another IRS facility and restored for availability to employees within 8 calendar days after the flooding. Many other vital servers were moved and restored within 2 weeks after the flooding.

We commend the efforts of the IRS and believe the actions taken by the IRS protected taxpayer data and minimized the disruption of computer operations caused by the flooding. However, we found the tracking of computer assets removed from the building was not initiated timely. For example, several Wage and Investment Division servers were removed from the Headquarters building without the knowledge or approval of the MITS organization. These servers were temporarily stored overnight in non-IRS space. Also, the Criminal Investigation Division removed many servers from the building before the asset tracking system was implemented.

MITS organization employees were unable to perform a physical inventory validation of computers remaining in the building because the building was closed. However, now that the building has reopened, the annual physical inventory validation is scheduled to begin in

Taxpayer data stored in the entire building were adequately protected against the risk of unauthorized access. In addition, destroyed taxpayer data stored in the basement were properly protected and disposed of.

¹ A server is a computer that delivers information and software to other computers linked by a network.



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

January 2007. We encourage the completion of this inventory validation because it will provide documented evidence that all computers are properly accounted for.

Recommendation

The Chief, Agency-Wide Shared Services, should ensure the Incident Management Plans for all IRS locations include the implementation of an asset tracking system and related processes immediately after a disaster.

Response

The Chief, Agency-Wide Shared Services, agreed with our findings and recommendation. The Director, Agency-Wide Shared Services Employee Support Services, developed and implemented an Emergency Incident Asset Retrieval form, which has been incorporated into the Incident Management Plan Addendum. In addition, incident management planning was updated to include the asset tracking process, and training was provided to appropriate personnel. Management's complete response to the draft report is included as Appendix IV.

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.



*The Internal Revenue Service Adequately Protected Sensitive
Data and Restored Computer Operations After the Flooding of
Its Headquarters Building*

Table of Contents

Background	Page 1
Results of Review	Page 3
The Internal Revenue Service Adequately Protected Sensitive Data in the Aftermath of the Flooding Disaster	Page 3
<u>Recommendation 1:</u>	Page 8
The Internal Revenue Service Adequately Restored Computer Operations for Its Employees After the Flooding Disaster	Page 8
Appendices	
Appendix I – Detailed Objective, Scope, and Methodology	Page 10
Appendix II – Major Contributors to This Report	Page 11
Appendix III – Report Distribution List	Page 12
Appendix IV – Management’s Response to the Draft Report	Page 13



*The Internal Revenue Service Adequately Protected Sensitive
Data and Restored Computer Operations After the Flooding of
Its Headquarters Building*

Abbreviations

AWSS	Agency-Wide Shared Services
CI	Criminal Investigation
IRS	Internal Revenue Service
MITS	Modernization and Information Technology Services
TIGTA	Treasury Inspector General for Tax Administration
W&I	Wage and Investment



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

Background

A rare tropical deluge over the Washington, D.C., metropolitan area on June 24 and 25, 2006, unleashed floods of water that swamped the Federal Triangle area of the nation's capital and forced the closure of many Federal Government offices, including the Internal Revenue Service (IRS) Headquarters building at 1111 Constitution Avenue, NW. Electrical and maintenance equipment in the subbasement of the building was submerged in more than 20 feet of water. Also, the basement of the building, which contained additional electrical equipment, a health fitness facility, stored records, computer equipment, and vehicles garaged in the building, was partially submerged.



On early Monday morning, floodwaters submerge Constitution Avenue and engulf the IRS building. (Photo provided by the IRS)



The floodwaters surrounding the IRS building broke through windows in several rooms in the basement of the IRS building. (Photo provided by the IRS)

The IRS Headquarters building houses more than 2,200 employees from various IRS business units. Among these employees are the top-level management officials, such as the Commissioner and Deputy Commissioners.

On July 6, 2006, the Assistant Secretary for Management, Department of the Treasury, met with the Treasury Inspector General for Tax Administration (TIGTA) and expressed concern about how the IRS was responding to the disaster. On July 12, 2006, the ranking member of the Senate Finance Committee sent a letter to the Inspector General requesting that the TIGTA determine the extent and nature of disruption to IRS operations and identify the functions and locations that have been most affected by the flooding. As a result, the TIGTA Office of Audit initiated three audits to answer concerns about the flooding disaster at the IRS Headquarters building. This review focused on data security and computer operations, while the objectives of the other



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

reviews¹ relate to general business resumption efforts and determining the costs related to the flooding disaster.

This review was performed at the IRS National Headquarters in Washington, D.C.; the IRS Office of Chief Counsel at 950 L'Enfant Place, Washington, D.C.; the New Carrollton Federal Building at 5000 Ellin Road, Lanham, Maryland; and the IRS Real Estate and Facilities Management office at 2221 South Clark Street, Crystal City, Virginia, during the period July through October 2006. 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.

¹ *The Internal Revenue Service Building Flood Caused No Measurable Impact on Tax Administration* (draft report issued November 28, 2006) and *Replacement Costs for Flood Damage to the Internal Revenue Service National Headquarters* (Audit Number 200710031, Engagement letter issued November 30, 2006).



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

Results of Review

The Internal Revenue Service Adequately Protected Sensitive Data in the Aftermath of the Flooding Disaster

The flooding into the IRS' Headquarters building occurred on Sunday evening, June 25, 2006. The building was unoccupied at the time except for the usual security guards posted at the perimeter. A short-circuit in the electrical system caused by the flooding set off the fire alarm at 10:45 p.m., and a security guard contacted the IRS building manager. The building manager promptly went to the building to assess the situation. At that point, Constitution Avenue was under 3 feet of water. Within 2 hours of arriving, the building manager had arranged for water pumps to begin pumping water out of the basement. On Monday, June 26, 2 other firms, 1 under contract by the General Services Administration and another under contract by the IRS, joined the first group in the removal of an estimated 3 million gallons of water.

The IRS building manager notified the Incident Commander² of the flooding at 12:45 a.m. on Monday, June 26, 2006, and the Incident Commander contacted key management officials to advise them of the flooding and that the building would be closed for the day. At 3:01 a.m., the Incident Commander authorized a message to be sent to all IRS executives advising them of the flooding of the building. The Incident Commander enlisted the support of the IRS Communications Officer to contact the local media. By 3:37 a.m., all local television channels and a radio station had been contacted for public notification of the building closure. The announcement on the radio also included a contact telephone number for employees to call for additional information. In addition, a voice mail message was issued to all IRS District of Columbia employees advising them of the closure of the building for the day, and the IRS' official web site provided current information on the building closure. Also, on June 26, 2006, senior IRS leadership established operations in another local IRS building in accordance with the IRS Business Resumption Plan.³

As the water receded, it became apparent that all contents located in the basement had been damaged or destroyed. Doors had been forced from their hinges, some of the windows were broken, and furniture was piled into doorways. Many records were soaked and all computers were damaged. The highest water level in the basement reached approximately 5 feet. The

² An Incident Commander is directly responsible for frontline management of an incident. The Incident Commander, in conjunction with other onsite business team managers, will develop and implement response strategies and will use existing disaster preparedness documents for the recovery of business operations.

³ The IRS Business Resumption Plan provides guidelines for reestablishing operations after a disaster.



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

water depth in the small subbasement, containing electrical and maintenance equipment, was estimated at 20 feet.

Perimeter security was maintained at the building, and entry was tightly controlled after the flooding occurred

In the days following the flooding, the IRS placed additional security guards to prevent any unauthorized entry into the building. Physical access into the building was controlled through a single entry point. All employees entering the building were required to sign in and out. By Wednesday, June 28, 2006, it was determined by the Incident Commander and senior IRS executives that the building would be closed for an extended period of time. Because the building was secure at all times, taxpayer data maintained throughout the building were not at risk of unauthorized access.

Damaged equipment and destroyed taxpayer data stored in the basement were properly protected and disposed of

Unsalvageable records stored in the basement included over 100 boxes containing taxpayer and other personally identifiable information belonging to the Office of Chief Counsel and the Office of the Tax Exempt and Government Entities Division, personnel records of the Criminal Investigation (CI) Division,⁴ employee medical records maintained by the Health Unit, and Freedom of Information Act⁵ litigation documents. Based on potential health and contamination issues caused by the floodwaters and the fact that many of the documents with long-term retention periods were replicated in the records of United States District Attorneys and United States District Courts, the National Archives Records Administration approved the destruction of these records. On July 12, 2006, these records were destroyed by the document destruction company currently under contract with the IRS.

Employees of the primary cleaning contractor normally used by the IRS from an existing contract had been screened for suitability of employment; however, the additional 100 employees used for the emergency cleanup after the flood worked for a subcontractor and did not have security clearances. Cleaning of the flooded building was conducted around the clock, with the subcontractor employees working 12-hour shifts. These employees were required to sign in and out of the building and were restricted to the basement area. In addition, the primary contractor employees and the security guards on duty at the building monitored the cleaning activities. Given these circumstances and mitigating controls in place, we believe the use of unscreened contractors was appropriate to expedite cleanup efforts.

⁴ The CI Division is responsible for detecting and investigating criminal violations of the Internal Revenue Code and financially related crimes.

⁵ 5 U.S.C.A. § 552 (West Supp. 2003).



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

In addition to hardcopy files, Building Management function employees and contractors with offices in the basement had computers that were destroyed. These computers did not contain taxpayer information. The CI Division had three computers in the basement, one of which was used to issue credentials. The three damaged CI Division computers were taken to the CI Division laboratory for security purposes. The CI Division also had 12 new, unused notebook computers damaged by the flood. In addition, the Office of Chief Counsel had \$1.3 million of new, unused computer equipment stored in the basement. None of the new equipment contained taxpayer data. The new computers were disposed of by the contractor responsible for cleaning the basement area.

Tracking of computer assets removed from the building was not initiated timely, and computers were allowed to be taken out of the building without proper oversight and accountability

While the flooding disaster mainly affected the basement and subbasement floors, it indirectly affected the rest of the building because all electrical and ventilation equipment was damaged and would take months to repair or replace. In addition, summer weather temperatures and high humidity levels created concern about contamination and mold growth in the building. As a result, the entire building was closed and deemed unsuitable for employee occupancy.

To expedite the resumption of normal operations, the IRS allowed limited and escorted traffic into the building after the flooding. To account for and control building traffic, all persons entering and leaving the building were required to sign in and out. Employees were permitted to enter the building and remove personal items, files, and computers. For example, many employees who were assigned laptop computers entered the building to retrieve their computers. In some cases, IRS computer desktop support employees helped the employees pack their computers for shipment to the employees' new work locations. Some of the larger desktop computers were removed, but most of these computers remained in the building. The IRS provided replacement computers for these users at their new locations. Procedures for tracking computer assets in the event of a disaster had not been included in the IRS' Incident Management Plan.⁶

By Friday, June 30, 2006, the IRS had developed and implemented an asset tracking process to track the removal of assets, including equipment and records from the IRS Headquarters building. Modernization and Information Technology Services (MITS) organization⁷ managers requested that no computer equipment be moved except under controlled and secure conditions. In addition, employees who had already removed items were asked to retroactively complete the

⁶ An Incident Management Plan describes the overall coordinated actions to be taken by the Incident Management team to ensure recovery and restoration of a facility when an incident occurs.

⁷ The MITS organization is responsible for providing information technology support and services for the IRS by building and maintaining information systems that will help the IRS achieve its mission, objectives, and business vision.



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

asset tracking forms so inventory records would show the correct location for each item. To their credit, 148 employees completed the tracking forms, listing the equipment and items they had taken from the building between June 26 and June 29, 2006. According to these forms, 104 computers were removed, including 81 laptop computers. In total, employees removed 627 computers, including 464 laptop computers, from the Headquarters building.⁸

- On Wednesday, June 28, 2006, seven servers⁹ from the Wage and Investment (W&I) Division¹⁰ were removed from the Headquarters building by contractors and placed in a locked room within a secure but non-IRS building overnight without the knowledge or approval of the MITS organization. (b) (3)(d)

[REDACTED]

When the removal of the servers was discovered the following day, the MITS organization directed the W&I Division to immediately move these servers to a designated IRS building and the move was completed that same day. Before these computers were reconnected to the IRS network, the IRS tested the computers to ensure compliance with IRS security standards. The servers have been tracked to their current location.

- On Wednesday, June 28, 2006, and Thursday, June 29, 2006, employees from the CI Division removed 41 computer servers from the Headquarters building using a rented truck. The CI Division was able to move the computers before the asset tracking system was in place because the Division has its own computer staff and did not need assistance from the MITS organization. Prior to the removal of the equipment, the Chief, CI, obtained verbal authorization from the Chief, Agency-Wide Shared Services (AWSS).¹¹ The CI Division contends that the computer assets were always under its control and secure at all times, and it maintained documentation to verify that its computer assets were being tracked within the Division to their current locations.
- Many critical servers were moved to two different locations on Friday, June 30, 2006. Fifteen servers used by the W&I Division's Computer Assisted Publishing System¹² were moved by a contractor to the IRS Enterprise Computing Center in Martinsburg, West Virginia, where this equipment will remain permanently. The

⁸ The TIGTA obtained current inventory data on servers removed from the building through contacts with the affected IRS business units. We considered this information to be sufficient for achieving our audit objective.

⁹ A server is a computer that delivers information and software to other computers linked by a network.

¹⁰ The W&I Division services individual taxpayers and provides the information, support, and assistance these taxpayers need to fulfill their tax obligations.

¹¹ The AWSS Division provides administrative services to support IRS employees. These services include real estate and facilities management, procurements, equal employment opportunity, travel, and payroll and personnel.

¹² The Computer Assisted Publishing System provides computer resources to maintain a central printing and publication management organization for the development and distribution of published materials for 13 divisions of the IRS.



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

mainframe computer for this System, the only mainframe application operating out of the Headquarters building, was not moved and still resides in the Headquarters building. However, the application was reestablished on another mainframe computer at the Martinsburg location within 2 calendar days after the flooding. Thirty pieces of equipment, including 20 servers deemed critical to IRS operations, were moved the same day by a contractor to the computer room located in the IRS facility in Lanham, Maryland. Some servers provided shared storage space for several IRS business units, and others contained information vital to the Office of the Chief Financial Officer and to the Commissioner's staff. These two moves were performed securely, with inventory records prepared and verified throughout the moving process. The trucks were accompanied by CI Division special agents to ensure safe arrival at their destinations.

- One week later, on Friday, July 7, 2006, with 1 freight elevator in the building operational, IRS contract movers were able to more easily transfer 82 pieces of equipment, including 24 additional vital servers, from the Headquarters building to the computer room in the IRS facility in Lanham, Maryland, using required security and inventory controls.
- A review of IRS inventory records for the Headquarters building, as of August 15, 2006, showed that almost one-half of the servers assigned to the Headquarters building had not been scanned or modified after the date of the flooding event. While it is likely that many of these servers remain inside the building, we cannot be sure because the asset tracking system was not in place until 5 calendar days after the flooding.

Because the building was closed, MITS organization employees were unable to perform a physical inventory validation of the workstations and servers remaining in the building. The building reopened for occupancy December 8, 2006, and the IRS plans to begin its annual physical inventory in January 2007. We encourage the completion of this inventory validation because it will provide documented evidence that the computers are still located in the Headquarters building. We had made a similar recommendation during an audit on the IRS' efforts for Hurricanes Katrina and Rita.¹³ Specifically, we recommended the Chief Information Officer establish procedures to conduct a physical inventory validation of all computers at IRS facilities that suffer extensive damage after any major disaster, to identify possible loss or theft of computers. In addition, the report stated this validation should be performed within 30 calendar days after the disaster. Due to the closure of the Headquarters building, we were likewise unable to conduct a physical validation of computer assets located in the building.

¹³ *The Internal Revenue Service Successfully Accounted for Employees and Restored Computer Operations After Hurricanes Katrina and Rita* (Reference Number 2006-20-068, dated March 2006).



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

Recommendation

Recommendation 1: The Chief, AWSS, should ensure the Incident Management Plans for all IRS locations include the implementation of an asset tracking system and related processes immediately after a disaster.

Management's Response: The Chief, AWSS, concurred with the finding and recommendation. The IRS developed and implemented an Emergency Incident Asset Retrieval Tracking form, which has been incorporated into the Incident Management Plan Addendum. In addition, all written material concerning incident management planning has been updated to include asset tracking processes, and training was provided to appropriate personnel.

The Internal Revenue Service Adequately Restored Computer Operations for Its Employees After the Flooding Disaster

Because the flooding disaster damaged the electrical and ventilation functions of the building, employees were not allowed to work in the building, which required the IRS to locate temporary workspace for all displaced employees. This responsibility was assigned to the AWSS Division. Business Resumption Coordinators for each of the business units provided the Incident Commander with a prioritized list of employees who required space. The AWSS Division secured workstation space arrangements for the displaced employees in 15 different locations in the District of Columbia, Maryland, and Virginia.

In addition to finding workspace for displaced employees, the IRS needed to provide them with computer resources to resume tax administration activities and to move all computer infrastructure operations that existed in the building prior to the flooding. These responsibilities were assigned to the MITS organization. To this end, MITS organization employees worked many hours of overtime that resulted in overtime costs of about \$50,000.

Some employees who regained possession of their computers reported to work at other IRS offices and connected directly to the IRS network. For those employees who requested to temporarily work at home, IRS technicians installed secure connectivity software in their computers so these employees could connect to the IRS network.

For displaced employees who reported back to work but did not have computers with which to resume their duties, MITS organization personnel were tasked with locating unassigned computers, visiting the various worksites of displaced employees, and configuring computers to fit each employee's needs. With more than 2,200 displaced employees, this endeavor was daunting, yet the MITS organization provided all employees with assigned computers by July 28, 2006, a little over 1 month after the flooding occurred.



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

Additionally, the IRS provided network data and telephone lines in two new locations that were rented for the CI Division and Office of Chief Counsel staffs. Adaptive computer equipment required by some employees with special needs was moved to their temporary work locations.

As previously mentioned, the IRS moved many servers out of the Headquarters building to new locations. The MITS organization timely restored connectivity of these servers to the IRS network. For example, MITS organization personnel worked over the weekend to restore the critical servers removed from the building on June 30, 2006; the servers were restored by the following Monday, July 3, 2006 (8 calendar days after the flooding). Most of the vital servers moved on Friday, July 7, 2006, were placed into operation that weekend (2 weeks after the flooding). In addition, the connectivity of the W&I Division's Computer Assisted Publishing System was restored on another mainframe computer at the Enterprise Computing Center in Martinsburg, West Virginia, within 2 calendar days. Electronic mail servers and BlackBerry™ servers supporting Headquarters building employees were not located in the Headquarters building and were not affected by the flooding disaster.

Although the demands created by this disaster required additional equipment and services, the IRS did not request additional funding. We commend the efforts of the IRS and believe the actions taken by the IRS minimized the disruption caused by the flooding disaster.



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the actions taken by the IRS in response to the flooding of its Headquarters building. Specifically, we determined whether the IRS adequately protected data and computer operations and sufficiently recovered its computer systems and data damaged or disrupted by the flooding. To accomplish our objective, we:

- I. Determined whether the IRS protected taxpayer data during and after the flood.
 - A. Assessed the security of the IRS Headquarters building after the disaster.
 - B. Assessed the security of taxpayer records and computer equipment during cleanup activities.
- II. Determined whether the IRS sufficiently recovered its computer systems and data damaged or disrupted by the flooding.
 - A. Assessed whether the computer operations and related data were timely and adequately restored.
 - B. Assessed whether taxpayer records were being adequately protected by employees who were working in facilities outside the control of the IRS.



*The Internal Revenue Service Adequately Protected Sensitive
Data and Restored Computer Operations After the Flooding of
Its Headquarters Building*

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Stasha Smith, Lead Auditor
Charles Ekunwe, Senior Auditor
Myron Gulley, Senior Auditor



*The Internal Revenue Service Adequately Protected Sensitive
Data and Restored Computer Operations After the Flooding of
Its Headquarters Building*

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support
Chief Information Officer OS:CIO
Chief, Mission Assurance and Security Services OS:MA
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 Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
 Chief, Agency-Wide Shared Services OS:A
 Chief, Mission Assurance and Security Services OS:MA
 Director, Program Oversight OS:CIO:SM:PO



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

Appendix IV

Management's Response to the Draft Report

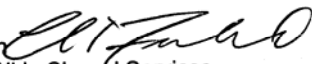


DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

RECEIVED
DEC 20 2006

DEC 20 2006

MEMORANDUM FOR MICHAEL R. PHILLIPS
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Carl T. Froehlich 
Chief, Agency-Wide Shared Services

SUBJECT: Draft Audit Report-The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building (Audit # 200620041)

I reviewed the subject report which was shared with other IRS organizations and concur with its content. During the business resumption process, we implemented additional procedures to better track the removal of assets, which are now part of our Incident Management Plans. Attached is our response to close the report recommendation.

I appreciate your commendation of our preparedness and performance in responding to this situation and our efforts in restoring computer operations and protecting data without adverse incident. While we acknowledge that some equipment was removed prior to asset tracking implementation, all equipment was subsequently accounted for and included in our tracking processes.

Each disaster or emergency poses different challenges. Our post-recovery activities have identified best practices resulting in our continuous improvement in the handling of situations. Hurricanes Katrina and Rita provided us valuable experience in reacting quickly and decisively, and demonstrated how we can more effectively execute our Incident Management Plans and infrastructure response. Our cumulative experiences served as our baseline to address the Headquarters flood situation.

If you have any questions, please call me at (202) 622-7500 or Stephen Kunze, Deputy Director, Employee Support, at (202) 283-9391. For matters addressing audit follow-up and liaison, please call Greg Rehak on (202) 622-3702.



The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building

RECOMMENDATION: The Chief, Agency-Wide Shared Services, should ensure the Incident Management Plans for all IRS locations include the implementation of an asset tracking system and related processes immediately after a disaster.

CORRECTIVE ACTION: IRS incorporated the use of Form 9167, Emergency Incident Asset Retrieval Tracking, in the Senior Commissioner Representative (SCR) Incident Management Plan Addendum. By using the form, the removal of assets during any disaster/emergency situation can be tracked and location(s) verified.

COMPLETED: July 31, 2006

RATIONALE FOR CLOSURE: By June 30, 2006 (four days after the building closed on June 26th), IRS developed and implemented Form 9167, Emergency Incident Asset Retrieval, and by July 31st, it was incorporated in the Incident Management Plan Addendum. All written material concerning Incident Management Planning has been updated to include asset tracking processes and training was provided to the SCRs and AOs. These actions will ensure that asset tracking system processes and procedures are in place for implementation during future disasters/emergencies.

RESPONSIBLE OFFICIAL: Director, AWSS Employee Support Services