156764

GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-271828

May 9, 1996

The Honorable Ted Stevens
Chairman
Committee on Governmental Affairs
United States Senate

Dear Mr. Chairman:

In our March 1996 testimony before your Committee on the Internal Revenue Service's (IRS) Tax Systems Modernization (TSM),[1] we identified significant physical security risks at IRS' data center, which is being planned to support a new electronic filing system called Cyberfile. This system is being developed for the IRS by the Department of Commerce's National Technical Information Service (NTIS). Our March 12, 1996, review of the data center–which according to the center's management was scheduled to be operationally ready on March 19, 1996–focused on seven functional areas where controls should have been in place by that time to mitigate security-related risks. We performed this review in response to your request that we determine whether IRS had incorporated adequate security measures for Cyberfile. However, because so many serious weaknesses were identified in about 1 hour, we did not continue with the in-depth review that we typically perform. Such a review, which we plan to perform before Cyberfile becomes operational, assesses physical security and software controls beyond obvious observations.

During our tour of the Cyberfile data center, we reviewed (1) data center operations, (2) physical security, (3) data communications management, (4) disaster recovery, (5) contingency planning, (6) risk analysis, and (7) security awareness. Our assessment incorporated control tests from GAO's Control and Risk Evaluation audit methodology, the Department of Defense Trusted Computer Systems Evaluation Criteria for controlled access protections, and federal standards and guidance from Federal Information Processing Standards Publications of the National Institute of Standards and Technology. Our March testimony provided

[1]Tax Systems Modernization: Management and Technical Weaknesses Must Be Overcome To Achieve Success (GAO/T-AIMD-96-75, March 26, 1996).

examples of the weaknesses we found in all seven areas. As agreed with your office, this letter provides a complete listing of the 49 weaknesses that we found.

DATA CENTER OPERATIONS

Effective data center operations include strong operational security safeguards to ensure the continuity of operations. We found 17 operational security weaknesses in a dusty construction environment that placed the equipment at operational risk.

1. Large amounts of combustible materials were found adjacent to and inside the data center. Paper and cardboard trash was piled in adjacent areas, and boxes of envelopes were stacked in the data center.

2. The data center's fire extinguishers required recharging and were haphazardly placed in the center, increasing vulnerability to extensive fire damage.

3. The center uses wet standpipe sprinklers for fire suppression in lower than normal ceilings. Taller individuals in the center have to duck to avoid hitting the sprinklers, which, if inadvertently sheared off, will release water that can damage the center.

4. The data center is located on the subbasement level of a building and does not have water detectors under the raised floor, increasing the risk of extensive electrical damage to computer equipment if the center floods.

5. Workstations have recordable drives that could be used to download taxpayer information or upload viruses.

6. An emergency power cut-off switch was not safeguarded against accidental cut-off or malicious tampering.

7. Equipment racks were not grounded, increasing the risk of electrical shock or fire.

8. Smoke detectors in the ceiling were not activated, increasing the risk of a major fire.

9. The center had no plans for a secured magnetic tape library, increasing the risk of potential data loss or extensive delays in data recovery.

10. Backup batteries were to be installed in an unventilated room, creating a potential health hazard from toxic fumes.

11. No wash facility was available for individuals should they accidentally come in contact with acid from the backup batteries.

12. Air induction panels on the outside of the data center walls provided easy access to the data center by unauthorized individuals.

13. Optical fiber lines for IRS and another building occupant were commingled in the same communications switch, exposing the IRS lines to risk of unauthorized access by the other occupant's personnel.

14. Foam used to stabilize cables in the floor could create a toxic fire hazard.

15. Cyberfile's uninterruptible power supply was housed in the other occupant's area, exposing it to risk of tampering by the other occupant's personnel.

16. The data center floor panels were open and electrical wires were exposed, increasing the risk of injury to personnel.

17. The data center equipment was operating while construction of the data center was taking place. The dusty environment, including high levels of drywall dust, placed the expensive and delicate computer and telecommunications equipment at significant risk of damage and failure.

PHYSICAL SECURITY

Physical security and access control measures, such as locks, guards, and surveillance cameras, are critical to safeguarding data and operations from internal and external threats. At the data center we found 14 physical security weaknesses.

18. The lock on the main door to the data center was improperly installed, exposing the mechanism and permitting unauthorized access by flipping the latch with a finger.

19. All doors to the data center had unsecured hinges on the outside, allowing easy removal of the doors to permit unauthorized entrance to the data center. During our walk through, the data center manager acknowledged that the doors had unsecured hinges. However, during our April 30, 1996, meeting, officials said that, of the center's external doors, two of three had secure hinges.

20. Multiple exit doors were not alarmed or monitored by security cameras, thereby allowing exit or entrance without detection.

21. Packages and other personal articles were not inspected before being allowed into the data center, increasing internal security threats. This leaves the center vulnerable to physical attack from concealed weapons as well as technical attack. For example, malicious software could be brought in to introduce viruses.

22. Electronic card key devices installed on doors in an environment without guards or cameras do not limit access to authorized personnel only. Unauthorized personnel can follow cardholders into the center and pose a threat to the equipment and taxpayer data.

23. Cigarettes were being smoked in the facility and we observed cigarette smoke and numerous butts in the piles of combustible materials.

24. A large hole made in the data center wall did not lead to the battery room, as data center personnel had stated. Instead, we found that it led to an area shared with the building's other occupant.

25. Background investigations required for personnel working on secure facilities had not been conducted for personnel doing construction, pulling communications wires, and setting up operations in the data center. These personnel worked for contractors and the building's other occupant.

26. Background investigations required for personnel working on sensitive systems had not been conducted for NTIS personnel working on Cyberfile applications in the production environment.

27. Personnel in the data center were not wearing any badges or other forms of identification to validate their authority to be in the data center.

28. Vendors were allowed unescorted access throughout the data center.

29. Contractor personnel told us they were developing and testing their software in the production environment. This should be performed in a separate development and test facility so that the production environment is not exposed to increased risk of sabotage and mishap due to errors. During our April 30, 1996, meeting, officials told us that contractors do not develop and test software in the data center.

30. The data center did not have a secure perimeter. Access to shared areas that completely encircle the data center was not controlled by NTIS, increasing the risk of sabotage to the facility.

31. Individuals entering the data center were asked to sign a log, but were not required to show valid identification.

DATA COMMUNICATIONS MANAGEMENT

Data communications management is the function of monitoring and controlling communications networks to ensure that they operate as intended, transmitting timely, accurate, and reliable data in a secure fashion to and from taxpayers. We found 10 communications management weaknesses at the data center.

32. Telecommunications equipment, such as telecommunication switches and patch panels, was not physically protected and could be accessed and damaged by unauthorized personnel.

33. A communications device intended to be used only to monitor data flow could also be used for altering data and for browsing.

34. Communications lines were mounted unprotected on the back wall of the data center instead of being enclosed in a secure telephone closet or box. This increased the risk of both malicious and unintentional communications disruptions.

35. No wiring plan for the communication lines was available to correlate the circuits with the wire locations. This makes it difficult to isolate particular circuits for maintenance and to restore communications after disruption.

36. Communications from other NTIS facilities, which we were told were dial-up lines, exposed the production environment to attack by individuals outside the facility. During our April 30, 1996, meeting, we were told that these communications lines were not dial-up, but were frame relay. Although frame relay is generally more secure than dial-up lines, it is still an exposure to the data center.

37. Communications cables running along the ceiling outside the data center were exposed, providing a readily accessible target to be cut or wiretapped.

38. A separate communications line observed running through the data center posed an undetermined risk since data center personnel could not identify its origin, destination, or purpose.

39. Patch panels, which can be used to redirect communications traffic, were installed at the data center, but no policies or procedures were established to

control their use. This increases the risk of communications disruptions caused by undisciplined patch panel operations.

40. A data communications block that was wired to route Cyberfile's Internet electronic filing traffic was also wired to route traffic for another application. Without additional information on how this block will be configured, there is a risk of communications disruptions from the other application.

41. Another data communications block that was wired to route Cyberfile's public switch telephone network traffic was also wired to route traffic for another application. Again, without additional information on how this block will be configured, there is a risk of communications disruptions from the other application.

DISASTER RECOVERY

Effective disaster recovery plans and procedures enable organizations to continue operations or to reestablish operations at a backup facility after disruptions caused by events such as earthquakes, floods, fires, and electrical power failures.

42. Cyberfile does not have a backup computer facility. If a disaster occurs at the data center, taxpayers will not be able to file electronically from personal computers.

43. Cyberfile does not have adequate alternate power sources to maintain computer operations during a power outage.

44. The data center does not have any building evacuation alarms to alert personnel and permit the orderly shut down of operations and safe evacuation of personnel.

CONTINGENCY PLANNING

Contingency planning specifies emergency procedures to restore critical operations and identifies the key individuals responsible for carrying out the procedures. NTIS has a draft contingency plan that provides some high-level instructions for maintaining continuous Cyberfile system operations.

45. The draft contingency plan does not have specific procedures to be followed in an emergency. For example, the action plan for recovering from fire damage calls for the initiation of proceedings for repair or replacement of damaged facilities and equipment, but does not specify how to accomplish this task.

46. The plan does not identify the key individuals responsible for executing specified procedures.

RISK ANALYSIS

A risk analysis identifies and determines the severity of security threats and, for each threat, formulates safeguards and estimates their cost. Without a comprehensive risk analysis, system vulnerabilities may not be identified and cost-effective controls may not be implemented to mitigate them.

47. The risk analysis conducted for Cyberfile was incomplete and did not adequately address physical, operational, and communications security threats to the data center. For example, despite the fact that the greatest risk to a data center is often attack by its own employees, the analysis does not address the threat of data center employees compromising taxpayer data.

SECURITY AWARENESS

A security awareness program communicates to employees the importance of security measures and emphasizes the employees' responsibility for protecting assets.

48. There was no security awareness program for Cyberfile.

49. Data center security practice was lax. For example, we found a note, written on a white board in the data center, instructing employees to hand off passwords to employees on the next shift. Because employees share passwords, system and data accesses and the use of system resources cannot be traced to individuals and, therefore, cannot be effectively controlled.

AGENCY COMMENTS AND OUR EVALUATION

The IRS Assistant Commissioner for Submission Processing provided us with written comments, which we discussed with IRS and NTIS officials on April 30, 1996. These comments have been incorporated where appropriate and are reprinted in the enclosure to this letter. IRS and NTIS officials told us that 32 of the 49 weaknesses we found during our tour of the Cyberfile data center had been corrected and that the remaining weaknesses would be corrected before tax processing begins.

- - - - -

We are sending copies of this report to the Ranking Minority Member of your Committee, interested congressional committees, the Secretary of the Treasury, and the Commissioner of Internal Revenue. Copies will also be made available to others upon request. If you or your staff have any questions about this letter, please contact me at (202) 512-6412.

Sincerely yours,

Dr. Rona B. Stillman
Chief Scientist for Computers
and Telecommunications

Enclosure

COMMENTS FROM THE INTERNAL REVENUE SERVICE

Note: GAO comments supplementing those in the report text appear at the end of this enclosure.

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

APR 29 1996

Dr. Rona B. Stillman
Chief Scientist for Computers
and Telecommunications
United States
General Accounting Office
Accounting and Information
Management Division
Washington, D.C. 20548

Dear Ms. Stillman:

This is in response to your draft letter to Senator Stevens addressing concerns with CyberFile, a new electronic filing system.

Your review of the CyberFile production site on March 12, 1996, identified several concerns and listed 49 weaknesses. We value your comments, however, you may not have been aware of all the facts.

See comment 1.

The statement by management at the data center that the system was scheduled for operation on March 19, 1996, was incorrect. On February 21, 1996, we determined the system would not be available for the traditional 1996 filing season, but that we would continue to explore options for limited filing in 1996. On March 1, 1996, this information was presented to the IRS executive committee and external partners.

The GAO review was conducted on a nonproduction site during the development phase. Most of the 49 cited concerns and weaknesses have been corrected. The attached list, prepared by National Technical Information Service (NTIS), addresses each of the 49 concerns, of which 32 have been corrected. The remaining 17 will be corrected in accordance with The Department of Treasury Security Manual, TD P 71-10; Automated Information System Security IRM 2(10)00, and Trusted Computer System Evaluation Criteria DOD 5200-28 STD, prior to live tax processing. In addition, we have contracted with the Tax Systems Modernization Institute (TSMI) for an independent assessment of the CyberFile system to provide a status of readiness.

It has always been the intent of IRS to meet all required physical and data security requirements. We maintain that the remaining issues can be resolved and we will continue to work with GAO to provide a secure system that accomplishes our common goals.

Dr. Rona B. Stillman

If you have any questions concerning this letter, please contact me, or a member of your staff may contact Donna Leach, of the Systems Support Section, at 202-283-1060.

Sincerely,

Peggy C Rule

Assistant Commissioner
(Submission Processing)

Enclosure
As Stated

NTIS Response to GAO April 1996 Letter
April 25, 1996

The GAO visited the CyberFile pilot facility well prior to any hand-off from the NTIS to IRS, much less actual operational readiness. It should be noted that NTIS staff only occupied the facility beginning in early February, 1996.

NTIS would never execute final turnover of a facility that was by NTIS' own determination an unsafe pilot, or did not meet the requirements spelled out for us. In addition, after turnover, IRS would have the opportunity to apply any additional security measures that it deemed necessary. Because of the timing of GAO's visit and the type of project in question, then, our responses to the issues raised by GAO fall in three categories. First, some of the issues raised by GAO clearly describe security issues that we understand and would address prior to any determination of operational readiness. These issues are identified below and if they have already been addressed, that is so stated. Second, some of the issues raised by GAO are appropriate security measures for a full production system, but had not been spelled out as requirements for the CyberFile pilot effort and may be excessive for a facility that is not expected to be used in other than a pilot capacity. Third, some of the issues raised by GAO may go beyond reasonable cost-benefit calculations of appropriate security even for a production facility. There is legitimate debate as to what burden of expense should be put on taxpayers to provide appropriate levels of security for the task at hand, particularly in the context of a limited pilot.

The IRS has always retained the option of moving the CyberFile functionality into one of its existing approved sites once the pilot has been demonstrated successfully. In that context it would be inappropriate to expend the taxpayer funds required to convert this pilot site to the higher standards necessary for permanent production.

Finally, it should be noted that NTIS was never presented with or briefed on this list of 49 items until April 25, 1996. All progress described against these concerns has been made according to our own determination of security requirements, as planned.

Itemized Responses:

1. Large amounts of combustible materials were found adjacent to and inside the data center. Paper and cardboard trash were piled in adjacent areas, and boxes of envelopes were stacked in the data center.

   On March 12 GAO found combustible material as a result of ongoing site construction. All construction ended on March 31 and the facility is free and clear of dust and debris or hazardous materials.

Additionally, GAO found envelopes that were temporarily being stored in the facility to support the mailing of acknowledgment letters. During the production of the CyberFile Pilot Program only a limited number of envelopes will be kept near the computer to fulfill the need of producing timely acknowledgment letters

2. The data center's fire extinguishers required recharging and were haphazardly placed in the center, increasing vulnerability to extensive fire damage.

NTIS has since installed in the facility properly mounted and charged fire extinguishers, mounted per fire code regulations. GAO examined fire extinguishers that were controlled solely by USDA.

3. The center uses wet standpipe sprinklers for fire suppression in lower than normal ceilings. Taller individuals in the center have to duck to avoid hitting the sprinklers, which, if inadvertently sheared off, will release water that can damage the center.

See comment 2.

According to Michael Sazonov (USDA Engineering), we have to install and use the wet standpipe fire suppression system for this computer facility.

4. The data center is located on the subbasement level of a building and does not have water detectors under the raised floor, increasing the risk of extensive electrical damage to computer equipment if the center floods.

True. The data center does not have water detectors. A proposal for the deployment of such a technology was submitted to IRS on 4/24/96.

5. Workstations have recordable CD-ROM and floppy drives that could be used to download taxpayer information or upload viruses.

There are no recordable CD-ROM devices nor have there ever been recordable CD-ROM devices at this site.

See comment 3.

Personal computers and workstations that are presently in the CyberFile computer center are there to support demonstrations, IRS SAT and office administration. During production, only diskless workstations are planned for this facility.

6. An emergency power cut-off switch was not safeguarded against accidental cut-off or malicious tampering.

See comment 4.

The emergency power cut-off switch is situated such that it could be readily accessed according to USDA Engineering, for safety purposes. This is in accordance and compliance with USDA Engineering and safety officials.

2

7. Equipment racks were not grounded, increasing the risk of electrical shock or fire.

True. This will be done in May.

8. Smoke detectors in ceiling were not activated, increasing the risk of a major fire.

The integrated smoke detection system was activated and tested on 4/23/96 as planned.

9. No plans for a secured magnetic tape library, increasing the risk of potential data loss or extensive delays in data recovery.

See comment 5.

The need for a tape library was identified last November. NTIS has a facility for offsite storage of data.

See comment 6.

10. Backup batteries were to be installed in an unventilated room, creating a potential health hazard from toxic fumes.

According to Liebert Corporation, the manufacturer of the UPS, lead calcium batteries do not require ventilation.

11. No wash facility was available for individuals should they accidentally come in contact with acid from the backup batteries.

See comment 6.

True. These batteries contain acid in a sealed unit. USDA Engineering states these batteries are approved for use in a computer room facility and pose no hazard.

12. Air induction panels on the outside of the data center walls provided easy access to the data center by unauthorized individuals.

The 20" panel is a transfer grill that returns air to the main handler and prevents over-pressurization of the space. To ensure unauthorized access is not permitted, steel bars will be installed.

13. Optical fiber lines for IRS and another building occupant were commingled in the same communications switch, exposing the IRS lines to risk of unauthorized access by the other occupant's personnel.

True. The IRS' optical fiber line is planned to be isolated by mid-summer. The vendor, MFS, is adding new fiber cable runs into the USDA building.

14. Foam used to stabilize cables in the floor could create a toxic fire hazard.

3

This foam was removed from the facility on April 11.

15. CyberFile's uninterruptible power supply was housed in the other occupant's area, exposing it to risk of tampering by the other occupant's personnel.

True. USDA Engineering has begun to develop a cost proposal to make the UPS tamper-proof. This document should be available by April 30.

16. The data center floor panels were open and electrical wires were exposed increasing the risk of injury to personnel.

The facility was still under construction on March 12.

17. The data center equipment was operating while construction of the data center was taking place. The dusty environment, including high levels of drywall dust, placed the expensive and delicate computer and telecommunications equipment at significant risk of damage and failure.

True. This situation no longer exists and there have been no known component failures as a result of this concern.

18. The lock on the main door to the data center was improperly installed, exposing the mechanism and permitting unauthorized access by flipping the latch with a finger.

True. There is a plan to replace this door by mid-May.

19. All doors to the data center had unsecured hinges on the outside, allowing easy removal of the doors to permit unauthorized entrance to the data center.

See comment 7.

There are three external doors to the CyberFile data center. Of those, two had secure hinges on 3/12. The secure hinges were installed on the third door the first week of April.

20. Multiple exit doors were not alarmed or monitored by security cameras, thereby allowing exit or entrance without detection.

True. Of the four doors in the facility, two emergency doors are currently alarmed and will only be used in event of emergency. One of the other doors which is an internal door, dividing lab and office area, will not be alarmed. The remaining door is an entry door to the office area protected by card key and door key devices and will not be alarmed since the facility is operated on a 24 x 7 basis.

4

21 Packages and other personal articles were not inspected before being allowed into the data center, increasing internal security threats. This leaves the center vulnerable to physical attack from concealed weapons, as well as technical attack. For example, malicious software could be brought in to introduce viruses.

True. Planned operational procedures will address this concern.

22. Electronic card key devices installed on doors in an environment without guards or cameras do not limit access to authorized personnel only. Unauthorized personnel can follow cardholders into the center and pose a threat to the equipment and taxpayer data.

True. Planned operational procedures will address this concern.

23. Cigarettes were being smoked in the facility and we observed cigarette smoke and numerous butts in the piles of combustible materials.

True. Planned operational procedures will address this concern.

24. A large hole made in the data center wall did not lead to battery room as stated by data center personnel. Instead, we found that it led to an area shared with the building's other occupant.

True. This "large hole" does not exist today and was there to connect a conduit pipe between the UPS and backup batteries, residing in an isolated area.

25. Background investigations required for personnel working on secure facilities had not been conducted for personnel doing construction, pulling communications wires, and setting up operations in the data center. These personnel worked for contractors and the building's other occupant.

See comment 8.

True. All contractors who have worked in any way on the CyberFile initiative are subject to a minimum background investigation in accordance with the IRS SOW dated 10/10/95. This SOW does not require MBIs prior to the commencement of the CyberFile System.

26. Background investigations required for personnel working on sensitive systems had not been conducted for National Technical Information Service's (NTIS) personnel working on CyberFile applications in the production environment.

See comment 8.

True. All employees who work on the CyberFile initiative are subject to a minimum background investigation in accordance with the IRS SOW dated 10/10/95. This SOW does not require background investigations prior to the commencement of the CyberFile System.

5

27. Personnel in the data center were not wearing any badges or other forms of identification to validate their authority to be in the data center.

True. Planned operational procedures will address this concern.

28. Vendors were allowed unescorted access throughout the data center.

True. Planned operational procedures will address this concern.

29. Contractors were developing and testing their software in the production environment, rather than using a separate development and test facility. This exposes the production environment to increased risk of sabotage and mishap due to errors.

See comment 9.

False This pilot facility was utilized to support final system test separately from our Development, and Integration facilities in Springfield, VA.

30. The data center did not have a secure perimeter. Access to shared areas that completely encircle the data center was not controlled by NTIS, increasing the risk of sabotage to the facility.

See comment 10.

The IRS CyberFile center is completely separate from the USDA computer room

False. The IRS data center is located within a controlled access USDA data center.

31. Individuals entering the data center were asked to sign a log but were not required to show valid identification.

True. Planned operational procedures will address this concern

32. Telecommunications equipment, such as telecommunications switches and patch panels, was not physically protected and could be accessed and damaged by unauthorized personnel.

True. As of 4/3/96 four people have key access to these patch panels.

33. Communications devices intended to be used only to monitor data flow, could also be used to alter data and for browsing.

See comment 11.

False. There is no device in the facility that would allow this to happen.

34. Communications lines were mounted unprotected on the back wall of the data center instead of being enclosed in a secure telephone closet or box. This

increased the risk of both malicious and unintentional communications disruptions.

True. The communication lines terminate within the computer room.

35. No wiring plan for the communication lines was available to correlate the circuits with the wire locations. This makes it difficult to isolate particular circuits for maintenance and to restore communications after disruption.

True. All wiring plans have been submitted to CM and are in use at USDA.

36. Dial-in communications from other NTIS facilities exposed the production environment to attack by individuals outside the facility.

See comment 12.

False. No dial-in communication is permitted from other NTIS facilities.

37. Communications cables running along the ceiling outside the data center were exposed, providing a readily accessible target to be cut or wiretapped.

See comment 13.

These external communications cables belong to USDA and are not being used by the data center.

38. A separate communications line observed running through the data center posed an undetermined risk since data center personnel could not identify its origin, destination, or purpose.

True. This cable has been rerouted and is no longer operational.

39. Patch panels, which can be used to redirect communications traffic, were installed at the data center, but no policies or procedures were established to control their use. This increases the risk of communications disruptions caused by undisciplined patch panel operations.

True. Planned operational procedures will address this concern.

40. A data communications block that was wired to route CyberFile's Internet electronic filing traffic was also wired to route traffic for another application. Without additional information on how this block will be configured, there is a risk of communications disruptions from the other application.

See comment 14.

True. The IRS' optical fiber line is planned to be isolated by mid-summer. The vendor, MFS, is methodically adding new cable runs into the building.

41. Another data communications block that was wired to route CyberFile's 800 number traffic was also wired to route traffic for another application. Again,

7

without additional information on how this block will be configured, there is a risk of communications disruptions from the other application.

See comment 14.

False. No 800#s route to another application.

42. CyberFile does not have a backup computer facility. If a disaster occurs at the data center, taxpayers will not be able to file electronically from personal computers.

See comment 15.

CyberFile does not have a backup facility. However, given that CyberFile is a pilot system, the IRS will rely on alternative EFS programs as a CyberFile contingency.

43. CyberFile does not have adequate alternative power sources to maintain computer operations during a power outage.

True. Having no back-up power generator is an acceptable risk for this pilot system.

44. The data center does not have any building evacuation alarms to alert personnel and permit orderly shut down of operations and safe evacuation of personnel.

There is a building alarm that indicates danger in other parts of the building An alarm speaker was installed at the end of March.

45. The draft contingency plan does not have specific procedures to be followed in an emergency. For example, the action plan for recovering from fire damage calls for the initiation of proceedings for repair or replacement of damaged facilities and equipment, but does not specify how to accomplish this task.

True. Planned operational procedures will address this concern.

46. The plan does not identify the key individuals responsible for executing specified procedures.

True. Planned operational procedures will address this concern

47. The risk analysis conducted for CyberFile was incomplete and did not adequately address physical, operational, and communications security threats to the data center. For example, despite the fact that the greatest risk to a data center is often attack by its own employees, the analysis does not address the threat of data center employees compromising taxpayer data.

See comment 16.

The IRS conducted a CyberFile risk assessment.

8

48. There was no security awareness program for CyberFile.

True. Planned operational procedures will address this concern

49. Data center security practice was lax. For example, we found a note, written on a white board in the data center, instructing employees to hand-off passwords to employees on the next shift. Because employees share passwords, system and data accesses and the use of system resources cannot be traced to individuals, and therefore, cannot be effectively controlled.

True. Planned operational procedures will address this concern

The following are GAO's comments on the Internal Revenue Service's letter dated April 29, 1996.

GAO Comments

1. Data center management told us that the center would be operationally ready on March 19, 1996. This statement was consistent with previous and subsequent statements made to us by IRS and NTIS management.

2. The weakness we identified was that wet standpipe sprinklers were installed in lower than normal ceilings, not that wet standpipe sprinklers were used.

3. We modified the finding to cite the recordable drives which were functioning in the center during our review and deleted the reference to the CD-ROM.

4. The weakness we identified was inadequate safeguarding of an emergency cut-off switch, not its location. Officials at the April 30, 1996, meeting said that modifications had been made to the switch to address our concern.

5. Our concern is with the need for a tape library in the center. It did not address the need for off-site data storage.

6. During our review, batteries were not yet installed. Batteries typically used to maintain computer center operations require ventilation and wash facilities. We will reassess this issue after the batteries are installed.

7. During our review, there was no evidence of secured hinges on any data center doors. Center management at that time acknowledged our concern.

8. Background investigations are required for all contractors working in IRS computer centers that handle or will handle taxpayer data. This includes the contractors building the Cyberfile facility.

9. Contractor personnel interviewed during our walk through of the Cyberfile data center said they were developing and testing software.

10. The IRS Cyberfile center can be accessed through areas shared with USDA. As a result, IRS security depends upon USDA and its personnel, as well as IRS and its personnel. This poses additional risk to IRS that must be controlled.

11. During our review, computer center personnel told us that such a device was on order for use in the center.

12. Computer center personnel told us that the center had dial-in communications. The issue here, however, is that any communications into the data center pose a risk and must be adequately controlled.

13. Without a wiring plan, as noted in weakness number 35, we cannot substantiate whether these communications cables are part of the Cyberfile computer center.

14. The response does not address the weakness. To meet IRS' security requirements, these data communications blocks cannot be shared.

15. The response asserts that other electronic filing systems will handle Cyberfile submissions if Cyberfile fails but does not explain how or when this will occur since the other systems cannot handle Cyberfile submissions now.

16. It is true that IRS conducted a Cyberfile risk assessment. Our point was that it was incomplete and inadequate.

(511516)

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested