OIG

OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

Improvements Are Needed for Information Technology Controls at the Las Vegas Finance Center

Report No. 2003-P-00011

May 29, 2003

Report Contributors:

Edward Densmore
Wen Song
Corey Costango
Cheryl Reid

Abbreviations

ARTS	Asbestos Receivable Tracking System
EPA	U.S. Environmental Protection Agency
LAN	Local Area Network
LVFC	Las Vegas Finance Center
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

May 29, 2003

MEMORANDUM

SUBJECT: Audit Report:
Improvements Are Needed for Information Technology Controls
at the Las Vegas Finance Center
Report No. 2003-P-00011

FROM: Patricia H. Hill, Director
Business Systems (2421T)

TO: Alan Lewis, Branch Chief
Las Vegas Finance Center

This is the final report on the Information Technology Controls at the Las Vegas Finance Center, as conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This audit report contains findings that describe problems the OIG has identified and corrective actions the OIG recommends. This audit report represents the opinion of the OIG and the findings contained in this report do not necessarily represent the final EPA position. Final determinations on matters in this report will be made by EPA managers in accordance with established EPA audit resolution procedures.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to the findings and recommendations presented in this report within 90 days of the date of this report. You should include a corrective actions plan for agreed upon actions, including milestone dates. We have no objections to the further release of this report to the public. For your convenience, this report will be available at http://www.epa.gov/oigearth/eroom.htm.

If you or your staff have any questions regarding this report, please contact me at (202) 566-0894 or Wen Song, Project Manager, at (202) 566-2558.

Purpose

The objective of this audit was to determine whether general information technology controls at the Las Vegas Finance Center (LVFC) are adequate to safeguard the integrity of Agency resources and ensure continuity of critical EPA operations.

Background

The LVFC, in Las Vegas, Nevada, is a field branch of the Financial Services Division of EPA's Office of the Chief Financial Officer. LVFC provides a full range of accounting and financial services to EPA co-located activities, such as the Team Vegas Human Resources Office, National Exposure Research Las Vegas Laboratory, and the Radiation and Indoor Environments National Laboratory; remote activities, such as labs in Oklahoma, Oregon, and Colorado; and Criminal Investigations Division offices in Boston, San Francisco, Philadelphia, Chicago, and New York. These services include processing procurement orders, Government bills of lading, and travel-related documents. The LVFC is also responsible for grant payments and financial closeout for all assistance agreements in both EPA Headquarters and Region 7.

The LVFC Local Area Network (LAN) provides network support for the staff at LVFC and the Office of Solid Waste and Emergency Response, and hosts the Las Vegas National Value-Added Backbone Service accessible to all other EPA field office organizations in the Las Vegas area (i.e., Human Resources, Office of Radiation and Indoor Air, and the Office of Research and Development). The LVFC LAN consists of 3 Novell servers running Novell NetWare 5.0, 32 client workstations operating on a mix of DOS and Windows 95/98/2000/XP operating systems, 7 networked workgroup printers, and a tape drive for performing backups.

The LVFC is also responsible for Asbestos Grant and Loan Program post-award loan activity. Related to this program, the Asbestos Receivable Tracking System (ARTS) microcomputer database application was developed to record and track repayments as well as manage EPA's asbestos loans and provide for reporting direct loans under the Credit Reform Act of 1990. The software contains subsidiary ledger detail data that feeds into EPA's Integrated Financial Management System accounts receivable general ledger balances. ARTS tracks the disbursement of loans and collection of payments, and also issues bills and reminder notices to loan recipients. In addition, ARTS provides detailed data for internal and external reports regarding asbestos loans for the Office of Management and Budget, Treasury, and Congress.

Scope and Methodology

The primary focus of this audit was security controls over the LVFC LAN and ARTS. Specifically, we reviewed security program planning and management, access controls, segregation of duties, and service continuity practices. We conducted our audit field work from December 2002 to February 2003, at LVFC and at EPA Headquarters in Washington, DC.

To accomplish the audit objective, we used a variety of Federal and Agency regulatory documents, including:

- Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.
- National Institute of Standards and Technology (NIST) Special Publication 800-12, *An Introduction to Computer Security*.
- EPA Directive 2195A1, *Information Security Manual.*
- EPA Directive 2195.1 A4, *Agency Network Security Policy*.

We conducted the audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. We reviewed the LVFC LAN and ARTS security plans, and the Continuity of Operations Plan. We interviewed personnel at LVFC and at EPA headquarters. In addition, we performed tests on the logical security controls and observed physical security controls at the LVFC.

Prior Audit Coverage

A prior EPA OIG report entitled *Fiscal 1994 Financial Statement Audit of EPA's Trust Funds, Revolving Funds and Commercial Activity*, No. E1SFL4-20-8001-5100192, dated February 28, 1995, identified several control weaknesses related to ARTS at LVFC. Specifically, the report noted ARTS lacked: (1) adequate security over computer programs and loan data, (2) a virus protection program, (3) standardized backup and recovery procedures, (4) an Integrated Financial Management System interface, and (5) a problem/change control log. Recommendations included: developing written policies and procedures describing ARTS backup, recovery, and contingency plans; maintaining ARTS data and program backups in a secure off-site location; and implementing an electronic interface between ARTS and the Integrated Financial Management System. In responding to the draft report, the Chief Financial Officer agreed to take corrective action on all of the recommendations.

Results of Review

Improvements are needed to general information technology controls at LVFC to effectively ensure continuation of services. Backup media (i.e., on- and off-site storage) were not properly secured, system documentation was not being stored off-site, and network connection boxes were unlocked. As a result, should a disruption of service occur, LVFC's ability to start up operations in a timely manner could be impeded. The weaknesses relating to off-site backup media and system documentation occurred because management had not developed a comprehensive continuity of support plan for the LVFC LAN. In addition, management did not perform a complete risk assessment for the LVFC LAN that may have identified the weaknesses relating to on-site backup media and the network connection boxes. A continuity of support plan establishes the necessary procedures for managing and continuing operations following disasters or interruptions of service, while a risk assessment assists management in identifying threats and vulnerabilities. To improve continuity of operations capabilities, management also needs to follow

generally accepted practices for securing backup media and storing systems documentation. Details on conditions noted follow.

Unsecured Backup Media

LAN. LVFC did not properly secure the on- and off-site storage of its LAN backup tapes. Incremental backups of the LAN are performed daily and a full backup every Friday. Although the on-site LAN backup tapes were stored in the LVFC computer room, the current weekly backup tapes were located in an unlocked tape drive and thus were not adequately secured. In addition, another set of backup tapes was stored on open racks within the computer room. Although LVFC officials did not think further controls were needed because the computer room utilizes a card reader system for access, anyone entering the computer room could compromise the on-site backup tapes. For example, a number of contractors outside of the finance group have access to the computer room. These contractors need access to shared telecommunications equipment installed in the room, but they do not need access to the backup tapes. Regarding off-site storage, the LAN backup tapes are removed to an off-site storage location every other Friday. However, the off-site storage location for these tapes was an EPA employee's personal residence. Management cannot ensure the physical security of backup tapes at a personal residence, and may not be able to retrieve such backup tapes during an emergency situation if the employee is on travel or otherwise not available.

ARTS. Backup tapes for ARTS also were not properly secured on- and off-site. ARTS is backed up weekly, and the backup tapes are stored on-site in an unlocked cabinet located in shared LVFC office space accessible to all personnel in that space. Only authorized personnel (e.g., the system administrator and employee responsible for performing backups) should have access to the backup media. In addition, although the tapes are also sent monthly to the Financial Systems Branch at EPA Headquarters, the Branch leaves the tapes unsecured on top of a file cabinet inside shared office space. Furthermore, since ARTS files are backed up to the LVFC LAN, they are exposed to the weaknesses previously discussed for the LAN backup tapes.

ARTS System Documentation Not Stored Off-Site

Management did not store ARTS system documentation off-site. A copy of the documentation stored on-site includes procedures to back up, restore, and recover the application. If LVFC operations are disrupted and on-site system documentation cannot be obtained, the ARTS application manager stated she would be able to restore ARTS without the documentation. Nonetheless, she agreed maintaining another copy of system documentation off-site would be helpful, since she did not think anyone else would be able to restore ARTS application without the system documentation. Industry best practices dictate that off-site storage of documentation should be established to support recovery and business continuity plans.

Unlocked Network Connection Boxes

The network connection boxes between the LVFC LAN and the building housing the Office of Solid Waste and Emergency Response's connectivity to the LVFC LAN were not locked. That office uses the LVFC server to connect to the EPA network. The unlocked network connection boxes were located on the exterior of the two buildings and were opened by releasing two latches, exposing the fiber optic cables. According to NIST Special Publication 800-12, physical access controls should address not only the area containing system hardware but locations of wiring used to connect elements of the system and data lines. Within a few hours of the unlocked network connection boxes being brought to the attention of the LVFC management, padlocks were placed on the boxes.

As a result of the conditions noted, LVFC's ability to start up operations in a timely manner may be impeded, should a disruption of service occur. Consequently, LVFC may not be able to effectively continue its operations or have the most current data available, if a disaster occurs. Specifically, management may not be able to timely obtain the backup tapes and system documentation needed to restart necessary financial management services for its customers.

The weaknesses relating to off-site backup media and system documentation occurred because management had not developed a comprehensive continuity of support plan for the LVFC LAN. In addition, management did not perform a complete risk assessment for the LVFC LAN that may have identified the weaknesses relating to on-site backup media and the network connection boxes. Management needs to expand the LVFC continuity of operations plan to ensure LAN operations can continue smoothly. The current plan assigns responsibilities for plan activation and identifies some essential functions, positions, and equipment needed for relocating to an alternate site. However, it does not provide detailed procedures for continuing LAN operations, such as business priorities and timing for restoration and recovery. EPA Directive 2195A1 includes steps to develop continuity of support plans. These steps include (1) defining and describing what needs to be done for shutting down the hardware during and immediately after an emergency; (2) identifying business priorities, the order of importance, and timing for restoration and recovery of system processing capabilities; and (3) determining how hardware supplies and other needed items will be obtained.

Office of Management and Budget Circular A-130, Appendix III, requires Federal agencies to consider risk when deciding what security controls to implement. It states a risk-based approach is required to determine adequate security, and encourages agencies to consider major risk factors, such as threats, vulnerabilities, and the effectiveness of current or proposed safeguards. Also, EPA Directive 2195.1 A4 states risk assessments must be conducted and updated for general support systems (which include LANs) and/or major applications at least every 3 years, or when a substantive configuration change occurs.

LVFC management currently relies on "BindView," a system management product, to perform risk assessments for its LAN. BindView can be used to monitor and report on password activity, intruder

detection, and the presence of unauthorized files in the login directory. Although BindView is a very useful management tool, it does not address the whole LAN environment and does not satisfy risk assessment requirements. LVFC managers also utilized the agency's self-assessment tool to gather data on the LAN in support of NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. Self assessments provide a method for managers to determine the current status of their information security programs. This NIST Special Publication states a risk assessment should be conducted in conjunction with or prior to the self-assessment. It further states a self-assessment does not eliminate the need for a risk assessment. According to NIST Special Publication 800-12, a risk assessment includes collecting and analyzing data (e.g., asset valuation, consequence analysis, threat identification, safeguard analysis, and vulnerability analysis). If management had performed a risk assessment that included threat identification, it may have identified the weaknesses relating to unsecured backup media and the unlocked network connection boxes.

To improve continuity of operations capabilities, management also needs to follow generally accepted practices for securing backup media and storing systems documentation. As noted, LVFC did not have adequate LAN and ARTS backup procedures. Generally accepted practices dictate that management design media controls to prevent the loss of confidentiality, integrity, or availability of information when stored outside the system. EPA's LAN Operating Procedures also endorse such practices.

Recommendations

We recommend that the Branch Chief, LVFC:

1. Conduct a complete risk assessment for the LVFC LAN.

2. Develop, implement, and test a comprehensive continuity of support plan for the LVFC LAN.

3. Update and implement the LAN and ARTS backup procedures to include an adequate off-site storage location and adequate physical controls for both on- and off-site backup media and system documentation and update LAN and ARTS security plans accordingly.

Agency Response and OIG Evaluation

In responding to the draft report, the LVFC Branch Chief concurred with our recommendations (see Appendix A). In the response, some language changes were suggested and, in most cases, we modified the report language accordingly.

The response indicated LVFC officials are working with their Information Security Officer to identify an individual and/or organization who will conduct a complete risk assessment during fiscal 2004. They have also agreed to develop, implement, and test a comprehensive continuity of support plan for the LVFC LAN. Furthermore, LVFC management has installed a locked, fireproof cabinet in the LVFC

computer room for on-site storage of the LAN and ARTS backups. A second locked, fireproof cabinet has been installed in a secured room off-site, in order to provide storage for the LAN and ARTS backups, as well as for copies of the ARTS system documentation. The door to the backup tape drive is also now under lock and key.

In our view, the corrective actions described in response to Recommendations 1 and 2 are appropriate and should, when fully implemented, adequately address the recommendations. However, LVFC management did not fully address Recommendation 3 by indicating concurrence or non-concurrence with updating the LAN and ARTS security plans. If the LAN and ARTS security plans are subsequently updated to reflect the corrective action described in LVFC's response for Recommendation 3, this recommendation will also be adequately addressed.

Agency's Response to Draft Report

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

MAY 15 2003

OFFICE OF THE
CHIEF FINANCIAL OFFICER

MEMORANDUM

SUBJECT: Draft Audit Report, "Improvements Are Needed for Information Technology Controls at the Las Vegas Finance Center," Project No. 2003-00048, dated April 14, 2003

FROM: Alan Lewis, Branch Chief
Las Vegas Finance Center

THRU: Ron Bachand, Director
Financial Services Division

TO: Edward Densmore, Assignment Manager
Business System Audits, OIG

We have reviewed the draft report provided by your office and are providing the following comments regarding both the factual accuracy of the report and our concurrence or nonconcurrence with your findings and recommendations.

Background

Not included in the background section is the Las Vegas Finance Center's (LVFC) responsibility for grant payments and financial closeout for all assistance agreements in both EPA HQ and Region 7. Since the financial management of grants is the primary mission of the LVFC, we feel it is important to have it mentioned here.

Also, there are seven networked workgroup printers on the LVFC LAN, not three as stated in the draft report. There are three in the LVFC office and four in the OSWER office.

Prior Audit Coverage

The draft makes mention of recommendations made in a 1995 OIG report and states that OCFO agreed to take corrective action, but does not clarify whether or not these actions were actually completed. We would like an additional sentence added at the end of the existing paragraph as follows, "LVFC officials stated that all corrective actions were implemented by 1996, but no follow up IG review has been conducted to verify this."

Results of Review

There is no direct evidence that, as the draft states, "The weaknesses noted occurred because management had not performed a complete risk assessment and developed a comprehensive continuity of support plan for the LVFC LAN." There is no proven, direct relationship between the two events. A more accurate statement would be "The weaknesses noted may have occurred because management had not performed...." There is a similar statement at the beginning of the third paragraph on page 5 of the draft which should also be changed to "These weaknesses may have occurred because..."

Unsecured Backup Media - LAN - While we concur with the overall finding, the statement "For example, a number of contractors outside of the finance group have access to the computer room" is somewhat exaggerated. In fact, only a very limited number of non-federal personnel outside the finance staff have been given necessary access to the computer room.

Recommendations

1. Conduct a complete risk assessment for the LVFC LAN.

   Concur - We are working with the Information Security Officer (ISO) to identify the individual and/or organization who will conduct the review during FY04.

2. Develop, implement, and test a comprehensive continuity of support plan for the LVFC LAN.

Concur - Schedule:	Develop plan	by Aug 15
	Implement plan	by Nov 1
	Test plan	by Dec 30

3. Update and implement the LAN and ARTS backup procedures to include an adequate off-site storage location and adequate physical controls for both on- and off-site backup media and system documentation and update LAN and ARTS security plans accordingly.

Concur - We have installed a locked, fireproof cabinet in the LVFC computer room for on-site storage of the LAN and ARTS backups. A second locked, fireproof cabinet has been installed in the OSWER secured room in a separate building to provide off-site storage for the LAN and ARTS backups, as well as for copies of the ARTS system documentation. The door to the backup tape drive is also now under lock and key. Internal controls are in place for all of the keys to ensure only authorized personnel gain access.

Thank you for the opportunity to review and comment on the draft. We appreciate the OIG's efforts in reviewing the IT controls for LVFC's systems. If you have any questions, please contact me at (702) 798-2480 or Dany Lavergne at (702) 798-2483.

Appendix B

Report Distribution

Comptroller (2731 A)
Deputy Chief Financial Officer (2710A)
Director, Financial Services Division, Office of Chief Financial Officer (2734R)
Director, Financial Management Division, Office of Chief Financial Officer (2733R)
Audit Liaison, Office of Chief Financial Officer (2710A)
Inspector General (2410)