Office of Inspector General

Report of Audit

SECURITY OF SCIENCE AND ECOSYSTEMS SUPPORT DIVISION (SESD) LOCAL AREA NETWORK (LAN)

SEPTEMBER 30, 1997

Audit Report E1NMF7-15-0001-7100309

Inspector General Division Conducting the Audit:	ADP Audits and Assistance Staff
Region Covered:	Region 4
Program Offices Involved:	Athens Laboratory

Security of SESD Local Area Network (LAN)[1]
Report No. E1NMF7-15-0001-7100309

Our audit determined that the Science and Ecosystems Support Division (SESD) in Athens, Georgia, did not have a security plan or backup/disaster recovery plan. Audit results also disclosed that SESD management plans to place non-LAN administrative personnel in the room where the LAN's file servers and telecommunication wiring reside. In addition, there were no formal procedures for overall LAN maintenance or standard operating procedures for daily routines, such as granting and terminating access, making backup tapes, etc. Management was unaware of the Agency guidelines and requirements concerning plans and procedures, prior to the recent receipt of Agency-issued guidance. Lack of plans and procedures could lead to unauthorized disclosure or manipulation of sensitive Agency data. Finally, we noted that there were a number of Novell server settings and configuration irregularities which need to be corrected.

PURPOSE

The objectives of this audit were to: 1) test the physical, security, and detective controls over the SESD LAN, especially those controls involving physical and logical access; 2) verify the adequacy of controls relative to the backup and recovery of the SESD file servers; and 3) verify that adequate policy, procedures and administrative controls exist relative to SESD LAN management.

BACKGROUND

SESD LAN

SESD is located in the Regional laboratory in Athens, Georgia. The SESD LAN consists of 2 file servers. These file servers connect with the backbone for the 10 local area networks serving the following Divisions and Offices: Environmental Accountability Division, Waste Management Division, Water Management Division, Science & Ecosystem Support Division, Air Pesticides, Toxics Management Division, and the Offices of Policy & Management, Congressional Affairs, and Public Affairs.

[1] A data communication network operating over a limited geographical area, typically within a building or group of buildings.

LAN Management

The majority of EPA's employees are connected to local and Agency applications and data through LANs and the value-added backbone services. The Enterprise Technical Services Division's (ETSD) LANSYS group is responsible for maintenance of the backbone servers, the backbone software, and the backbone wiring throughout EPA. However, each individual LAN is managed locally by the program office it serves.

ETSD requires adherence to EPA's security standards in order for a LAN to be connected to an Agency facility backbone and to obtain ETSD support. However, these are minimum security standards and it is ultimately left up to local management and LAN System Administrators to design and implement security for their LAN. The degree of security needed at a LAN site will vary with the type of data processed and the physical security afforded by the facility. Each LAN must comply with the security standards listed in Section 6 of NDPD Operational Directive No. 310.09. These standards state the minimum levels of security which must be implemented and maintained. Compliance with these security policies is a prerequisite for connection to the Agency backbone and for support by ETSD. Failure to comply with these policies will result in disconnection of a LAN from the Agency internetwork and removal of ETSD support.

Currently, there are approximately 300 LANs within EPA, supporting an estimated 14,000 workstations. Within a few years, it is projected that all Agency employees will be connected by a LAN. Furthermore, it is an ETSD goal to move toward 'workgroup computing' (i.e., everyone uses the same hardware and software in the same way) and eventually to 'Enterprise LANs' where data can be distributed, collected, processed and accessed throughout the Agency.

As the number of new LAN installations increases, so does the number of programs and quantity of data stored on these LANs. Microcomputers or Personal Computers (PCs) pose numerous security issues by themselves, but the task of securing these resources is even more difficult when work group PCs are connected to form LANs in order to share resources. Any one work group LAN may be adequately self-contained and have a LAN System Administrator. Once these separate LANs are connected via a facility-wide backbone, physical access among work groups is granted. Therefore, with the increased number of access points, security becomes a larger issue for all users and LAN System Administrators.

SCOPE AND METHODOLOGY

The primary focus of this audit was to evaluate the security of the Region 4's LANs. Field work was conducted from January 1997 through March 1997, at SESD in Athens, Georgia. We conducted this

audit in accordance with Government Auditing Standards (1994 revision) issued by the Comptroller General of the United States. We reviewed the procedures for granting access to the SESD LAN, and requested and reviewed applicable system documentation. In addition, we performed a security "walkthrough" and discussed security considerations and requirements with responsible SESD LAN representatives. Finally, we evaluated the compliance of LAN settings and configuration with established Agency information security policies and standards, federal regulations and industry standards using the Enterprise Security Manager (ESM) software. For further details on the ESM software, see Appendix II.

PRIOR AUDIT COVERAGE

There has not been any prior audit coverage relating to security controls affecting SESD LANs.

CRITERIA

Federal and Agency guidelines, as well as industry publications, were used to form a framework of prudent, stable business practices and therefore served as a means to evaluate LAN security. Provided below is a summary of the criteria used during this review. References to other published guidelines are specified throughout the report.

Computer Security Act of 1987 (P.L.100-235)

The Computer Security Act of 1987 creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use. The Computer Security Act requires the establishment of security plans by all operators of Federal computer systems that contain sensitive information. The Act also requires mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

The Act assigns to the National Institute of Standards and Technology (formerly the National Bureau of Standards) responsibility for developing standards and guidelines for Federal computer systems. This responsibility includes developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate. Also, this Act provides for the promulgation of such standards and guidelines.

Office of Management and Budget (OMB) Circular A-130

OMB A-130 mandates that reviews should assure that management, operational, personnel, and technical controls are functioning effectively. Security controls may be reviewed by an independent audit or a self review. The type and rigor of review/audit should be commensurate with the acceptable level of risk which is established in the rules for the system, as well as the likelihood of learning useful information to improve security. Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest patches), and penetration testing can assist in the on-going review of different facets of systems. However, these tools are no substitute for a formal management review at least every three years. Indeed, for some high-risk systems with rapidly changing technology, three years will be too long.

Depending upon the risk and magnitude of harm which could result, weaknesses identified during the review of security controls should be reported as deficiencies in accordance with OMB Circular No. A-123, "Management Accountability and Control" and the “Federal Managers' Financial Integrity Act” (FMFIA). In particular, if a basic management control such as assignment of responsibility, a workable security plan, or management authorization are missing, then consideration should be given to identifying a deficiency.

Local Area Network Operational Procedures and Standards (LOPS)

The Local Area Network Operational Procedures and Standards (LOPS) describes the minimum, or baseline, standards required for all EPA LANs. These procedures provide a reference for LAN implementation and operation within the Agency’s standardized framework.

EPA Information Security Manual (ISM)

This manual provides the necessary direction to implement Federal regulations concerning information security, and outlines the specific procedures and requirements necessary to ensure adequate protection of all EPA information systems. The manual addresses both manual and automated information systems. The security concepts, roles and responsibilities, apply to both manual and automated systems. The manual serves as a baseline for EPA organizations and personnel to measure and determine whether 1) the information they are using is being protected adequately, and 2) their organization is in compliance with all requirements of the Agency’s Information Security Policy.

The ISM applies to all EPA organizations and their employees. It also applies to the facilities and personnel of EPA’s agents (including contractors) who are involved in designing, developing, operating, maintaining, or accessing Agency information and information systems.

SESD NEEDS A LAN DISASTER RECOVERY PLAN

SESD does not have a disaster recovery plan for their LAN. In the event of a disaster, critical information would be lost and management would have a difficult time restoring the LAN to pre-disaster condition. SESD management was unaware of Agency requirements for a formal disaster recovery plan. A disaster scenario is any likely event that has a chance of occurring and if it occurs has the potential for significantly interrupting normal business processing. These events include fires, severe thunderstorms, floods, tornados, and hurricanes.

Operations continuity deals with the notion that a business should be able to survive and continue operations even if a disastrous event occurs. Rigorous planning and commitment of resources are necessary to adequately plan for such an event. Contingency planning is the primary responsibility of senior management as they are entrusted with the safeguarding of both the program information and viability of the program office to perform its duties.

All of the SESD file servers are located in one room within the Athens laboratory. A disaster need only to occur to that particular room to be considered a disaster for the Athens facility. In the event that the file server room should experience a disaster, such as fire or another form of natural disaster, the Athens facility would be unable to institute a timely disaster recovery process. Responsible personnel would have to create information on how to get systems restored *after* the disaster, thereby increasing restoration time.

During a disaster an adequate disaster recovery plan is of upmost importance. It lends organized plans to what can sometimes be a chaotic situation. An adequate disaster recovery plan should include but is not limited to the following:

- **Notification**
  Procedures for notifying relevant managers in the event of a disaster. Typically, this includes a contact list of home and emergency telephone numbers.

- **Disaster Declaration**
  Procedures pertaining to the assessment of damage following a disaster, criteria for determining whether the situation constitutes disaster, and procedures for declaring a disaster and invoking the plan.

- **Systems Recovery**
  Procedures to be followed to restore critical and vital systems at emergency service levels within a specified time frame, in accordance with the systems recovery strategy defined in the plan.

- **User Recovery**
  Procedures for recovering critical and vital user functions within a specified time frame in accordance with the planned strategy. This includes documenting instructions for processing data manually, even though the data may previously have been processed via an automated system. Even if the manual procedure was the standard at one time, continued knowledge of such procedures should not be assumed. This is especially true as tenured employees who may have once performed manual procedures may transfer or retire, and manual documentation and forms can be destroyed or misplaced.

SECURELY STORE BACKUP FILES OFF-SITE

Taped file backups are not securely stored off-site. Although facility personnel back up data files manually on a periodic basis, the backups are kept in the LAN administrator's home, an EPA contractor. The NDPD Operational Directives Manual No. 310.05, entitled LAN Data Management, requires that LAN administrators perform backups and store the backups securely off-site. The off-site location needs to be as safely secured and controlled as the originating site. This includes adequate physical access controls such as locked doors, no windows, and human surveillance. This requirement is especially critical for sensitive Agency data. The SESD LAN administrator stated he was unaware of Agency backup data storage requirements.

In addition, the SESD facility does not have formal policies and procedures to perform backup and off-site storage of Agency data. Currently, an experienced LAN administrator performs regularly scheduled backups. However, formal policies and procedures should be established to ensure that any appointed personnel could perform the necessary procedures to back up data.

SESD NEEDS A FORMAL LAN SECURITY POLICY AND MAINTENANCE AND OPERATING PROCEDURES

SESD Needs A LAN Security Plan

SESD does not have a LAN security plan as required by OMB A-130. In addition, SESD did not report incomplete security documentation as a control weakness in their fiscal 1996 Federal

Manager's Financial Integrity Act (FMFIA) Assurance Letter. SESD was unaware of the OMB Circular A-130 requirement. Management security policies document the standards of compliance. Security policies should state the position of the organization with regard to all security risks, and should also identify who is responsible for safeguarding organization assets, including programs and data. Without an adequate LAN security plan employees are unable to provide adequate protection against violators.

OMB Circular A-130 requires that management approve security plans at least every three years through the OMB Circular A-123 process. In addition, it specifies that security control weaknesses be reported as part of the Agency's OMB Circular A-123 annual review process. The Information Resources Management Security Program is relying on the managers of the individual sites and program offices to implement these IRM security requirements or to report information security weaknesses as part of the OMB Circular A-123 process.

OMB Circular A-130 is entitled "Management of Federal Information Resources." Appendix III of this Circular is entitled "Security of Federal Automated Information Systems." This appendix details the required policy and guidance agencies must provide to ensure that automated systems have adequate security programs and documentation. It establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular A-123. The Appendix revises procedures formerly contained in Appendix III to OMB Circular A-130 (50 FR 52730; December 24, 1985), and incorporates requirements of the Computer Security Act of 1987 (P.L.100-235) and responsibilities assigned in applicable national security directives.

OMB Circular A-130 also requires the development of a security plan and provides guidance regarding the content of an adequate security plan. Key components of such a security plan include the following:

- Management support and commitment;
- Access philosophy;
- Access authorization;
- Reviews of access authorization;
- Security awareness;
- A defined role for the security administrator;
- Security committee; and
- Hardware and software inventory control.

No Desk Procedures for LAN Administrator

There are no "desk" procedures for backup or new LAN administrative personnel to follow in the event that the primary LAN administrator is unable to perform his/her duties. SESD attributed the non-existence of procedures to conflicting priorities. These standard operating procedures should include granting and terminating access to the SESD file servers, making backup tapes, contingency plans, troubleshooting the LANs, and general computer security administration matters. If the primary LAN administrator is not available, other LAN administrative staff may have to assume their duties. Without written procedures to guide the replacements, the SESD LAN could be left vulnerable, especially in the event of a disaster.

No Maintenance Plan For SESD LAN

There is no maintenance plan for SESD LANs. Consequently, there is no regularly scheduled LAN maintenance. For example, according to the LAN administrator, account maintenance is performed as other duties permit. Regular maintenance is essential to maintain the integrity and continuity of the SESD LAN. SESD attributed the non-existence of policies and procedures to conflicting priorities and scarce resources. Currently, SESD retains a contractor who functions as the SESD LAN administrator to manage two file servers. A lack of policies and procedures could lead to inconsistent application of settings and loss of accountability**.**

PROPOSED SEATING ARRANGEMENTS PLACE EMPLOYEES IN THE LAN ROOM

SESD laboratory management plans to place program employees in the same room where the LAN file servers are located. If these employees are situated in this room, the file servers will be exposed to non-LAN administrative personnel. This arrangement would create physical and environmental exposures which could result in loss of credibility and accountability. Discussions with management identified spacing constraints as the cause for this potential weakness.

Access and environmental controls provide for confidentiality, integrity, protection, and managed availability of computer facilities and systems. These controls reduce the risk of adverse business conditions due to computer malfunction, data or software failure, or abuse of responsibilities, while still providing computerized information and resources for the people who need them. These controls must address both human and natural threats to the computer system. Exposures to the SESD LAN that exist from accidental or intentional violation of these physical and environmental controls include the following:

- Damage to equipment and property;
- Vandalism to equipment and property;
- Theft of equipment and property;
- Copying or viewing of sensitive information;
- Alteration of sensitive equipment and information; and
- Public disclosure of sensitive information.

Anyone in the room housing the LAN would have access to the servers. The servers could be accidentally or intentionally unplugged or damaged. Also, since the on\off switch is accessible, the servers could simply be turned off. Another concern stems from the fact that the file servers boot up from the "A drive." Therefore, a person can switch off the file server and then bring it back up after placing a diskette into the A drive. A diskette containing batch[2] files with unauthorized instructions for the file server could be run once the system reboots. Also, a knowledgeable person could introduce a virus through the A drive.

The file servers must be secured so that they are not exposed to employees who do not require access. If they are not properly secured, the file servers will be vulnerable to accidental or intentional damage and\or loss of data.

LAN SETTINGS ARE NOT IN ACCORDANCE WITH AGENCY STANDARDS AND INDUSTRY GUIDANCE

Some of the SESD LAN account settings are not in compliance with the Agency's LOPS manual and best industry practices. We determined, through the use of Enterprise Security Manager (ESM) software and discussions with responsible officials, that the SESD LAN does not follow all of the guidelines set forth in the Agency's LOPS manual. This could leave the SESD LAN vulnerable to security breaches from hacker attacks within and outside the Agency. Discussions with SESD representatives determined that they were unaware of required Agency LAN settings.

ESM is a client/server product which reports on the status of the existing client operating system, in terms of security compliance to a set of standards. ESM designed the client to be installed on all supported multi-user operating systems to improve network security. Host (Agency) security standards are used as the benchmark for evaluating security. The ESM software consists of a manager and an agent component designed to collect and report security relevant data (e.g., password length required by the system, potential security vulnerabilities, etc.) for an entire enterprise from a central location. We provided further details on the ESM product in Appendix II.

[2] The processing of a group of related transactions at planned intervals.

Due to the nature of the vulnerabilities noted, we decided to present them in a table format. The following table summarizes the vulnerabilities and potential effects on the SESD LAN, as determined by ESM:

Table has been redacted due to sensitive nature

RECOMMENDATIONS

We recommend that the Director of SESD:

1. Develop a disaster recovery plan for the SESD LAN.

2. Ensure that Agency data backups are securely stored off-site.

3. Establish formal policies and procedures to ensure that any appointed personnel could perform the necessary procedures to back up data.

4. Develop a security plan which addresses the full complement of OMB Circular A-130 requirements. In addition, the Director should report the absence of a security plan as a "material weakness" in subsequent FMFIA Assurance Letters, until the plan is completed.

5. Establish a formal maintenance plan for the SESD LAN. This plan should include, but is not limited to, software installation, hardware upgrades, and capacity management. Regular maintenance is essential to maintain the integrity and continuity of the SESD LAN.

6. Establish and maintain desk procedures for backup or new LAN administrative personnel to follow in the event that the primary LAN administrators are unable to perform his/her duties.

7. Ensure that LAN file servers are not exposed to employees who do not specifically require physical access to them.

8. Based on the conditions identified, adjust the Novell NetWare settings on the SESD LAN to comply with Agency and industry guidance.

AGENCY COMMENTS AND OIG EVALUATION

In a memorandum dated August 19, 1997, the Director of Region 4's Science and Ecosystems Support Division (SESD) responded to our draft report (See Appendix I). In summary, SESD management agreed with all eight of our recommendations.

SESD management agreed to develop a disaster recovery plan based upon the one being created for the Region IV LANs in Atlanta, Georgia. Management officials also agreed to store data backups off-site at the SESD Field Equipment Center by September 1, 1997. SESD management will also establish policies, by October 1, 1997, to ensure that any appointed personnel could perform the necessary procedures to back up data.

In addition, SESD staff will work with Region IV's Information Management Branch and their Information Security Officer to develop a security plan. SESD management also agreed to produce a maintenance plan based upon the one developed by Region IV. Furthermore, SESD staff will formulate an initial draft of standard operating procedures for SESD LAN administrators by November 1, 1997. SESD management also agreed to limit access to the room which houses the LAN file servers and telecommunication wiring. They will contact the General Services Administration regarding the installation of a wall and locked door to separate the computer equipment from the staff work area. Finally, using the Enterprise Security Manager software to provide needed details, SESD will adjust their LAN settings to comply with Agency LAN security policies.

We concur with SESD’s response to our recommendations and will evaluate their corrective actions during our follow-up review.

.

THIS PAGE INTENTIONALLY LEFT BLANK

ENTERPRISE SECURITY MANAGER (ESM)

Enterprise Security Manager (ESM) is a client/server product which reports on the status of the existing client operating system in terms of security compliance to a set of standards. Axent Technologies designed the client to be installed on all supported multi-user operating systems to improve network security. Host (Agency) security standards are used as the benchmark for evaluating security.

The ESM software consists of a manager and an agent component designed to collect and report security relevant data (e.g., password length required by the system, potential security vulnerabilities, etc.) for an entire enterprise from a central location. The manager provides control over global functions (e.g., report scheduling, report generation, etc.) that are independent of ADP architecture and operating system (e.g., SUN/Solaris). The agent portion is specific to the particular operating system architecture and provides the basic function of data collection for reporting to the manager. The data collected and reported is stored on the manager system, alleviating storage constraints on the agent system. Agents exist as "processes" on VMS systems, as "daemons " (owned by root) executing on UNIX systems, and as "NLMs " on Novell servers. An NLM enhances or provides additional server functions in a server running Netware Version 3. A graphical user interface is provided by ESM through which manager/agent functions can be controlled.

A manager can be installed on any system type currently supported by ESM (e.g., UNIX, NETWARE, VMS, etc.) and can service multiple agent systems (e.g., a NETWARE server with a manager can service agents on UNIX, Netware, and VMS systems). Alternately, separate managers can be used for each architecture (e.g., NETWARE servicing NETWARE, UNIX servicing UNIX, etc.), although this approach is more expensive than one manager servicing multiple architectures.

The ESM architecture provides for security of manager/agent communication through a password. The password is supplied when the agent is installed and when the manager is invoked for communication with the agent. Since the agents are owned by the operating system (e.g., executes as a daemon owned by root on UNIX systems), privileged access to the system on which the agent is installed is not required by the user invoking the manager component. Privileged system operation by the user invoking the ESM manager is disallowed and prevented. This properly segregates the role of system administrator from that of the person conducting a review of system security through use of the ESM software.

Further segregation of administrator/security reviewer roles can be achieved when using ESM. For example, agents can be registered to (controlled by) more than one manager component. Each manager component can be invoked by different personnel to achieve personnel backups, or to provide use of the product by both a security reviewer and a system administrator. In addition, a manager can be designated as a super manager. Therefore, installing a manager component in each EPA region would allow each region its own detailed use of ESM. The designation of an ETSD super manager would allow ETSD's Security Staff to receive only summary data from each regional manager for the purposes of statistical or other reporting. The specific installed configuration is determined by the site installing the product, and will be driven by availability of resources and expertise, funding, political concerns, etc.

APPENDIX III

GLOSSARY

DOS	-	Disk Operation System
ESM	-	Enterprise System Manager
ETSD	-	Enterprise Technology Services Division (formerly NDPD)
FMFIA	-	Federal Managers' Financial Integrity Act
LAN	-	Local Area Network
LOPS	-	LAN Operational Procedures and Standards
NDPD	-	National Data Processing Division (See ETSD)
NLMs	-	Network Loading Modules
OMB	-	Office of Management and Budget
SESD	-	Science and Ecosystems Support Division

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX IV

REPORT DISTRIBUTION

Office of Inspector General

Acting Inspector General (2410)

Assistant Inspector General for Audit (2421)

Principal Deputy Assistant Inspector General for Audit (2421)

Deputy Assistant Inspector General for Internal Audits (2421)

EPA Headquarters

Agency Audit Followup Official (3101)
Attn: Assistant Administrator for Administration and Resources Management

Agency Audit Followup Coordinator (2710)
Attn: Audit Management Team

EPA HQs Library

Athens, Georgia

Director, Science and Ecosystems Support Division

Region IV

Chief, Information Management Branch
Attn: Office of Policy and Management

Chief, Grants, IAG and Audit Management Section