Office of Inspector General

Report of Audit

SECURITY OF REGION IV LOCAL AREA NETWORKS (LANs)

SEPTEMBER 29, 1997

Audit Report E1NMF7-15-0001-7100308

Inspector General Division Conducting the Audit:	ADP Audits and Assistance Staff
Region Covered:	Region IV
Program Offices Involved:	Information Management Branch

EXECUTIVE SUMMARY

PURPOSE

The objectives of this audit were to: 1) test the physical, security, and detective controls over the Region IV Local Area Networks (LANs)[1], especially those controls involving physical and logical access; 2) verify the adequacy of controls relative to the backup and recovery of the regional file servers; and 3) verify that adequate policy, procedures and administrative controls exist relative to regional LAN management.

BACKGROUND

The majority of EPA's employees are connected to local and Agency applications and data through LANs and the VABS. 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(s) it serves. The Information Management Branch (IMB) controls all of Region IV's LAN administration.

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 (SAs) 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.

As the number of new LAN installations increases, so does the number of programs and quantity of data stored on these LANs. The task of securing 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.

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

AUDIT RESULTS IN BRIEF

Our audit of IMB LAN security determined that termination procedures to the LANs are not formalized. We also determined that IMB did not have a security plan or backup/disaster recovery plan. In addition, we determined that there were no formal policies covering LAN maintenance procedures. Management was unaware of the Federal 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. We also noted that there were a number of Novell server settings and configuration irregularities which need to be corrected. Region IV recognized the importance of the security deficiencies outlined in our findings, and their response to the draft report recommendations demonstrates their willingness to enhance regional security controls.

PRINCIPAL FINDINGS

Region IV Needs A Disaster Recovery Plan

IMB has not developed a disaster recovery plan for the Region IV LANs. These LANs contain sensitive agency information dealing with a variety of program office data. In the event of a disaster, critical information would be lost and IMB would have a difficult time restoring the LANs to pre-disaster condition. 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, tornados, hurricanes and floods. IMB management was unaware of Agency requirements for a formal disaster recovery plan.

Formal LAN Access Termination Control Procedures Are Needed

IMB does not have a structured, consistent process for rescinding access to Region IV LANs. There are no formal procedures to be followed in the event that an employee is terminated or transferred. Currently, the LAN administrator is not directly notified when an employee is terminated or transferred. Since the LAN group moved to a new building in August of 1996, management had not made developing formal termination and transfer policy and procedures a high priority. Unauthorized access could lead to the manipulation and destruction of data.

Region IV Needs A LAN Security Plan

Region IV does not have a LAN security plan as required by OMB Circular A-130. In addition, IMB did not identify the lack of a LAN security plan as a “material weakness” in their fiscal 1996 Federal Manager’s Financial Integrity Act (FMFIA) Assurance Letter. IMB was unaware of the OMB Circular A-130 requirement. 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. Without an adequate LAN security plan employees would be unable to provide adequate protection against violators.

Formalize LAN Policy And Maintenance Procedures

Region IV lacks policies and procedures for overall LAN maintenance as well as standard operating procedures for daily routines, such as granting and terminating access, making backup tapes, etc. IMB attributed the non-existence of policies and procedures to conflicting priorities and scarce resources. Currently, IMB has only two LAN Administrators to manage 28 servers. However, a lack of policies and procedures could lead to inconsistent application of settings and loss of accountability.

LAN Settings Are Not In Accordance With Agency Standards And Industry Guidance

Some of Region IV's LAN account settings are not in compliance with the Agency's LAN Operational Procedures and Standards (LOPS) manual and industry standards. We determined, through the use of Axent Technologies' OmniGuard/Enterprise Security Manager (ESM) software and discussions with responsible program officials, that IMB does not follow all of the guidelines set forth in the Agency's LOPS. Non-compliance with standard security requirements could leave the LAN vulnerable to hacker attacks from within and outside the Agency. Discussions with IMB management determined that they were unaware of required Agency LAN settings.

RECOMMENDATIONS

We recommend that the Chief for Region IV's Information Management Branch develop a security plan and a disaster recovery plan. In addition, we recommend that IMB develop formal policies covering overall LAN maintenance as well as routine operating procedures for LAN administrators. We also recommend that IMB formalize LAN termination procedures. Finally we recommend that IMB bring Novell server settings in accordance with Agency and industry guidance.

AGENCY COMMENTS AND OIG EVALUATION

In a memorandum dated September 10, 1997, Region IV's Chief for Information Management responded to our draft report (See Appendix I). In summary, Agency officials agreed with all of our recommendations. Region IV agreed to develop both disaster recovery and security plans, establish formal LAN policy, maintenance and termination procedures, and to use ESM to bring regional LAN settings in accordance with Agency guidelines.

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

CHAPTERS

1 INTRODUCTION 1

PURPOSE 1

BACKGROUND 1

SCOPE AND METHODOLOGY 3

CRITERIA 3

2 REGION IV NEEDS A LAN DISASTER RECOVERY PLAN 5

3 FORMAL LAN ACCESS TERMINATION CONTROL PROCEDURES ARE NEEDED 7

4 REGION IV NEEDS A LAN SECURITY PLAN 9

5 FORMALIZE LAN POLICY AND MAINTENANCE PROCEDURES 11

6 LAN SETTINGS ARE NOT IN ACCORDANCE WITH AGENCY STANDARDS AND INDUSTRY GUIDANCE 13

APPENDICES

I AGENCY RESPONSE TO DRAFT REPORT 25

II ENTERPRISE SECURITY MANAGER (ESM) 27

III GLOSSARY 29

IV REPORT DISTRIBUTION 31

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1

INTRODUCTION

PURPOSE

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

BACKGROUND

Region IV LANs

The Information Management Branch (IMB) controls all of Region IV's LAN administration. Region IV has occupied the newly constructed Atlanta Federal Center (AFC) since August 1996. The EPA Region IV LAN consists of 33 file servers operating on eight floors of the AFC in Atlanta, Georgia and at the Regional laboratory in Athens, Georgia. These file servers comprise 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.

Each server can provide some or all of the following applications within the Region:

- Communication services - e.g.,electronic mail, Internet access, EPA Mainframe access, remote access to employees working outside the office, dial up access to remote computers;

- Agency Standard Software - e.g., WordPerfect word processor, Lotus Spreadsheets, dBASE III & IV database applications, Windows 3.1, Freelance and Harvard Graphics;

- Electronic Forms - e.g., time sheets, supplies ordering, travel authorization and laptop checkout;

- Miscellaneous Applications- e.g., Oracle Database, Superfund document management and Lotus Notes;

- Information Resources - CDROM Services.

IMB purchased state-of-the-art equipment for the Region's move to the new AFC. The ten file servers forming the major backbone for the LAN were bought at the time the Region moved to this building.

LAN Management

The majority of EPA's employees are connected to local and Agency applications and data through LANs and the VABS. 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 (SAs) 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. 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 IV's LANs. Field work was conducted from January 1997 through March 1997, at Region IV in Atlanta, 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 Region IV LANs and requested and reviewed applicable system documentation. In addition, we performed a security "walkthrough" and discussed security considerations and requirements with responsible IMB 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.)

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 audit. References to other published guidelines are specified throughout this 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.

OMB Circular A-127

OMB A-127 incorporates the requirement of the Computer Security Act of 1987, stating that agencies plan to secure their systems commensurate with the risk and magnitude of loss or harm which could result from the loss, misuse, or unauthorized access to information contained in those systems. It includes assuring the integrity, availability, and appropriate confidentiality of information. It also involves protection against the harm that could occur to individuals or entities outside of the Federal Government, as well as the harm to the Federal Government. Appendix III to this circular prescribes a minimum set of controls to be included in Federal automated information resources security programs and assigns Federal agency responsibilities for the security of automated information resources. This circular also includes limits on collection and sharing of information and procedures to assure the integrity of information, as well as requirements to adequately secure the information.

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. This manual addresses both manual and automated information systems. The security concepts, roles and responsibilities, apply to both manual and automated systems. This manual serves as a baseline for EPA organizations and personnel to measure and determine whether the information they are using is being protected adequately, and that EPA organizations are 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 agents (including contractors) of the EPA who are involved in designing, developing, operating, maintaining, or accessing Agency information and information systems.

CHAPTER 2

REGION IV NEEDS A LAN DISASTER RECOVERY PLAN

Disaster Recovery Plans

IMB has not developed a disaster recovery plan for their Region IV LANs. There are variety of program offices which use the Region IV LANs. In the event of a disaster, critical information would be lost and IMB would have a difficult time restoring the LANs to pre-disaster condition. IMB 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 Region IV's file servers are situated in one room within the IMB, which is located in the Martin Luther King Building in Atlanta, Georgia. A disaster need only to occur to that particular room to be considered a disaster for Region IV. In the event that Region IV should experience a disaster, such as fire or another form of natural disaster, IMB would be unable to institute a timely disaster recovery process. IMB 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 IMB personnel backup data files manually on a periodic basis, the backups are kept in the homes of the backup administrators.
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. IMB's backup administrators were unaware of the Agency backup data storage requirements.

In addition, Region IV does not have formal policies and procedures to perform backup and off-site storage of Agency data. Currently, experienced LAN administrators perform regularly scheduled backups. However, formal policies and procedures should be established to ensure that any appointed personnel could perform the necessary procedures to backup data.

RECOMMENDATIONS

We recommend that the Chief, Region IV IMB:

2-1. Develop a disaster recovery plan for the Region IV LANs.

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

2-3. Establish formal policies and procedures to ensure that any appointed personnel could perform the necessary procedures to backup data.

AGENCY COMMENTS AND OIG EVALUATION

In a memorandum dated September 10, 1997, Region IV's Chief for Information Management responded to our draft report (See Appendix 1). In summary, Region IV officials agreed with all three recommendations and stated they would:

1. Develop a disaster recovery plan by March 1, 1998.

2. Store backup media with an off-site storage company no later than November 28, 1997.

3. Establish formal policies and procedures to ensure that any appointed personnel could perform the necessary procedures to backup data. These polices and procedures should be complete by December 26, 1997.

We concur with Region IV's response to our recommendations and will evaluate these corrective actions during our follow-up review.

CHAPTER 3

FORMAL LAN ACCESS TERMINATION CONTROL PROCEDURES ARE NEEDED

IMB does not have a structured and consistent process for rescinding access to Region IV LANs. There are no formal procedures to be followed in the event that an employee is terminated. Currently, the LAN administrator is not notified when an employee is terminated or transferred. Management was unaware of the need to formalize the process for terminating LAN user accounts. If the employee has a mainframe account, personnel notifies the computer specialist responsible for mainframe access, as well as the computer specialist responsible for access to the E-mail system. One or both of these computer specialists informs the LAN administrator to remove the employee’s account from the particular LAN.

This method of notifying the LAN administrator regarding unnecessary accounts is haphazard and should be formalized. The accounts of terminated employees may remain active and may pose a potential security weakness. In addition, these accounts should be removed in a timely manner.

Human Resources provides an “Employee Separation or Transfer Checklist” (EPA Form 3110-1) for employees to follow when separating from the Agency or transferring internally. In addition to documenting the return of Agency property, this list includes removing mainframe accounts. However, the checklist does not cover LAN accounts. This checklist was never updated to include removing LAN accounts.

RECOMMENDATION

We recommend that the Chief, Region IV's IMB formalize LAN termination and transfer procedures by:

3-1. Requesting that the Office of Human Resource Management modify the “Employee Separation or Transfer Checklist” to include removal of LAN accounts.

AGENCY COMMENTS AND OIG EVALUATION

Region IV did not address this issue in the response to the draft report. However, on September 16, 1997, Region IV's Chief for Information Management informed us that regional staff are working with Region IV Human Resources to correct the termination form by December 31, 1997.

We concur with Region IV's corrective action and will evaluate its effectiveness during our follow-up review.

CHAPTER 4

REGION IV NEEDS A LAN SECURITY PLAN

Region IV does not have a LAN security plan as required by OMB A-130. In addition, IMB did not report incomplete security documentation as a control weakness in their fiscal 1996 Federal Manager's Financial Integrity Act (FMFIA) Assurance Letter. IMB 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

RECOMMENDATION

We recommend that the Chief, Region IV's IMB:

4-1. Develop a security plan in accordance with OMB Circular A-130. In addition, management should report this deficiency as a "material weakness" in subsequent FMFIA Assurance Letters until the plan is completed.

AGENCY COMMENTS AND OIG EVALUATION

In a memorandum dated September 10, 1997, Region IV's Chief for Information Management responded to our draft report (See Appendix 1). In summary, Region IV officials concurred with our recommendation and agreed to develop a security plan in accordance with OMB Circular a-130 by November 28, 1997.

We concur with Region IV's response to our recommendations and will evaluate the security plan during our follow-up review.

CHAPTER 5

FORMALIZE LAN POLICY AND MAINTENANCE PROCEDURES

Region IV lacks policies and procedures for overall LAN maintenance. IMB attributed the non-existence of policies and procedures to conflicting priorities and scarce resources. Currently, IMB has only two LAN Administrators to manage 28 servers. A lack of policies and procedures could lead to inconsistent application of settings and loss of accountability.

No Desk Procedures for LAN Administrators

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

No Maintenance Plan for Region IV LANs

There is no maintenance plan for the Region IV LANs. Consequently, there is no regularly scheduled LAN maintenance. IMB attributed the non-existence of policies and procedures to conflicting priorities and scarce resources. For example, according to the LAN administrators, account maintenance is performed as other duties permit. Regular maintenance is essential to maintain the integrity and continuity of the Region IV LANs.

RECOMMENDATIONS

We recommend that the Chief, Region IV's IMB:

5-1. Establish a maintenance plan for the Region IV LANs. 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 Region IV LANs.

5-2. Establish and maintain standard operating procedures for backup or new LAN administrative personnel to follow in the event that the primary LAN administrators are unable to perform their duties.

AGENCY COMMENTS AND OIG EVALUATION

In a memorandum dated September 10, 1997, Region IV's Chief for Information Management responded to our draft report (See Appendix 1). In summary, Region IV officials agreed with our two recommendations. Specifically, management agreed to complete a new policy and maintenance procedures plan by December 26, 1997.

We concur with Region IV's response to our recommendations and will evaluate these corrective actions during our follow-up review.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 6

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

Some of the Region IV 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 program officials, that IMB does not follow all of the guidelines set forth in the Agency's LOPS manual. This could leave the Region IV LANs vulnerable to security breaches from hacker attacks within and outside the Agency. Discussions with IMB management 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 provide further details regarding the ESM product in Appendix II.

Due to the nature of the vulnerabilities noted, we decided to present them in a table format. On the following pages, we used two tables to summarize the vulnerabilities and potential effects on the Region IV LANs, as determined by ESM:

Tables have been redacted due to sensitive nature

RECOMMENDATION

We recommend that the Chief, Region IV's IMB:

6-1. Based on the conditions identified, bring the Novell NetWare settings on the Region IV LANs in accordance with Agency and industry guidance.

AGENCY COMMENTS AND OIG EVALUATION

In a memorandum dated September 10, 1997, Region IV's Chief for Information Management responded to our draft report (See Appendix 1). In summary, Region IV officials agreed with our recommendation. Region IV management stated that they will begin correcting these settings immediately, and will continue to run the ESM program on a quarterly schedule to prevent this from ever being a problem again. They also plan to include this procedure in their standard operations procedures and policy guidelines

We concur with Region IV's response to our recommendations and will evaluate the corrective actions during our follow-up review.

APPENDIX I

THIS SECTION RESERVED FOR AGENCY RESPONSES
TO FORMAL DRAFT REPORT

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX II

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 "NLM's " on Novell servers. An NLM enhances or provides additional server functions in a server running Netware Version 3. A graphical user interface (GUI) 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 IV

GLOSSARY

AFC	-	Atlanta Federal Center
DOS	-	Disk Operation System
ESM	-	Enterprise System Manager
ETSD	-	Enterprise Technology Services Division (formerly NDPD)
FMFIA	-	Federal Managers’ Financial Integrity Act
GUI	-	Graphical User Interface
IMB	-	Information Management Branch (Region IV)
LAN	-	Local Area Network
LOPS	-	LAN Operational Procedures and Standards
NDPD	-	National Data Processing Division (See ETSD)
NLMs	-	Network Loading Modules
OIRM	-	Office of Information Resource Management
OMB	-	Office of Management and Budget
RTP	-	Research Triangle Park
SA	-	Systems Administrator
VABS	-	Value Added Backbone Services

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

Region IV

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

Chief, Grants, IAG and Audit Management Section

Athens, Georgia

Director, Science and Ecosystems Support Division