Office of Inspector General

Audit Report

INFORMATION RESOURCES MANAGEMENT

SECURITY OF REGION VIII's DIAL-UP ACCESS

Report No. 2000-P-16

March 31, 2000

Inspector General Division(s) Conducting the Audit	**ADP Audits and Assistance Staff**
Region(s) covered	**Region VIII**
Program Office(s) Involved	**Data Systems Management Branch**

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

March 31, 2000

OFFICE OF
THE INSPECTOR GENERAL

MEMORANDUM

SUBJECT: **Final Report:** Security of Region VIII's Dial-up Access
Audit No. 1999-0000165
Report No. 2000-P-16

FROM: Patricia H. Hill, Director
ADP Audits and Assistance Staff (2421)

TO: Patricia D. Hull, Assistant Regional Administrator
Office of Technical and Management Services (8TMS-D)

Rick Martin, Director
National Technology and Services Division, MD-34

Attached is our final report entitled "Security of Region VIII's Dial-up Access." The primary objectives of the audit were to determine if: 1) dial-up controls currently implemented by the region adequately secure dial-up access; 2) the region is logging and auditing all dial-up attempts to their systems; and 3) any terminated employees have dial-up access to the network.

This audit report contains findings that describe problems the Office of Inspector General has identified and corrective actions the OIG recommends. This audit report represents the opinion of the OIG, and the findings contained in this audit report do not necessarily represent the final EPA position. Final determinations on the matters in the audit report will be made by EPA managers in accordance with established EPA audit resolution procedures.

Action Required

Region VIII

In response to the draft report, your office provided responsive action plans and milestone dates for correcting the findings. As a result, and in accordance with our longstanding agreement outlined in EPA Order 2750, we find your response to the report acceptable. If the previously disclosed milestones dates for corrective actions have changed, then we ask that you E-mail a description of ongoing actions and provide an updated timetable for completing corrective

actions. In addition, please track all action plans and milestone dates in EPA's Management Audit Tracking System.

NTSD

In accordance with EPA order 2750, you, as an action official, are required to provide us with a written response to the audit report within 90 days of the final report date. If corrective actions will not be complete by the response date, we ask that you describe the actions that are ongoing and reference specific milestone dates which will assist us in deciding whether to close this report. In addition, please track all action plans and milestone dates in EPA's Management Audit Tracking System.

We appreciate the cooperation afforded us during the course of this audit by NTSD and Region VIII's TMS staff. We also appreciate the Region's many comments to the recommendations presented in the report, as well as the many actions you and your staff have already initiated to address issues concerning regional dial-up security. We have no objections to the further release of this report to the public. Should you or your staff have any questions regarding this report, please contact Ed Shields, Audit Team Leader, AAAS, at (202) 260-3656.

Attachment

cc: P. Riederer, Director, Data Systems Management Branch (8TMS-D)
G. Bonina, Director, IT Policy and Planning Division (2831)
D. McGinnis, Chief, IT Policy and Planning Division (2831)
J. Worthington, Audit Liaison, OEI (2811R)

EXECUTIVE SUMMARY

PURPOSE

The objectives of this audit were to determine if : (1) the dial-up controls currently implemented by the region adequately secure dial-up access; (2) the region is logging and auditing all dial-up attempts to their systems; and (3) terminated employees have dial-up access to the network.

BACKGROUND

The Environmental Protection Agency National Technology Services Division (NTSD) provides the centrally managed Automated Data Processing (ADP) and telecommunications infrastructures required to support the Agency's mission. Without proper controls over dial-up access, confidential and sensitive data may be disclosed during transmission over telecommunication lines.

Security of information systems may be defined as the control structure established to manage the integrity, confidentiality, and availability of information systems (IS) data and resources. A combination of controls must be implemented to minimize the risk of a successful attack by (1) making unauthorized access difficult to attain and (2) carefully monitoring the dial-up access attempts and responding swiftly to potential security incidents as they occur. The advent of telecommuting increases the risk associated with dial-up access, because more and more users employ this mode of entry to access EPA's system.

The Public Switched Network is used to gain access to the internal network. Any individual possessing the proper equipment can attempt to gain access. Dial-up users, who are not situated in close physical proximity to a network connection, frequently use the public switched telephone networks to dial into the internal network. The security risks vary depending on the type of dial-up connection established with the public networks. Connections through public switched data network are established in a manner similar to that of connections in public telephone network.

RESULTS IN BRIEF

While Region VIII and NTSD management are trying to tighten security controls, the current dial-up access controls do not adequately secure access to the network. In particular, we found that Region VIII was not using advanced authentication techniques to protect the dial-up access to the Network. We also determined that logical and physical access controls contributed to poor security over dial-up access. Furthermore, Region VIII was not logging and auditing all dial-up attempts to their system. In addition, we discovered that some of the Region's terminated employees still possessed access to the regional servers. More importantly, our audit disclosed that NTSD is not planning to force dial-up access through the Agency's Internet Firewall, scheduled for implementation in April 2000. Nor does NTSD plan to provide programs or services to help the regional offices interpret logged data captured at EPA's National Computer Center. These weaknesses enable potential intruders to exploit external dial-up access points and increase the vulnerability of Regional data, as well as the Agency's network and national systems. We conclude that Agency and regional managers need to make security a top priority by allocating appropriate resources to implement and maintain adequate security processes, increasing management oversight of such processes, and developing adequate formal policies and procedures to guide regional security personnel in the administration of security matters.

PRINCIPAL FINDINGS

We evaluated the adequacy of the Region's dial-up controls in accordance with Federal and Agency guidelines, as well as commonly accepted industry practices. The following three weaknesses relate to audit objective #1, and affect the region's ability to adequately secure dial-up access to its information systems and network data.

Advanced Authentication Techniques and Encryption Not Used

Region VIII is not using any advanced authentication techniques, such as one-time password technology and dial-back mode, to protect their dial-up access to the network. Therefore, once dial-up access is permitted, the network is potentially opened to the public by providing inadequately secured external access points. Additional controls should be implemented to properly secure and

control these external dial-up access points. At the moment, Region VIII is only using encrypted static passwords for authentication of dial-up access attempts to EPA's Network. Although encrypted, static passwords do not prevent a perpetrator from capturing and replaying authenticated password data to impersonate an authorized user and gain access to the network.

Logical Network Account Settings Do Not Comply with Directives, Policies, and Best Practices

Some of Region VIII's Local Area Network (LAN) account settings are not in compliance with Agency Directives, Region VIII policies, and best industry practices. Complying with minimum LAN settings is important, because they implement the logical security enforced by the network operating system. By not consistently following these guidelines, the region is leaving its LANs, as well as EPA's network, vulnerable to security breaches from hacker attacks within and outside the Agency.

Inadequate Physical Controls Further Diminish Security

Although Region VIII uses access Card Keys to restrict physical access to the computer room, management is not adequately addressing other controls necessary to ensure the safety of computer resources and network data. For example, regional management does not adequately control the issuance, termination, and oversight of the access cards to the computer room. Neither has management implemented policies and procedures for adequately supervising and documenting visitors in the computer room. These inadequacies provide perpetrators with a means of circumventing the logical security in place.

No Logging or Monitoring of Dial-Up Access and Control of Modem Usage

Region VIII does not log, audit, or perform follow-up reviews on dial-up access attempts to their computer systems. Neither do NTSD staff monitor the logs generated in connection with dial-up access to Region VIII, as provided through the main access number for the Agency's remote access project. Maintaining dial-up logs and monitoring these journals is necessary to safeguard these computer access points against security violations. As a result, the region does not have specific incident response policies and procedures for handling detected dial-up access attempts. Instead, management has to rely on other organizations to notify them of attacks to the regional system. We also determined that regional staff are not

tracking and controlling the use of modems, nor are there any policies and procedures to govern modem usage. Consequently, unauthorized dial-up access and access points could allow the exploitation of EPA data. Region VIII management stated they were not using audit logs, because they were waiting for EPA's NTSD to identify a standard configuration for setting up the logging capability.

Inadequate Termination Control Procedures

Our audit results concluded that Region VIII has terminated/separated employees with user accounts which allow them to still access the network directly via dial-up. In addition, terminated/separated employees still possess card key account access to the computer room. Not removing the access of terminated/separated personnel allows potentially disgruntled personnel the ability to access the computer room and network. Furthermore, these accounts are prime targets for hackers to get a foothold into the network, because no users exist to complain should changes occur to their account.

NTSD Plans Impact the Adequacy of Security

EPA's current plans do not sufficiently ensure that dial-up access and the associated dial-up entry points to the Agency's network will be adequately secured. In particular, NTSD management has no plans to force dial-up access through the Internet Firewall, once implemented. NTSD plans to allow dial-up connections directly to the network through communications servers, once they are all established. These servers will not direct the dial-up traffic through the Firewall(s). Such a configuration will defeat the purpose of the firewall by providing backdoors into EPA's network.

Management Needs To Make Security A Top Priority

Although regional operations management state they consider security to be important, they have not committed sufficient resources to adequately secure and maintain dial-up access control points. Specifically, management needs to apply an appropriate portion of available resources to fully staff and improve security processes. In addition, increased management oversight is necessary to ensure that security over regional systems is implemented and maintained. Furthermore, management needs to develop acceptable formal policies and procedures which can communicate regional control requirements and specify

how controls should be implemented. Lastly, NTSD management needs to: (1) plan to route dial-up access through EPA's Internet Firewall, once implemented; and (2) provide additional guidance, training and tools to regional staff to ensure proper administration of regional security programs.

RECOMMENDATIONS

Due to the nature of the audit findings, both Region VIII and the Agency's NTSD will need to implement corrective actions to effectively address these weaknesses. We recommend that the Assistant Regional Administrator for Technical and Management Services (TMS) implement advanced authentication techniques and provide periodic dial-up training for all remote users. We also recommend that TMS bring their LAN account settings into compliance with Agency Directives, Region VIII Policies, and best industry practices, and establish additional controls to secure sensitive activities. Furthermore, TMS should establish policies and procedures to ensure that the logical and physical access rights to the computer facilities are limited to those employees who require access to perform their jobs, and TMS should log and monitor dial-up access. Finally, we believe TMS should establish policies and procedures that (1) require all users be formally approved prior to being provided with remote access, (2) require the system to enforce the access list of remote access users, and (3) ensure the access of terminated/separated users is removed in a timely manner.

In connection with our report findings, we also issued recommendations to the Director of NTSD. Specifically, we recommend that NTSD establish formal policies and procedures that require all dial-up connections to pass through the firewall. In addition, we recommend that NTSD provide system administrators and information security officers (ISO) with formal guidance and training related to monitoring dial-up access.

AGENCY COMMENTS AND OIG EVALUATION

In summary, Agency officials responded favorably to the report recommendations (see Appendices I & II). In a memorandum dated March 24, 2000, Region VIII's Assistant Regional Administrator for TMS agreed to

implement all report recommendations under their span of control. Likewise, in a memorandum dated March 27, 2000, the Director for NTSD agreed with the audit findings, although he stated that NTSD must review various ways of implementing corrective actions before committing to a specific plan of action.

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

ABBREVIATIONS

ADP	Automated Data Processing
ESTC	Employee Separation or Transfer Checklist
IS	Information Systems
ISO	Information Security Officer
LAN	Local Area Network
NDS	NetWare Directory Services
NTSD	National Technology Services Division
OMB	Office of Management and Budget
SA	System Administrator
TAPP	Time and Attendance, Payroll and Personnel
TMS	Technical and Management Services

THIS PAGE INTENTIONALLY LEFT BLANK

GLOSSARY OF TECHNICAL TERMS

Authentication	The verification of the source, uniqueness and integrity of a message, action, or individual for establishing user accountability
Ciphertext	Data or plaintext which has been encrypted or enciphered, thus producing unintelligible text or signals.
Decipher	To convert encrypted text, by use of the appropriate key and transformation technique, into its equivalent plaintext (clear text).
Dial-Back	The user notifies the system to establish network connection (typically by voice call) and enters a password or access code. The network places an outbound call back to the user at a pre-established, authorized phone number. This mechanism can be subverted by call-forwarding.
Encryption	The basic manner of protecting data communications from unauthorized interception. Communications can be encrypted using end-to-end encryption. If communications are end-to-end encrypted, the messages are encrypted at transmission and decrypted at the receiving station. The data do not appear in clear form at any intermediate node. With link-encrypted communications, the messages are encrypted before entering a telecommunications link and decrypted after exiting the link.
Firewall	A control point where the access portion of a security policy can be enforced; generally enabled by a Network Communication Device of some sort, ranging in size from an A - B switch to a complex integrated system.
Key Card	Physical device used to control and monitor access to sensitive areas.
Modem	Electronic device that enables digital data to be sent through analog transmission facilities. Modems enable the user to link to network resources through a dial-in connection.
Security Incidents	Events which result from a computer virus, other malicious code, or a system intruder.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1

INTRODUCTION

PURPOSE

The objectives of this audit were to determine if: (1) the dial-up controls currently implemented by the region adequately secure dial-up access; (2) the region is logging and auditing all dial-up attempts to their systems; and (3) terminated employees have dial-up access to the network.

BACKGROUND

The Environmental Protection Agency National Technology Services Division (NTSD) provides the centrally managed Automated Data Processing (ADP) and telecommunications infrastructures required to support the Agency's mission. Without proper controls over dial-up access, confidential and sensitive data may be disclosed during transmission over telecommunication lines.

Security of information systems may be defined as the control structure established to manage the integrity, confidentiality, and availability of information systems (IS) data and resources. A combination of controls must be implemented to minimize the risk of a successful attack by (1) making unauthorized access difficult to attain and (2) carefully monitoring the dial-up access attempts and responding swiftly to potential security incidents as they occur. The advent of telecommuting increases the risk associated with dial-up access, because more and more users employ this mode of entry to access EPA's system.

The Public Switched Network is used to gain access to the internal network. Any individual possessing the proper equipment can attempt to gain access. Dial-up users, who are not situated in close physical proximity to a network connection, frequently use the public switched telephone networks to dial into the internal network. The security risks vary depending on the type of dial-up connection established with the public networks. Connections through public switched data network are established in a manner similar to that of connections in public telephone network.

SCOPE AND METHODOLOGY

The primary focus of the audit was to evaluate the security of dial-up access in Region VIII. Audit fieldwork was conducted from May 1999 through August 1999, at Region VIII in Denver, Colorado. We also spoke with NTSD representatives and reviewed documentation published on the Agency Intranet site related to EPA's Remote Access Implementation Project. We conducted this audit in accordance with Government Auditing Standards. We reviewed and requested applicable system documentation governing dial-up access. In addition, we evaluated the compliance of LAN settings and configuration with established Agency Information Security policies and standards, Federal regulations, and industry standards, using the Novell LAN Manager Software. In addition, we performed a security "walkthrough" and discussed security considerations and requirements with responsible Region VIII representatives.

While evaluating Region VIII's dial-up controls, we identified security issues which impact the Region's ability to adequately protect their dial-up access, although they were out of their direct control. These particular security issues fall under the control of EPA's National Technology Services Division (NTSD), and impede the Region from (1) implementing adequate dial-up controls and (2) effectively and efficiently monitoring dial-up access. Because of the significance of these issues, we are including them as a part of our audit report.

PRIOR AUDIT COVERAGE

No prior OIG audit coverage relates to dial-up access controls at the Region VIII facilities in Denver, Colorado.

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 dial-up security.

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

OMB A-130 requires each agency to ensure that a capability exists to help users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. 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 the systems.

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.

National Institute of Standards and Technology: An Introduction to Security Handbook, Special Publication 800-14

This handbook provides the necessary direction for computer security incidents which might result from a computer virus, other malicious code, or a system intruder or outsider. Containing an incident should include an assessment of whether the incident is part of a targeted attack on the organization or an isolated incident. This publication emphasizes that a good incident handling capability is closely linked to an organization's training and awareness program.

Identification and authentication is a technical measure that prevents unauthorized people (or an unauthorized process) from entering an IT system and, therefore, a critical building block of computer security. This measure is the basis for most types of access control and for establishing user accountability, although not all types of access controls require identification and authentication.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2

ADVANCED AUTHENTICATION, LOGICAL AND PHYSICAL CONTROLS

The authentication, logical, and physical controls implemented by Region VIII do not adequately secure dial-up access. In particular, Region VIII does not use advanced authentication techniques to help secure its dial-up access. Also, some of Region VIII's LAN account settings are not in compliance with Agency Directives, Region VIII policies, and best industry practices; therefore, logical security is not optimally enforced via the network operating system. Furthermore, Region VIII does not adequately control physical access to its computer room. All of the above represent critical controls which must be adequately implemented to help ensure dial-up access to the region's systems, as well as to EPA's Network, are adequately protected. Based on discussions with Region VIII management, we believe that the lack of personnel resources has made security a low priority. These control inadequacies could leave the region's systems, as well as EPA's Network, vulnerable to security breaches from hacker attacks within and outside the Agency.

Advanced Authentication Techniques And Encryption Needed to Secure Access

Region VIII is not using any advanced authentication techniques, such as one-time password technology and dial-back, to protect their dial-up access to the network. Access to a LAN is generally limited to personnel with access to the facility. However, once dial-up access is provided, the network is potentially opened to the public by providing external access points. In our opinion, dial-up access to EPA's Network needs additional controls to properly secure and control these external access points.

The region's current means of authenticating dial-up users, encrypted static passwords, does not provide sufficient protection for EPA's network. Static encryption does not prevent a perpetrator from capturing the authentication password data and replaying it later to login as an authorized user. When a password is encrypted, an

algorithm is applied to the password to generate a "nonsense" string of characters (ciphertext) that represent the password. After the password is transmitted and received, a second algorithm is applied to undo (decipher) what the original algorithm did to generate the ciphertext. Because the Novell system applies the same algorithm to each password, whenever the same password is encrypted, the resulting ciphertext will be the same. Therefore, although a perpetrator cannot read your encrypted password (ciphertext), they still can provide the system with the correct password. The system is not expecting the password itself to be transmitted; rather, it is expecting to receive the encrypted password (ciphertext) which it will decrypt to validate the password. Any perpetrator can break into the system by grabbing the ciphertext (without knowing the password it represents) and submitting it to the system to be decrypted and validated. In this scenario, the ciphertext (the encrypted password) becomes the password, because the system is searching for the ciphertext to authenticate the user, not the password itself. Region VIII management indicated that they only use static encrypted passwords because they choose not to invest in more advanced technologies.

EPA's Information Security Manual requires encryption for the transmission of confidential information. Region VIII management stated they had not implemented encryption of the data due to a lack of funds. Region VIII indicated that users are not supposed to have any confidential information on the network. However, many of EPA's national applications require input of confidential information and these applications are accessed through the Network. For example, the Time and Attendance, Payroll and Personnel (TAPP) system is accessed through the LAN and requires the input, transmission, and storage of Privacy Act Information, such as social security numbers (considered confidential) maintained on the system. If Region VIII's LAN is compromised, perpetrators could use this unauthorized access to collect transmissions of confidential information sent over the LAN connection to the national system. The perpetrator could also use the unauthorized LAN access to compromise other systems that are accessed through the LAN connection, such as the national systems.

In response to our audit inquiries, management indicated that they plan to implement the 128-bit encryption provided with Novell Version 5, by the end of fiscal 2000.

In our opinion, encryption is also necessary to protect sensitive information transmitted by privileged users working on the system remotely. Novell system software provides the means (i.e., "remote console") for a user to perform, remotely, privileged tasks that are normally performed at the server itself. One way to obstruct perpetrators from performing privileged tasks is to prevent them from gaining physical access to the server. Remote console was designed to allow these privileged functions to be performed from a regular work station, so that the real server could be locked away in a safe place without a keyboard and monitor. To initiate a remote console session, the user must know and enter the remote console password for that particular server. When a privileged user logs into the network remotely to initiate a remote console session, the user must transmit that static password which gives the right to initiate the remote console session. Any user who gains access to a remote console session is allowed to:

- use console commands as if they were physically at the server console;
- scan directories and edit text files in both NetWare and DOS partitions on the server;
- transfer files to, but not from, a server;
- bring down or reboot a server; and
- install or upgrade NetWare.

If a "remote console" password is captured by a perpetrator, it provides privileged access that could potentially compromise the EPA network. Even if a perpetrator simply monitors a privileged user's session, the perpetrator can learn sensitive information about the server and how it is configured and secured. Such information could assist the perpetrator in subsequently manipulating or destroying

EPA data. These types of sessions are very sensitive and should require end-to-end encryption for the entire session. The system administrator indicated that he transmits sensitive information when he stated that he sometimes works remotely on the system, as a privileged user, to perform fixes rather than driving all the way to the office.

Our audit also disclosed that Region VIII uses the same remote console password for multiple servers, even though NTSD pointed out this vulnerability in a risk assessment, dated August 1, 1997. As a result, if a perpetrator figured out the remote console password for one of the servers, they could successfully gain remote console access on a number of others by trying the same password. As NTSD pointed out in their assessment, this practice is convenient, but it allows a security breach on a single server to compromise security on other servers and condones additional exposure of privileged IDs.

Logical LAN Account Settings Not Compliant With Directives, Policies and Best Practices

Some of the Region VIII LAN account settings are not in compliance with Agency Directives, Region VIII Policies, and best industry practices. Complying with minimum LAN settings is important because they implement the logical security enforced by the network operating system. The dial-up access relies on the logical security provided by the network operating system to help secure access to the Novell network. By not consistently following these guidelines, the region is leaving its LANs, as well as EPA's network, vulnerable to security breaches from hacker attacks within and outside the Agency. Due to the nature and quantity of the vulnerabilities noted, we are presenting them in a table format. The following table summarizes the vulnerabilities and effects on the Region's LANs, as discovered during our audit:

NOVELL LAN MANAGER RESULTS REGION VIII DENVER, CO	
CONDITION	**EFFECT**
Organizational Units with Intruder Detection Not Turned On	The Organizational Units within the NetWare System must be set to Detect Intruders in order to enable its Intruder Detection capabilities. When enabled, the system can track login attempts and lock accounts after the established number of consecutive

NOVELL LAN MANAGER RESULTS REGION VIII DENVER, CO	
CONDITION	**EFFECT**
	incorrect login attempts have been reached. Not turning on the Intruder Detection permits unlimited access attempts to the user accounts associated with the applicable Organizational Units by an intruder.
Organizational Units with Incorrect Login Attempts set greater than 3	The Incorrect Login Attempts represent the number of consecutive Incorrect Login Attempts within the time period specified within the organizational units of the system (by the Intruder Attempt Reset Interval) before the system detects the attempts as an intruder. Too high a number of allowed incorrect login attempts can give intruders multiple opportunities to gain access to the user accounts associated with the applicable Organizational Units within the system..
Organizational Units with Intruder Attempt Reset Interval set too low (less than 24 hours)	The Intruder Attempt Reset Interval is the amount of time the system stores the count of consecutive incorrect login attempts (without resetting them to zero) necessary for identifying access attempts as an intrusion. The count is set back to zero when the time interval expires or when a successful login occurs. Too short a period before the count of incorrect login attempts resets to 0, can give intruders multiple opportunities to access the user accounts associated with the applicable Organizational Units by allowing them more attempts on an account within a specified period without detection.
Organizational Units Not set to Lock Account after Detection	An intruder can repeatedly attempt to log into the server on user accounts associated with applicable Organizational Units without interruption if an organizational unit is not set to lock account after detection.
The Intruder Lockout Reset Interval not set to maximum number of days (999 days).	The Intruder Lockout Reset Interval is the amount of time the system maintains an account lockout without automatically resetting (unlocking) the account. The region stated that they set their Intruder Lockout Reset Interval to 90 days. EPA requires that it be set to the maximum that the operating system will allow or until the System Administrator unlocks the account.

NOVELL LAN MANAGER RESULTS REGION VIII DENVER, CO	
CONDITION	**EFFECT**
Accounts that Do Not Require a Password	All non-privileged user accounts (objects) should be required to have a unique alphanumeric password that is at least 6 characters long. Privileged user accounts (objects) should be required to have a unique alphanumeric password that is at least 8 characters long. The system should be setup to require a password for all user accounts. Requiring a password limits the exposure of a network to unlimited unauthorized usage.
Accounts that Do Not Require a Unique Password	The system should be set to require unique passwords. Not requiring unique passwords allows the user to reuse the same password over and over again. Since unique passwords cannot be reused after they have expired, requiring them limits the exposure of a network from unauthorized use of compromised passwords.
Accounts that Do Not Require Periodic Changes to the Password	The system should be set to require forced periodic changes to passwords. Not requiring periodic (at the most, every 90 days) changes to passwords allows a user to continue using the same password indefinitely. Requiring that passwords be changed periodically (at the most, every 90 days) limits exposure of a network from unauthorized use of compromised passwords.
Maximum Concurrent Connections not Limited to One.	The maximum concurrent connections should be limited to one. Allowing more than one concurrent connection not only creates the risk of users leaving unattended workstations logged into the file server but also allows perpetrators to log into a user's account at the same time as the user. If it was limited to one concurrent connection, the perpetrator would not be permitted to login if the user was logged in and vice versa. If a perpetrator was using the user's account, the user would be aware of a problem because the user would not be able to log into their account. The user would then be able to bring it to the system administrator's attention. With it not set at one concurrent connection, the user might never know that someone else was using their account.

NOVELL LAN MANAGER RESULTS REGION VIII DENVER, CO	
CONDITION	**EFFECT**
Minimum Password Length was not set at 6 for all non-privileged accounts and at 8 for all privileged accounts	The system should be set to require that all non-privileged accounts have a minimum password length of 6 and that all privileged accounts have a minimum password length of 8. Short passwords are easier to crack by a "brute force" method than are long passwords. Region VIII recognized this concept and was proactive in requiring privileged accounts to have a minimum password length of 8.
The Region stated they are only using Time and Day Restrictions for performing backups. The Region indicated that time and day restrictions are set at liberal levels to provide an optimum level of customer responsiveness.	The system should be set to restrict access to the network for hours that are not used for performing work (such as from 11:00PM to 4:00AM Mountain Time as a default). Users with a legitimate business need can have their restrictions set specifically to meet that need. By restricting access to the system by day and time, perpetrators will have a smaller window of opportunity to compromise accounts.

NTSD Server Setting Not Consistent with Best Industry Practices

The NTSD security server, used for dial-up access through the main numbers, is currently set to lock out an account on the fifth consecutive incorrect login attempt. As indicated in the table above, the system should be set to lockout an account after three consecutive incorrect login attempts. Setting the number of allowed incorrect login attempts too high can give intruders additional opportunities to gain access to the system.

Physical Access to Computer Room Inadequately Controlled

Although Region VIII uses access Card Keys to restrict physical access to the computer room, management is not adequately addressing other controls necessary to ensure the safety of computer resources and network data. For example, regional management does not adequately control the issuance, termination, and oversight of the access cards to the computer room. Neither has management implemented policies and procedures for adequately supervising and documenting visitors in the computer room. These inadequacies provide perpetrators with a

means of circumventing the logical security in place. In addition, security cameras only monitor the entrance and exit points to the EPA office space and do not monitor access to the computer room.

We also found that Region VIII has far too many employees and contractors with Card Key access to the computer room. Specifically, the Region has 139 Card Key IDs with key-card access to the computer room. This access is broken down as follows:

- 48 Card Key IDs with a Card Key access code of "06" (Access to computer room 24 hours a day/ 7days a week);

- 5 Card Key IDs with a Card Key access code of "60" (Access to computer room from 6:00 AM to 6:00 PM/ Monday through Friday); and

- 86 Card Key IDs with a Card Key access code of "08" (Access to everywhere in the Region, including the computer room 24 hours a day/7 days a week).

Furthermore, a survey performed by Region VIII's ISO determined that:

- only 6 personnel need Card Key 24 hours/7 days a week access to the computer room, because their job functions require them to enter the computer room on a regular and frequent basis, as well as, after hours (weekends, evenings); and

- an additional 7 personnel need Card Key workday access to the computer room, because their job functions require them to enter the computer room on a regular and frequent basis during normal work hours.

Access Code 60 was intended to be used to limit access by personnel (such as contractors and grantees) to the computer room to only those hours when it is manned by normal operations staff. Our analysis disclosed that the personnel (with Access Code 60) that were assigned limited

access to ensure that the computer room is manned during their visits, have the ability to access the computer room while it is not manned. Regional management confirmed that the computer room is manned during normal workday hours, from 06:30 AM to 05:00 PM, Monday through Friday. However, the limited hours assigned to personnel (Code 60) is from 6:00 AM to 6:00 PM, Monday through Friday. This difference in the hours allows these personnel (employees, grantees and contractors) the ability to gain access to the computer room while it is not manned.

Management Needs to Make Security A Top Priority

Operations management needs to make security a higher priority and apply an appropriate portion of available resources to properly secure, as well as maintain, dial-up access controls. Region VIII operations management indicated they were understaffed, because several people had left and their positions had never been refilled. They stated that the weaknesses we found were due to the lack of adequate staffing. Regional managers also indicated that they intentionally chose not to invest in more advanced security technologies due to a lack of funds. In our opinion, management needs to place a higher priority on information security by providing appropriate funding and additional qualified staff necessary to implement and maintain adequate security.

In our opinion, Region VIII also lacks the management oversight necessary to ensure that adequate security over their systems is implemented and maintained. For example, regional managers were aware of the results of the NTSD risk assessment, dated August 1, 1997, and yet many of the noted deficiencies were still present when we conducted our fieldwork two years later. In addition, Region VIII did not have a quality control function to ensure the controls were actually implemented and working as intended. For example, Region VIII policy states that all non-privileged users are required to use passwords which are at least six characters long. However, we found that the system did not require all non-privileged users to use passwords at least six characters long. A quality control function could have ensured that the system requirement was adequately enforced and working as intended.

Region VIII should also designate resources to establish adequate formal policies and procedures concerning the implementation of advanced authentication, logical access, and physical access controls. At present, Region VIII lacks acceptable formalized policies and procedures which (1) communicate to applicable personnel the control requirements and (2) specify how controls are to be implemented to ensure proper security.

RECOMMENDATIONS

Due to the nature of the issues, it is our opinion that both Region VIII and the Agency's NTSD need to implement corrective actions to effectively address these weaknesses. We recommend that the Assistant Regional Administrator for Technical and Management Services:

2-1. Require the use of advanced authentication techniques, such as one-time password technology and dial-back, to help protect their dial-up access to the network.

2-2. Provide initial and periodic training for all dial-up users to ensure they understand the policies and procedures related to protecting sensitive information.

2-3. Implement the following controls for privileged user's accounts and whenever "remote console" is used:

- a callback list or some other form of advanced authentication for authenticating the sessions,
- end-to-end encryption for the entire session, and
- console logging to record actions performed within the session.

2-4. Implement "remote console" password controls by requiring:

- read & browse access to the Autoexec.ncf file be limited to very few privileged users,
- different passwords for each server,
- periodic changing of the passwords,
- unique passwords,
- alphanumeric passwords (i.e., passwords containing a mixture of alpha and non-alpha characters),
- passwords that are at least 8 characters long, and
- encryption of the password.

2-5. Implement Agency and industry standards to correct the conditions identified in the Novell LAN Manager Results Table.

2-6. Establish and implement formal policies and procedures that ensure adequate control over the issuance, termination, and oversight of the access cards to the computer room. The formal policies and procedures should ensure that:

- requests for access identify the specific job duties requiring physical access to the computer room on a frequent basis. Requests should also identify the specific job duties requiring frequent access to the computer room during other than normal work hours, in order to justify card key access that allows other than normal workday hours access to the computer room.
- documentation is maintained to support the review and approval process.
- facilities personnel promptly remove an employee's access rights from the card key

system when such access is no longer required.

- all card key access to the computer room is reviewed and verified by the owner of the resource at least every six months. This process will ensure that the access possessed by the applicable personnel is still required for the performance of their jobs.

- code 08, which provides access to the *entire* regional space, not include access to the computer room. Access to the computer room should be limited to codes specifically for that purpose (e.g., codes 06 and 60).

- card key access to the computer room is limited to personnel with the proper level background investigation and whose job duties require them to have physical (not logical) access to the computer room on a regular and frequent basis. Non-EPA employees which fall into this category should have their access limited to normal work hours when the computer room is manned.

- times permitted for limited card key access to the computer room are modified to match the hours when the computer room is scheduled to be manned, and

- secured access cards are maintained by building security, and signed in and out by guards, building engineers, and building owners on an as needed basis.

2-7. Develop policies and procedures for supervision and documentation of visitors to the computer room. These policies and procedures should include, but not be limited to, the following guidelines:

- All personnel who do not possess a computer access card for the computer room should be considered a "visitor."

- All visitors should be required to: (1) sign in and out, and write the purpose for their visit on the computer room visitors' log; and (2) be escorted by personnel authorized to access the computer room without an escort (i.e., non-visitors) while in the computer room.

- Cleaning personnel should always be treated as a visitor.

In addition, we recommend that the Director of NTSD:

2-8. Implement formal policies and procedures for communications servers, which are set to lock out an account after 3 consecutive, incorrect login attempts.

AGENCY COMMENTS AND OIG EVALUATION

In a memorandum dated March 24, 2000, Region VIII's Assistant Regional Administrator for Technical and Management Services responded to our draft report (See Appendix I). The Region agreed with and established milestones for all seven chapter recommendations. Furthermore, the Region identified and set milestones for additional actions which will further secure authentication, logical and physical controls pertaining to dial-up access. Among other things, Region VIII's response indicated they will: (1) not implement dial-up access until NTSD implements an approved solution; (2) not use "remote console" until encrypted sessions and advanced authentication techniques are implemented; (3) implement policies and procedures to control the issuance, termination, and oversight of access cards to the computer room, as well as supervise and document visitor access; (4) continue to modify LAN account settings to comply with Agency and industry standards; and (5) provide initial and periodic training for all dial-up users to ensure they understand policies and procedures concerning the protection of sensitive information.

In our view, the corrective actions and milestone dates described in Region VIII's response to the seven recommendations are appropriate and should, when fully implemented, respond adequately to those recommendations. We will evaluate these corrective actions during our follow-up review.

NTSD's Director also responded to our draft report via a memorandum dated March 27, 2000 (See Appendix II). In summary, NTSD agreed with our audit findings and conceptually agreed with the report recommendation. However, management did not provide a detailed action plan and milestones for implementing corrective action because they are currently reviewing ways to implement the recommendation. NTSD has agreed to investigate the issue and reduce the number of allowed access attempts to an absolute minimum. However, they are concerned that revoking access after three failed attempts may be impossible, because multiple levels of authentication are required by the remote access login process.

CHAPTER 3

REGION IS NOT MONITORING DIAL-UP ACCESS AND THE USE OF MODEMS

Our audit disclosed that Region VIII does not log, audit, or follow-up on dial-up access to their computer systems, although such functions are basic to monitoring computer access points for security violations. In addition, the region does not have specific incident response policies and procedures for handling detected dial-up security incidents. During our audit, we discovered that NTSD was logging the dial-up access to Region VIII through the main access number connected with the Agency's remote access project. However, we determined that neither regional nor NTSD personnel are auditing the logs to identify potential security violations. Furthermore, logging for Region VIII's systems was turned off, because management stated they were waiting for Agency IRM officials to provide them with a standard configuration for establishing the logging capability. We also determined that Region VIII is not tracking and controlling the use of modems, nor are there any policies and procedures to govern modem usage.

In response to our audit, Region VIII issued policies and procedures related to the use of modems. These policies and procedures require that:

- modems must be approved in writing by the LAN Administrator, and

- only modems and software meeting approved Region VIII standards may be purchased or used.

However, our review found these new policies and procedures to be inadequate because they do not:

- adequately incorporate Agency Interim National Telecommunications Network Security Policy requirements which state: (1) all remote dial-up into the Agency's telecommunication network must utilize the Agency's approved remote access

solution; (2) the solution will be implemented by November 30, 1999; and (3) within 180 days following that date, all non-approved dial-up data circuits, modems, and modem banks must be removed by the local information management officials.

- ensure that authentication data is adequately protected with access controls, one-way encryption, and advanced authentication techniques to prevent unauthorized individuals, including system administrators, from obtaining and using the data.

- ensure that the location of modems, and individual(s) who control the use of the modems, are formally identified.

- ensure that the use of modems will be logged and audited for security incidents and that follow-up procedures are performed on incidents.

- ensure that formal written procedures are in place for approving connection of a modem before it can be connected to the network itself or to any workstation connected to the network. Procedures should specify how the formal approval process (in writing) will be performed and documented, as well as how the documentation will be maintained.

- ensure that inventory records will be maintained, providing information such as the location, phone number, etc. of each approved modem.

- ensure that the modem is added to the network schematic as a recognized dial-up connection.

- strongly state that unauthorized modems will not be permitted nor specify the consequences if the policy is not followed.

In response to our audit, Region VIII attempted to identify their approved modems. However, they could not identify the approved modems because they do not maintain an inventory of the modems and their locations.

The aforementioned dial-up access requirements are all critical controls that must be in place to adequately protect not only Region VIII's servers, but EPA's network as well. Without identifying all dial-up access points (such as modems), Region VIII is unable to identify which access points need to be monitored and controlled. Dial-up access points provide potential backdoors into the network and, therefore, must be continually logged and monitored. Without logging the dial-up access, the region cannot capture information necessary to hold users accountable, detect security incidents, and prosecute offenders. Furthermore, if the logs are not audited for potential security violations, then attacks on EPA's systems will not be discovered.

Management Needs to Make Security A Top Priority

As previously stated in Chapter 2, Region VIII's operations managers have not assigned security as a top management concern and, as a result, have not designated sufficient resources to adequately secure and maintain dial-up access. Regional management stated that they did not have sufficient human resources to address security controls, citing that several personnel vacancies were never refilled

We also believe that Region VIII lacks the management oversight necessary to ensure that adequate security over their systems is implemented and maintained. In particular, we refer to a prior regional risk assessment, performed by NTSD in August 1997. Although NTSD alerted Region VIII managers to various control deficiencies, we noted that many of these deficiencies still exist. In many respects, management seemed to be unaware of what network activities were and were not being conducted within the region. For example, management indicated they thought dial-up access was being logged and monitored; however, our audit disclosed that the Region was not conducting such activities and that the audit logging capability for Regional servers was not turned on at all. Similarly, management thought they could generate a list of approved modems, but later realized that they could neither identify how many modems existed within the region nor where these modems were located. Our audit results demonstrated that Region VIII has not implemented a quality control function to ensure sufficient controls exist and are operating as intended.

In our opinion, another contributing cause is the absence of acceptable formal policies and procedures needed to communicate regional control requirements and specify how controls should be implemented. Currently, Region VIII does not have adequate formalized policies and procedures to address control functions over dial-up access, such as (1) logging, auditing, and follow-up and incident response processes, and (2) the identification, use and administration of modems.

Furthermore, Region VIII staff believe they lack the guidance and training they need to perform their jobs. For example, during our audit, Regional managers indicated that they were waiting for guidance and training before implementing any logging, auditing, follow-up, and incident reports regarding dial-up access. Additionally, management indicated that they were waiting for guidance and training from NTSD (as described in Chapter 5) before turning on the Network logging function. As a result of our audit findings, management indicated that they would contact NTSD and start logging, auditing and following up on dial-up access attempts.

RECOMMENDATIONS

We recommend that the Assistant Regional Administrator for Technical and Management Services:

3-1. Establish formal policies and procedures that require all dial-up accesses to be logged and monitored for security incidents. These logs should be reviewed on a daily basis to detect security incidents through the use of exception reports, statistics, etc.

3-2. Develop formal policies and procedures that detail the specific responses to be taken when a security incident is identified.

3-3. Revise formal policies and procedures related to the use and control of modems. Ensure that modems are identified and adequately secured.

AGENCY COMMENTS AND OIG EVALUATION

TMS's March 24, 2000, response to our draft report indicated that they agreed with all of the report recommendations (See Appendix I). Specifically, the Region established milestones for implementing corrective actions to address the three recommendations detailed in this chapter. In summary, Region VIII officials agreed to (1) establish formal policies and procedures covering dial-up access logging, as well as security incident handling; and (2) revise formal procedures related to the use and control of modems.

In our view, the corrective actions and milestone dates described in Region VIII's response to this chapter's three recommendations are appropriate and should, when fully implemented, respond adequately to those recommendations. We will evaluate these corrective actions during our follow-up review.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4

DIAL-UP ACCESS AND TERMINATION CONTROL PROCEDURES ARE INADEQUATE

Our review disclosed that terminated employees retain dial-up access to the network. Specifically, we found that many of Region VIII's terminated/separated employees still possess card key account access to the computer room or on-line access to EPA's network. Our audit also disclosed that Region VIII is maintaining two conflicting lists of personnel approved to dial into and work on the network from locations such as home, hotel, etc. (i.e., telecommuters). In addition, neither of the two lists of approved telecommuters are enforced by the network operating system. Although Region VIII had policies and procedures related to the aforementioned areas, those policies and procedures, as well as their implementation, did not ensure telecommuter access was properly approved and controlled. Furthermore, those policies and procedures did not ensure that the access rights of terminated personnel were removed. These are critical controls which must be in place to adequately protect Region VIII's Systems, as well as EPA's network.

Terminated/Separated Employees Maintain Access Rights

Our audit results disclosed that terminated/separated employees still possess card key account access to the regional computer room or the ability to access the network directly or via dial-up. Although an employee is required to submit their card key as a part of the Employee Separation or Transfer Checklist (ESTC), not removing the access allows the card to continue to be used by whomever possesses it. If used, the card would indicate that the terminated employee entered the computer room, rather than the person who actually possessed the card.

Currently, Region VIII uses an ESTC to process personnel transfers, terminations, and separations. The ESTC provides a checkoff block to verify removal of LAN User IDs, but the form does not provide a checkoff item for removing personnel from the computer room access list. All the ESTCs reviewed indicated that Network access had

been removed; yet we noted many instances in which terminated employees still had active Network User IDs. Management indicated that, in most cases, they signed off on the checklist, recognizing the need to actually disable the account at a later date. Management believed that the cases we found were instances where the signing official forgot to return to disable the account.

Not eliminating access of terminated/separated personnel gives potentially disgruntled persons the ability to access the computer room and network. This regional weakness also propagates accounts assigned to users who no longer exist on EPA's employment rolls. These accounts are prime targets for hackers to get a foothold into the network, because no users exist to complain, should changes occur to their account.

Region Needs Better Policies and Procedures To Govern Personnel Departures

In our opinion, the Region's current policies and procedures regarding terminated and separated personnel are not adequate. Current policies do not ensure that terminated/separated employees' access rights are removed on the effective date or prior to the notification date of the action, dependent on whether the departure is friendly or unfriendly. Furthermore, these policies and procedures do not adequately address important control considerations, such as:

- requiring all requests for access to state the level of access to be granted, perhaps by function or by specifying a particular user profile. This control will help ensure that the access levels of the account will be consistent with those requested by the supervisor.

- tracking new applications to add, upgrade and remove access to ensure that (1) users only are allowed access to those functions necessary to perform their assigned duties and (2) the access rights provided are up to date.

- specifically describing separate procedures for handling friendly and unfriendly terminations.

- ensuring that (1) access rights of potentially unfriendly terminations (e.g., fired or laid-off personnel) are removed *prior* to notifying said employees, and (2) management's position regarding consequences when such procedures are not followed is clearly stated and enforced.

- issuing management's position regarding (1) the prompt removal of access rights for all terminated personnel's user accounts, (2) required removal of all terminated personnel's user accounts within a specified time frame, and (3) consequences which will occur if procedures are not followed within the specified time frame.

- requiring SIRMOs to follow-up on procedures for deactivating accounts and ensure that such procedures have been accomplished, as required by EPA's Information Security Manual.

List Of Approved Dial-Up Users Is Not Complete, Accurate or Enforced

Region VIII maintains two conflicting lists of approved telecommuters and neither list is enforced by the system. Both human resources and the systems group maintain lists of approved telecommuters, but these two lists do not agree with each other. Furthermore, we discovered that any user who is included in the NetWare Directory Service (NDS) Tree (that is, every user in Region VIII with Network access) is permitted, by the network operating system, to access the network via dial-up connection.

Accurately identifying, tracking, and enforcing user-specific dial-up access needs is a critical control which must be in place to adequately protect not only Region VIII's servers, but EPA's Network as well. Inadequate controls over who can access the network via dial-up allows all users, by default, to have this access. Moreover, the situation provides more potential user accounts through which a hacker can attempt to gain access. In addition, this exposed method of controlling access requires the system administrator to monitor (on a daily basis) the dial-up usage of a larger number of user accounts for potential security violations.

Region Needs Policies, Procedures and System Controls to Secure Remote Access

Our audit disclosed that Region VIII has not established policies and procedures to ensure that the Human Resources list of approved telecommuters represents a valid and complete accounting of people who require dial-up access to the system. Furthermore, Region VIII has not established a separate user group within the network operating system which only includes authorized dial-up users as members. Establishing a separate system group would restrict the dial-up access to only authorized users who require remote access to perform their job.

RECOMMENDATIONS

We recommend that the Assistant Regional Administrator for Technical and Management Services:

4-1. Develop formal dial-up policies and procedures that ensure terminated/separated employees' access rights are removed on the effective date for friendly actions or as soon as possible for unfriendly actions (i.e., immediately upon notification if initiated by the employee or prior to the notification date if initiated by EPA).

4-2. Establish and implement policies and procedures that require periodic review and verification (at least every 6 months) of logical and physical access rights to the computer facilities to ensure that personnel still need such access to perform their jobs.

4-3. Establish and implement formal dial-up policies and procedures that require all users requesting remote access to go through a formal approval process prior to being provided with remote access to the Network.

4-4. Establish a separate NetWare user group within the Operating System that provides dial-up access rights to the Network. Only add a user to this group once the user has been formally approved to access the network via dial-up connections.

AGENCY COMMENTS AND OIG EVALUATION

In a March 24, 2000 memorandum, Region VIII's Assistant Regional Administrator for TMS responded favorably to our report recommendations. The Region agreed with the four recommendations outlined in this chapter and established milestones for implementing corrective action. Furthermore, Region management identified and set milestones for additional actions which, they agreed, would further secure dial-up access and termination control procedures. In summary, Region VIII officials agreed to establish and implement formal policies and procedures covering: (1) the granting of remote access rights, (2) periodic review and verification of logical and physical access rights to computer facilities, and (3) the prompt removal of access rights for terminated or separated employees. Regional personnel also stated that NTSD is now controlling the access list of all dial-up users and that they will rely on NTSD's solution.

In our view, the corrective actions and milestone dates described in Region VIII's response to the four recommendations from this chapter are appropriate and should, when fully implemented, respond adequately to those recommendations. We will evaluate these corrective actions during our follow-up review.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5

CURRENT PLANS WILL NOT ADEQUATELY SECURE THE NETWORK VIA DIAL-UP ACCESS

While evaluating Region VIII's dial-up controls, we identified security issues which impact the Region's ability to adequately protect their dial-up access, although they were out of their direct control. These particular security issues fall under the control of EPA's National Technology Services Division (NTSD), and impede the Region from (1) implementing adequate dial-up controls and (2) effectively and efficiently monitoring dial-up access. Because of the significance of these issues, we are including them as a part of our audit report.

EPA's current plans do not sufficiently ensure that dial-up access to the Agency's network will adequately secure the dial-up entry point(s) to the network, nor do their plans ensure that the monitoring of dial-up access will be accomplished in an effective and efficient manner. In particular, we discovered that NTSD currently has no plans to force dial-up access through the Internet Firewall (i.e., the firewall intended to separate the Agency's internal network from all external sources). In addition, we found that NTSD management has no plans to provide additional statistics, logs, exception reports, guidance or training to assist cognizant sites with monitoring dial-up access for security violations. We believe that the Agency's implementation of controls to support and secure dial-up access are critical, because they represent the first line of defense to the EPA Network. In our opinion, management needs to assign a higher priority to security to help ensure that dial-up access is adequately secured.

Current Plans Will Allow Backdoors Into EPA's Network

NTSD currently allows dial-up users to connect directly to EPA's network through communications servers; furthermore, management has no plans to force dial-up access to these servers through the Firewall, once implemented. As such, dial-up connections to regional communication servers will not be directed through the Agency's firewall(s). In our opinion, such a configuration

will defeat the purpose of the firewall(s) by providing backdoors into EPA's network. One of the basic requirements for a firewall to be effective is that all external traffic must pass through it. The more exceptions management makes to that basic philosophy, the less reliance the Agency can place on its ability to secure data from external users.

No Statistics Or Exceptions Reports To Assist System Administrators

NTSD management has no plans to create additional statistics, logs, or exception reports to assist system administrators in monitoring dial-up access for security violations. Although logged information is available for monitoring security, no exception reports or statistical information are specifically designed and disseminated to assist the System Administrators (SAs) in monitoring dial-up access for security incidents. At present, SAs must execute queries against log files to obtain information useful for monitoring the dial-up access to their systems. While providing SAs with the ability to query the log files is a good option, we believe that a more time- and cost-effective approach would be to provide them with standardized exception reports and statistics. In our opinion, providing SAs with reports and statistics to monitor their systems' security may help combat the inconsistencies which currently exist regarding the application of security controls between regions and program offices within EPA.

Lack Of Guidance And Training Inhibit Insightful Analysis Of System Data

Our audit disclosed that NTSD management assigns responsibility and provides a tool for System Administrators to use in fulfilling that responsibility, but they do not provide adequate guidance and training on how to use the tool to fulfill the responsibility assigned. Currently, NTSD management has no plans for providing training or formal guidance to SAs regarding how logs, statistics, or reports should be used to monitor dial-up access for security violations. However, NTSD management stated that they plan to disseminate information to Agency Security, Telecom, and Information Technology operations managers to inform them that such information is available for use. In our opinion, providing adequate tools, guidance and training to the personnel responsible for monitoring dial-up access is necessary to

help ensure that monitoring is performed correctly and in a consistent, efficient and effective manner.

Management Not Planning To Afford Security Adequate Resources

Management needs to assign a higher priority to security to help ensure that dial-up access is adequately secured. NTSD officials state that the cost of implementing a firewall for each of the planned remote access servers is prohibitive; for that main reason, they do not plan to force the dial-up access through the Firewall. Furthermore, NTSD management believe that exception reports, additional logs or statistics are not needed to assist regions in monitoring dial-up access. Management believes that regional staff can do an adequate job of monitoring access if NTSD (1) continues to log all available data from the Cisco Secure System and (2) provides cognizant personnel query access to these logs. NTSD management also indicates that guidance, policies, and procedures related to remote access will be included in the Agency's Network Security Policy, which is still in the process of being developed.

RECOMMENDATIONS

We recommend the Director of NTSD:

5-1. Establish and implement formal policies and procedures that ensure that all dial-up connections are routed through the Firewall(s) once the firewall is completed.

5-2. Develop standardized exception reports and statistics that would assist system administrators and ISOs in monitoring dial-up access to their systems for security incidents.

5-3. Develop and implement formal guidance and training for system administrators and ISOs to instruct them in the use of the logged information currently available (as well as any additional logs/statistics/reports) used to monitor their systems for security incidents. This training and guidance should also educate them on how to respond to security incidents.

AGENCY COMMENTS AND OIG EVALUATION

In a memorandum dated March 27, 2000, the Director of NTSD responded favorably to our draft report (see Appendix II). Although NTSD generally agreed with our audit findings, management did not provide a detailed action plan in response to recommendation #5-1, nor did they identify milestones for implementing a corrective action. NTSD management stated that they are reviewing ways to implement that recommendation and will provide a detailed action plan to the OIG by June 1, 2000.

To date, NTSD management has agreed to: (1) investigate and implement standard exception reports and statistics to facilitate the access log review process; (2) develop guidance to assist EPA personnel in using log information to monitor access and respond to security incidents; and (3) provide formal training to system and security staff via an ISO conference.

APPENDIX I

Response to Draft Report
Region VIII

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
REGION 8
999 18TH STREET - SUITE 500
DENVER, CO 80202-2466
http://www.epa.gov/region08

REF: 8TMS-ISP MAR 24 2000

MEMORANDUM

SUBJECT: Security of Region VIII's Dial-up Access
Audit No. 0000165

FROM: Patricia D. Hull, Assistant Regional Administrator
Office of Technical and Management Services

TO: Patricia H. Hill, Director
ADP Audits and Assistance Staff (2421)

This is to respond to your audit titled "Security of Region VIII's Dial-up Access," Audit No. 0000165 dated February 23, 2000.

I want to assure you that both I and our Region 8 Information Systems Program staff acknowledge the importance of the findings in this audit, especially in light of recent concerns regarding EPA's Internet and data security raised by the Government Accounting Office and members of Congress.

To manage some of the vulnerabilities identified in your audit, we in Region 8 have created and attached for your review a "Region 8 Remote Access Audit Mitigation Plan and Schedule" and have already completed a number of actions to correct practices and policies where we can. Please review this plan, and let us know any concerns you may have.

I do want to emphasize that many of the policies and procedures which you have judged inadequate to achieve secure remote access constitute agency-wide issues, with the primary responsibility for correction belonging to the Office of Environmental Information (OEI) and to the National Systems Technology Division (NTSD), the offices responsible for designing and implementing remote access agency-wide. In our work plan we have identified areas where we believe action and progress are dependent upon action for OEI and NTSD.

On behalf of myself and our Region 8 Information Systems team, I do wish to thank you and your staff for the cooperative manner in which this audit was conducted by Mr. Ed Shields and Mr. Chuck Dade. We look forward to a similar collaborative approach with you and with OEI and NTSD in managing the actions needed to achieve fully secure remote access to agency information systems and data.

If you have questions, you may contact Paul Riederer, Director of Information Systems at (303) 312-6635 or e-mail riederer.paul@epa.gov. or Carl Worster, Information Security Officer at (303) 312-6865 or e-mail worster.carl@epa.gov.

Attachment

cc: Ed Shields
Chuck Dade
Mark Day
Rick Martin

REGION 8 REMOTE ACCESS AUDIT

Mitigation Plan and Schedule

Item No.	Recommended Mitigation Action	Projected Completion Date	Actual Completion Date	Comments Or Action Taken To Mitigate The Vulnerability
1	Implement advanced authentication techniques such as one-time passwords or dial-back technology	7-30-01		Dial-in is now exclusively controlled by NTSD at the EPA router. Future dial-in is dependent upon an agency-wide implemented solution. Region 8 will not re-implement dial-in until an approved solution is in place.
2	Organizational Units with Intruder Detection Not Turned On		8-30-99	Corrected 8-30-99 and reverified 2-26-00
3	Organizational Units with Incorrect Login Attempts set greater than 3		8-30-99	Corrected 8-30-99 and reverified 2-26-00
4	Organizational Units with Intruder Attempt Reset Interval set too low (less than 24 hours)		8-30-99	Corrected 8-30-99 and reverified 2-26-00
5	Organizational Units Not set to Lock Account after Detection		8-30-99	Corrected 8-30-99 and reverified 2-26-00
6	The Intruder Lockout Reset Interval not set to maximum number of days (999 days).		8-30-99	Corrected 8-30-99 and reverified 2-26-00

7	Accounts that Don't Require a Password		8-30-99	Corrected 8-30-99 and reverified 2-26-00. Monitoring is performed three times per week (minimum) by ISO using an automated report program.
8	Accounts that Don't Require a Unique Password		8-30-99	Corrected 8-30-99 and reverified 2-26-00
9	Accounts that Don't Require Periodic Changes to the Password		8-30-99	Corrected 8-30-99 and reverified 2-26-00
10	Maximum Concurrent Connections not Limited to One.		2-26-00	Corrected 8-30-99 and reverified 2-26-00. Monitoring is performed three times per week (minimum) by ISO using an automated report program.
11	Minimum Password Length was not set at 6 for all non-privileged accounts and at 8 for all privileged accounts		8-30-99	Corrected 8-30-99 and reverified 2-26-00
12	The Region stated they are only using Time and Day Restrictions for performing backups. The Region indicated that time and day restrictions are set at liberal levels to provide an optimum level of customer responsiveness.	9-1-00 at the latest		These controls will be implemented as soon as hours of operation are approved by management and users are notified of the change. This control will be installed in the new desk-top images that are being created for the Ethernet conversion project.

13	The NTSD security server, used for dial-up access through the main numbers, is currently set to lock out an account on the fifth consecutive incorrect login attempt instead of three. ***NTSD response req'd***		8-30-99 Region 8 action is completed.	Requires action from NTSD. All accounts have been locked. The Region 8 Novell NOS is set to lock after 3 invalid login attempts for all users.
14	Implement policies and procedures to control the issuance, termination, and oversight of the access cards to the computer room based on documented frequency and need.	4-15-00		
15	Implement policies and procedures for adequately supervising and documenting visitors to the computer room.	4-15-00		
16	Region VIII has far too many employees and contractors with Card Key access to the computer room.	4-15-00		
17	LAN administrators and select critical staff should have 24 hour access to the computer room. Others only during scheduled duty hours.	4-15-00		
18	Security cameras do not monitor access to the computer room.	5-30-00		Two additional cameras are expected to be installed by 5-30-00. Wiring is completed.

19	Operations management needs to make security a higher priority and apply an appropriate portion of available resources to properly secure, as well as maintain, dial-up access controls.	6-30-00 9-30-00 12-31-00 3-31-01		LAN manager, LAN SA's, ISO and IRM chief will work on security. Will develop SOP's, training and implement. Will assess progress quarterly.
20	Management needs to place a higher priority on information security by providing appropriate funding and additional qualified staff necessary to implement and maintain adequate security.	12-30-00		R8 already has a full-time ISO. Additional staff are dependent upon budget and Senior Leadership Team authorization. NTSD leadership is needed for ISO PD, training and guidance.
21	Region VIII lacks the management oversight necessary to ensure that adequate security over their systems is implemented and maintained.		8-30-99	Management oversight was increased following the first exit interview by the IG audit team.
22	Management needs to be involved in establishing and implementing policies and procedures.	6-30-00 9-30-00 12-31-00 3-31-01		IRM chief has scheduled formal reviews each quarter with ISO and LAN manager.
24	Region VIII did not have a quality control function to ensure the controls were actually implemented and working as intended.	6-30-00		Audit reports are being written so ISO can monitor compliance with standards; formal review scheduled for 6-30-00.

25	Region VIII lacks acceptable formalized policies and procedures which (1) communicate to applicable personnel the control requirements and (2) specify how controls are to be implemented to ensure proper security.	6-30-00 9-30-00 12-31-00 3-31-01		ISO and LAN manager are assigned these tasks. Formal reviews are scheduled for each quarter.
26	Provide initial and periodic training for all dial-up users to ensure they understand the policies and procedures related to the protection of sensitive information.	8-30-00		Region 8 has done this and will do again as we roll out "Desktop 2000" with new, more secure remote access procedures.
27	Implement and require use of an advanced authentication technique like dial back or smart cards, console logging and end-to-end encryption whenever "remote console" is used.	9-30-01		Dial in is now controlled at the NTSD router. Dial in is dependent upon a selection and implementation by NTSD. Remote console will not be used until this is implemented. Encrypted passwords and screen savers with passwords have been installed on all Novell and NT servers.
28	Provide and require use of end-to-end encryption for dial up access when performing sensitive work or when using a privileged account.	9-30-01		Is dependent upon selection and guidance from NTSD. Users are instructed to not store or send confidential data over the network. Staff with a privileged account will not dial in unless end-to-end encryption is used.

29	Enable console logging to log actions performed when using privileged accounts.	8-30-00		When new servers with adequate disk space are installed. Parameter settings and testing needs to be performed.
30	Implement "remote console" password controls including 8 character alphanumeric, unique, encrypted passwords, periodic changes and different passwords for each server.		Passwords meeting standards were implemente d 1-30-00 or before.	Verified and passwords changed again 2-26-00. Passwords were set to 10 digits alphanumeric for the three primary LAN administrators. Remote console is not and will not be used until encrypted sessions and advanced authtentication is implemented.
31	Read and browse access to the Autoexec.ncf file needs to be limited to a very few privileged users.		1-30-00 Partially completed.	Autoexec.ncf is encrypted and hidden. Filters have been installed on all Novell servers with only the three primary LAN administrators having access.
32	Establish and implement formal policies and procedures to ensure that agency LAN NOS standard settings are maintained	5-30-00		Audit reports are being written and used so ISO can monitor compliance with standards. Monitoring has begun.
33	Establish and implement formal policies and procedures that require periodic reviews to ensure that the policies and procedures are practiced and effective.	6-30-00 9-30-00 12-31-00 3-31-01		IRM chief has scheduled quarterly, formal reviews for one year of follow-up action.

34	Install and use ESM software to assist in the oversight function.	7-30-00		**A major resource issue!** NTSD cost estimate is $1,000,000. Regions do not have the funding nor does WCF fund this. Dependent upon NTSD obtaining licenses and testing to confirm that earlier problems with the software have been fixed.
35	Review computer room key card access approvals at least every six months. Whenever no longer needed, access should be removed.	5-30-00		ISO will review monthly. Are getting a unique code assigned to the computer room. Are exploring separating operations from network operations with a new wall and separate access doors and locks.
36	Non-EPA employees and staff with limited key card access should have access to the computer room limited to hours when the computer room is staffed.	5-30-00		R8 is negotiating for day-time cleaning and other measures to meet this goal.

37	An access card should be kept in a sealed envelope that has been signed by the ISO by building security and should be signed in and out by guards, building engineers and building owners on an as needed basis. The ISO should be contacted by building security each time an access card is checked out to check the log and reseal and sign the access card.	5-30-00		
38	Develop policies and procedures for supervision and documentation of visitors to the computer room. All computer card access requests should be approved by management and a copy provided to the ISO to facilitate validation of the computer room access list on a regular basis.	4-15-00		
39	All personnel without an access card must be considered a visitor and must sign in and out and document their purpose for the visit. They must be escorted by a person with an access card.	4-15-00		
40	Cleaning personnel, building engineers and contractors should always be treated as a visitor.	4-15-00		
41	Establish formal policies and procedures that require all dial-up accesses to be logged and monitored for security incidents.	4-30-00		ISO will contact NTSD to learn how to obtain remote access log reports for Region 8 and will incorporate these procedures into a formal policy.

42	Review dial-up logs on a daily basis to detect security incidents through the use of exception reports, statistics, etc.	4-15-00		ISO will contact NTSD to learn how to obtain remote access log reports for Region 8 and will begin reviewing daily logs.
43	Develop formal policies and procedures that detail the specific responses to be taken when a security incident is identified.	4-30-00		
44	Revise formal policies and procedures related to the use and control of modems. Ensure that modems are identified and adequately secured.	4-30-00		
45	Develop formal dial-up policies and procedures that ensure terminated/separated employees' access rights are removed on the effective date or prior to the notification date of the action depending on whether it is a friendly or unfriendly termination.	4-15-00		
46	Establish and implement policies and procedures that require periodic review and verification (at least every 6 months) to ensure that the logical and physical access rights to the computer facilities are still required to perform their jobs.	4-30-00		

47	Establish and implement formal dial-up policies and procedures that require all users requesting remote access to go through a formal approval process prior to being provided with remote access to the Network.	5-30-00		
48	Establish a separate Netware user group within the operating system that provides dial-up access rights to the network. Only add a user to this group once the user is formally approved to access the network via dial-up.		Revised process implemented on or about 3-6-00	NTSD is exclusively and centrally controlling the access list of all dial-up users. This equivalent control is already implemented through the NTSD TACAS router software. NTSD is also currently using a formal approval and authentication process through TSSMS for remote users.
49	For employees who are known in advance to be leaving, incorporate the use of user account expiration dates to preset the NOS system to disable the account as of the specific applicable date and use security monitoring software (such as ESM) on a regular basis (i.e., every 30 days) to ensure that the access and account are actually removed.	4-15-00		

APPENDIX II

Response to Draft Report
NTSD

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
RESEARCH TRIANGLE PARK, NC 27711

MAR 2 7 2000

OFFICE OF
ENVIRONMENTAL INFORMATION

MEMORANDUM

SUBJECT: Security of Region VIII Dial-Up Access
Audit No. 0000165

FROM: Richard A. Martin, Director
National Technical Services Division (MD-34)

TO: Patricia H. Hill, Director
ADP Audits and Assistance Staff (2421)

Thank you for the opportunity to respond to your draft of audit 0000165 published on January 12, 2000. I agree with the findings of fact and conceptually agree with the recommendations presented in that portion of the audit to the Office of Technology Operations and Planning (OTOP). Specific responses to each finding and recommendation addressed to the National Technology Services Division (NTSD) are listed on the attachment.

Again, I appreciate the useful recommendations on this subject and look forward to your continuing input on these issues as we implement enhanced security controls. If you have any questions on this response, do not hesitate to contact me.

Attachment

Response to Findings and Recommendations: Audit No. 0000165

No Logging or Monitoring of Dial-Up Access and Control of Modem Usage

Agree. Regular and timely log reviews by local and national CISCO remote access managers will be implemented to improve the Agency's information security posture. The National Computer Center does collect data on attempts to access the CISCO remote access servers and formats them into a database for analysis. The logs are reviewed by both national and local CISCO remote access server managers on a frequent basis but the specific requirements will be delineated in a memorandum to be issued within 30 days.

NTSD Plans Impact of Adequacy of Security

Agree. As you are undoubtedly aware, recent actions taken by the Office of Environmental Information (OEI) in response to the General Accounting Office (GAO) audit have changed the overall information security posture of the Agency to a considerable degree.

On February 18, 2000 the Agency's Internet connection to the Wide Area Network at RTP was disconnected and Programs were instructed to disconnect their external network connections such as remote access servers, modems, and Cubix boxes. The OEI then began a comprehensive security review to rectify vulnerabilities present in our IT infrastructure. As we gain a clear understanding of the business requirements and potential security exposure of each network service, that service is restored with appropriate security improvements or discontinued. To date, we have restored a large portion of the Internet-based public access services and have limited restoration of Internet and dial-up remote access.

Across the Agency, security controls are being substantially upgraded for all systems using external connectivity. The long-term solution to remote dial-up access has a number of technical, risk and cost issues which we will address in our security planning effort. For example, we must examine the relative risk of allowing remote access services through our primary firewall as this may require the enabling of services which cannot be statefully inspected. Routing of all remote access through this single point may also greatly increase long distance costs and network capacity requirements and costs. Routing the traffic to local sites with enhanced authentication, access restrictions, and intrusion detection at each site may prove more cost-effective and allow greater network segmentation to limit the scope of any penetrations. These are technical, cost, and risk issues which we will balance as we proceed.

In the meantime, we are implementing additional protections for dial-in services. For example, we restored Notes email services after implementing greater access list verification, assuring that two factors are present for authentication, restricting the scope of routing of the remote access servers and implementing the CERT router filters in each server. All of these provide reasonable compensating controls in the short term. Additionally, locations will not be authorized for remote access restoration until after the access control lists have been quality assured.

Management Needs to Make Security A Top Priority

Agree. I hope that I have conveyed OTOP's serious commitment to all aspects of security management in our increasingly complex environment.

Recommendations

2-8 Implement formal policies and procedures for communications servers which lock out an account after 3 consecutive incorrect login attempts.

Agree. This policy is in effect for central systems and I conceptually agree it should be mandated for remote communications servers. However, additional analysis is required before the policy is fully implemented. Remote access login requires multiple levels of authentications (router, NDS, etc.) and revoking access after 3 failed attempts may be impossible. NTSD will investigate the issue and will reduce the number of allowed access attempts to an absolute minimum. A follow up memorandum detailing our actions will be provided by June 1, 2000.

5-1 Establish and implement formal policies and procedures that ensure that all dial-up connections are routed the Firewall(s) once the firewall is completed.

Agree. As with the preceding recommendation, careful technical analysis will be required to determine how this recommendation can be best implemented. The choice of protocols and encryption techniques have profound effects on how well the firewall controls access. The final answer on the implementation of this recommendation must wait until the Agency firewall(s) and remote access methods are fully configured. A follow up memorandum detailing our actions will be provided by June 1, 2000.

5-2 Develop standard exception reports and statistics that would assist system administrators and ISOs in monitoring dial-up access to their systems for security incidents.

Agree. Reports of this nature already exist and NTSD will investigate and implement improvements to facilitate the access log review process.

5-3 Develop and implement formal guidance and training for system administrator and ISOs to instruct them in the use of logged information currently available (as well as any additional logs/statistics/reports) used to monitor their systems for security incidents. The training and guidance should also educate them on how to respond to security incidents.

Agree. NTSD believes that the suggested training materials already exist in various documents. Consolidation of these materials into guidance will be completed by April 15, 2000. Formal training will be offered as part of the proposed ISO conference targeted for later this fiscal year.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX III

REPORT DISTRIBUTION

Office of Inspector General

Inspector General (2410)

Assistant Inspector General for Audit (2421)

Deputy Assistant Inspector General for Internal Audits (2421)

Deputy Inspector General for Audit – Southern Audit Division

Deputy Inspector General for Audit – Central Audit Division

Audit Manager, RTP, NC Audits Branch (MD-53)

Audit Manager, Denver, Colorado Audit Branch (8OIG)

EPA Headquarters

Chief Information Officer (3101)

Agency Audit Followup Official (2710)

Agency Followup Coordinator (2724)

Director, National Technology and Services Branch (MD-34)

Director, IT Policy and Planning Division (2831)

Chief, IT Policy and Planning Division (2831)

OEI Audit Liaison (2811R)

Region VIII

Assistant Regional Administrator,
Office of Technical and Management Services, (8TMS-D)

Director, Data Systems Management Branch (8TMS-D)

Region VIII Audit Liaison (8TMS-G)