GUIDE FOR PROTECTING LOCAL AREA NETWORKS AND WIDE AREA NETWORKS (LANs/WANs)

Department of Health and Human Services

1. INTRODUCTION AND SUMMARY

1.1 PURPOSE AND SCOPE

This guide provides a step-by-step approach for protecting Local Area Networks (LANs) and Wide Area Networ
security of LANs in a sensitive information environment. WANs are discussed as an extension of the LAN envi
information" as any information, the loss, misuse, disclosure, or modification of which could adversely affect the
individuals are entitled under the Privacy Act.

The Department of Health and Human Services (DHHS) depends on accurate and timely information to manage
These programs and
payments touch the lives of most citizens. Virtually all vital information is processed in some form by compute
research grants, to the processing of individual entitlement payments. "We are at risk," advises the National Res
Council in Computers at Risk. "Although we trust them, computers are vulnerable - to the effects of poor desig
deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may b
to do more damage with a keyboard than with a bomb. To date, we have been remarkably lucky."

Connecting computers into networks significantly increases risk. Networks connect large numbers of users to s
cooperation of each user. Security is only as strong as the weakest link. A computer security study by the Pres
Inspector General, found that "virtually
all of the abuses and frauds [identified in the study] were carried out by authorized users, not outsiders." As the n
becomes
a much more significant issue to deter fraud, waste, and abuse and to avoid embarrassment to the government.

This guide is intended to help LAN managers understand why they should be concerned about security, what the
of this document addresses the why, highlighting the basic statutory and Federal requirements for protecting LA
complexities of LANs, Section 2 briefly summarizes LAN components and features to serve as a foundation for
security requirements are in terms of the risk assessment process. Section 4 addresses how to implement LAN s
amplify Section 4 with specific examples that can be used. The result is a guide that can be tailored to specific

1.2 DEFINITION OF LAN AND WAN

OMB has classified computer systems into two categories: general support systems and major applications. Ge
or network support for a variety of users and applications. General support systems include LANs/WANs.

A LAN, or local area network, is a network of personal computers deployed in a small geographic area such as an office complex, building, or campus within the context of this discussion. A WAN, or wide area network, is an arrangement of data transmission facilities that provides communications capability across a broad geographic area (e.g., DIMES/FTS 2000).

More detailed definitions are listed in Appendix A. 1.3 FEDERAL SECURITY REQUIREMENTS FOR

LANs/WANs 1.3.1Computer Security Act

The Computer Security Act of 1987, P.L. 100-235, dated January 8, 1988, requires Federal agencies to:

- identify all computer systems that process sensitive data and prepare a plan for the security and privac

- provide mandatory periodic training in computer security awareness and accepted security practices for Federal computer systems within or under the supervision of that agency.

1.3.2 Regulatory Requirements

The Office of Management and Budget (OMB) is chartered to enforce provisions of the Act, and is the principal regulatory documents for security include: OMB Circular No. A-130, Appendix III, (Security of Federal Automa Systems). OMB Bulletins provide detailed security guidance (e.g., OMB Bulletin 90-08, dated July 9, 1990).

The Computer Security Act of 1987 assigned the National Institute of Standards and Technology (NIST) the resp Federal unclassified systems, including LANs/WANs. Appendix B lists NIST publications applicable to LAN/W

The Office of Personnel Management (OPM) provides guidance for designating sensitive positions and screening the incumbents. The General Services Administration (GSA) issues its guidance in the Federal Inform for OMB, NIST,
OPM, GSA, DHHS and other references applicable to LANs, and refer to the Department's AISSP Handbook for

1.3.3 Departmental Security Policy

LANs/WANs come under the purview of the Departmental security policy:

DHHS will implement a Department-wide AIS security program to assure that each automated informatio magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the informat contained in the system. Each system's level of security must protect the confidentiality, integrity, and availabil

a. each AIS have the appropriate technical, personnel, administrative, environmental, and telecommunica

b. AIS security should be cost-effective; and

c. an AIS that supports critical OPDIV [Operating Division] functions has a contingency or disaster recovery plan to provide continuity of operation.

Each OPDIV shall administer an AIS security program that meets statutory, regulatory, and Departmental

1.4 RISK MANAGEMENT OVERVIEW

Risk management, as defined in the DHHS Automated Information Systems Security Program (AISSP) Handbook, is a process for minimizing losses through the periodic assessment of potential hazards and the syster

Risk to information systems is generally expressed in terms of the potential for loss. The greater the value of th disgruntled employees, error-prone programmers, careless operators), things (e.g., unreliable hardware) or even

Nature itself (e.g., earthquakes, floods, lightning). Vulnerabilities are flaws in the protection of assets that can b
mitigate vulnerabilities.

"Managing risks means not only identifying threats but also determining their impact and severity. Some threat
and other computer crimes, have been highlighted through extensive press coverage. On the other hand, repeate
that errors and omissions generally cause more harm than virus attacks. Resources are often expended on threat
worth controlling, while other major threats receive little or no control. Until managers understand the magnitu
protecting vital computer resources will continue to be an arbitrary and ineffective proposition."

2. LAN/WAN ENVIRONMENT

This section provides a brief overview of the highly complex LAN/WAN environment to serve as a foundation fo
uses a mix of personal computers (PCs), LANs/WANs, terminals, minicomputers, and mainframes to meet its pro
many varieties and provide connectivity - directly or indirectly - to many of the Department's mini and mainfram

A LAN is a group of computers and other devices dispersed over a relatively limited area and connected by a com
network. LANs commonly include microcomputers and shared (often expensive) resources such as laser printer
a department or office building, for example), separate LANs can be connected to form larger networks. Altern
configured utilizing a client-server architecture which makes use of "distributed intelligence" by splitting the pro
"back-end" server. The client component, itself a complete, stand-alone personal computer, offers the user its fu
which can be another
personal computer, minicomputer, or mainframe, enhances the client by providing the traditional strengths offere
management, information sharing among clients, and sophisticated network administration and security features.

2.1 LAN/WAN COMPONENTS

PCs are an integral part of the LAN, using an adapter board, cabling, and software to access the data and devices
telephone line. The PC is the most vulnerable component of a LAN since a PC typically has weak security featur
Section 3.4, "Vulnerabilities."

LAN cabling provides the physical connections using twisted-pair cable, thin coaxial cable, standard
coaxial cable, or optical fiber (which provides the most security, as well as the highest capacity). Cabling is sus
due to the high cost of such action. A new alternative to cabling is a wireless LAN, which uses infrared light wa
radio, are vulnerable
to unauthorized interception.

Servers are dedicated computers, mostly PCs, that provide various support and resources to client workstations, i
small peer-to-peer LANs, the server can function as one of the client PCs. In addition, minicomputers and main
with PCs
that serve as "dumb terminals" to access minis and mainframes. Controlling access to the server is a basic LAN

A network operating system is installed on a LAN server to coordinate the activities of providing services to the
operating system, which performs the basic tasks required to keep one computer running, a network operating sy
managing such details as
network access and communications, resource allocation and sharing, data protection, and error control. The netw
Section 2.8, Access Control Mechanisms, for a discussion of these security features.

Input/output devices (e.g., printers, scanners, faxes) are shared resources available to LAN users and are suscepti
printer).

A Backbone LAN interconnects the small LAN work groups. For example, DHHS/Office of the Secretary (OS) uses copper and fiber optic cabling for their backbone circuits. Fiber optics provides a high degr

Internetworking devices include repeaters, bridges, routers, and gateways. These are communications devices f efficient and reliable internetwork access. These "traffic cops" can also have security control features for regulating access.

2.2 DIAL-IN ACCESS

A PC that is not physically connected by cables to a LAN may be permitted dial-in access via a modem and telephone line.

A PC dial-in connection can be made directly to a LAN server. This connection can occur when a server has be communications software, a modem/telephone line, and the LAN dial-in number to complete the connection. T logon/password requirements. LANs usually have specific controls for remote dial-in procedures. The remote

A PC can remotely control a second PC via modems and software such as pcAnywhere or Carbon Copy. When t first PC through the second PC into the LAN. The result is access to the LAN within the limits of the user's access controls. Or computer to dial in to his/her office PC and then remotely controls the office PC to access the LAN. (The office the LAN may not have the capability to detect that a remote control session is taking place.

Dial-in capabilities increase the risk of unauthorized access to the system, thereby requiring strong password pro Section 3.4.3.

2.3 TOPOLOGY

The topology of a network is the way in which the PCs on the network are physically interconnected. Network d combination of these. The name of the topology describes its physical layout.

In a star configuration, PCs communicate through a central hub device. Regarded as the first form of local area central or shared hub resource.

In a ring network, messages circulate the loop, passing from PC to PC in bucket-brigade fashion. IBM's Token- Only one token exists on the network at any one time, and the station owning the token is granted the right to co keeps one user from monopolizing the token indefinitely. When the token owner's work is completed or the tok

PCs on a bus network send data to a head-end retransmitter that rebroadcasts the data back to the PCs.

LAN topology has security implications. For example, in sending a sensitive data message from one user to an and bus topologies, the message is routed past other users.

2.4 PROTOCOLS

A protocol is a formal set of rules that computers use to control the flow of messages between them. Networking Organization (ISO) defined the now-popular seven layer communications model. The Open Systems Interconn (OSI) model describes communication processes as a hierarchy of layers, each dependent on the layer beneath it. interface is made flexible so that designers can implement various communications protocols - with security feat as depicted in Figure 2-1, OSI Model:

- The application layer is the highest level. It interfaces with users, gets information from databases, and transfers whole files. (E-mail is an application at this level.)

- The presentation layer defines how applications can enter the network.

- The session layer makes the initial contact with other computers and sets up the lines of communication devices to be referenced by name rather than by network address.)

- The transport layer defines how to address the physical locations/devices on the network, make connections between nodes, and handle the internetworking of

- The network layer defines how the small packets of data are routed and relayed between end systems or on interconnected networks.

- The data-link layer defines the protocol that computers must follow to access the network for transmitti layer and the physical layer, defined below.)

- The physical layer defines the physical connection between the computer and the network, and converts (Topology is defined here.)

Bridges, routers, and gateways are "black boxes" that permit the use of different topologies and protocols within layer protocol, can be connected with a simple, low-cost repeater. Two LANs that speak the same data-link laye If the LANs have a common network layer protocol, they can be connected with a router. If two LANs have no with a gateway.

These "black boxes" have features and "filters" that can enhance network security under certain conditions, but t elect to permit electronic mail (e-mail) to pass bidirectionally by putting in place a mail gateway while preventin e-mail)."

FIPS PUB 146-1, Government Open Systems Interconnection Profile (GOSIP), specifies a set of OSI protocols f agencies. "GOSIP does not mandate that government agencies abandon their favorite computer networking products. GOSIP does mandate that government agencies, when acquiring computer networking products, purchase OSI capabilities in addition to any other requirements, so that multi-vendor interoperability b life in conducting government business."

FIPS PUB 146-1, Chapter 6 (Security Options) and Appendix 1 (Security) discuss the security options in GOSIP

- Security is of fundamental importance to the acceptance and use of open systems. Part 2 of the Opens international standard (IS 7498/2). The standard describes a general architecture for security in OSI, and outlines a number of mechanisms that can be used in providing the services. However, no protoco

- An organization desiring security in a product that is being purchased in accordance with this profile mu the OSI architecture, the mechanisms to provide the services, and the management features required.

- Security is an option in GOSIP. As such, security services of the layers 2,3,4,6, and 7. The primary security services that are defined in the OSI security architect

-Data confidentially services protect against unauthorized disclosure.
-Data integrity services protect against unauthorized mod
deletion.
-Authentication services verify the identity of communica
source of data.
-Access control services allow only authorized communication and system access. -Non-repudiati
and protects against any attempt by the originator to falsely deny sending the data or its contents

2.5 APPLICATIONS/E-MAIL

Applications on a LAN can range from word processing (e.g., WordPerfect) to database management systems (e.

E-mail software provides a user interface to help construct the mail message and an "invisible" engine to move th
routed across the office via the LAN or across the country via LAN/WAN bridges and gateways. E-mail may al
cc:Mail, which is in use at SSA. Text or
binary files can be attached to e-mail. An important security note is that, on some systems, it is also possible to
instance).

Many application systems have their own set of security features, in addition to the protection provided by the ne
comprehensive security controls to limit access to authorized users.

2.6 The WAN

A natural extension of the LAN is the wide area network (WAN). A WAN connects remote LANs and
ties remote computers together over long distances. The WAN provides the same functionality as the individual
move throughout the organization-wide internet. WANs are, by default, heterogeneous networks that consist of
popular internetworking devices for WANs are bridges and routers. Hybrid units called brouters, which provide
bridge or route depends on protocols, network topology, and security requirements. Internetworking schemes o

The DHHS Departmental Information Management Exchange System (DIMES) is the wide area network
for the Department, operated on a fee-for-service basis by the Public Health Service's Parklawn Computer Cente
hub. The PCC
uses the FTS 2000 Digital Transmission Service for its backbone communications.

DIMES has evolved over the past decade to support a variety of networking capabilities for organizations within
government and private sector networks, and e-mail backbone capabilities. Network management and security

Figure 2-2, below, illustrates a basic LAN/WAN, connecting a Banyan LAN to the Parklawn Computer Center vi
routing functions
for the LAN under the direction of the network operating system. No bridges are used in this configuration. W
Group LAN rings when required by distance factors.

2.7 NETWORK MANAGEMENT

The overall management of a LAN/WAN is highly technical. The International Standards Organization's (ISO)
five subsystems: Fault Management, Performance Management, Configuration Management, Accounting Manag
Security Management. Security management includes controlling access to network resources.

Network management products, such as monitors, network analyzers, and integrated management

systems, provide various network status and event history data. These and similar products are designed for tro
information, patterns, and trends for security purposes.

For example, a typical LAN analyzer can help the technical staff troubleshoot LAN "bugs" (usually decoding all
network protocols, capture data packets for analysis (but usually does not decode data), and assist with LAN exp
identification code of someone making excessive logon errors (which might not be the owner), it may require a n
analyzer to determine the exact identity of the PC on which the logon errors are occurring. As passive monitori
server-software security. Therefore, analyzer operators should be appropriately screened.

2.8 ACCESS CONTROL MECHANISMS

Network operating systems have access control mechanisms that are crucial for LAN/WAN security. For example, access controls can limit who can logon, what resources will be available, what each user can do with t
security, and key user personnel should cooperate closely to implement access controls. The Banyan Vines (4.X
and Network Security, are highlighted
below to illustrate the range of security that a LAN can provide. Similar functions are provided by other produc

User Security. User access controls determine how, when, and where LAN users will gain access to the system. Setting up user security profiles includes the following tasks:

- oSpecify group security settings
- oSpecify settings for specific users
- oManage password security - length, expiration, etc. oPrevent user changes to settings
- oSpecify logon settings
- oSpecify logon times
- oSpecify logout settings
- oSpecify, modify, and delete logon locations (workstation, server, and link)
- oDelete a user's security
- oSpecify user dial-in access lists for servers

Network File Access. File security is determined by the level of security that is imposed on the directory "password protection" or other security mechanisms allowed by the specific application software.) Each StreetTalk names (users) and access levels. There are four levels of access:

- oControl - the user can assign access rights on directories and subdirectories; create, modify, read
- oModify - the user can create, modify, read, and delete files and subdirectories.
- oRead - the user can read and copy (and execute) any file within a directory.
- oNull - prevents user access to a particular directory. This access right is for protecting sensitive by name or indirectly by group or list membership, has null access - which can be changed by system administrators, i.e., control access.)

Console Security. The console security/selection function allows the system administrator to prevent un the system administrator to assign a console password, lock and unlock the console, and change the conso

Network Security. These controls determine how outside users and servers can access the resources in th Network security tasks include:

- oSpecifying user dial-up access

oSpecifying internetwork access

2.9 THE FUTURE OF LANs/WANs

The future direction of DHHS computing is increased information sharing across the Department. A host of tec computers connected to large bandwidth circuits to move huge amounts of information, open systems architectu systems, and desk-top multi-media capabilities, to name just a few.

The center of these evolving technologies is the LAN/WAN. Departmental networks will continue to grow rapidly, becoming the lifeline of Departmental activity. The goal is to provide transparent access to Departm increase commensurately. The key is to balance information sharing with information security. The information systems security officers (ISSOs) for the LAN environment of tomorrow will, by necessity, require a

3. RISK ASSESSMENTS

3.1 RISK ASSESSMENT METHODOLOGY

A risk analysis is a formalized exercise that includes:

- Identification, classification, and valuation of assets; o
- Postulation and estimation of potential threats;
- Identification of vulnerabilities to threats; and
- Evaluation of the probable effectiveness of existing safeguards and the benefits of additional safeguards.

3.2 LAN SENSITIVITY AND ASSET VALUE

3.2.1 Protection Needed

The purpose of this section is to determine the type and relative importance of protection needed for the LAN. Based on OMB guidance, a LAN system and its applications may need protection (e.g., administrative, physical, and technical safeguards) for one or more of the following reasons:

Confidentiality. The system contains information that requires protection from unauthorized disclosure. Examples: the need for timed dissemination, as with the DHHS Budget, personal data covered by the Privacy Act, and proprietary business information.
Integrity. The system contains information that must be protected from unauthorized,

unanticipated, or unintentional modification, including the detection of such activities. Examples: systems critical to safety or life support and financial transaction systems.

Availability. The system contains information or provides services that must be available on a timely basis to meet mission requirements or to avoid substantial losses. (One way to estimate criticality of a system is in terms of downtime. If a system can be down for an extended period at any given time, without adverse impact, it is likely that it is not within the scope of the availability criteria.)
For each of the three categories (confidentiality, integrity, and availability), it is necessary to determine if the protection requirement is:

- High - a critical concern of the organization.
- Medium - an important concern, but not necessarily paramount in the organization's priorities.
- Low - some minimal level of security is required, but not to the same degree as the previous two categories.

Refer to the DHHS AISSP Handbook, Chapter II, Security Level Designations, for more detail concerning sensitive security levels.

3.2.2 Asset Values

A valuation process is needed to establish the "risk" or potential for loss in terms of dollars. The greater the valu
security. Asset values are useful indicators for evaluating appropriate safeguards for cost-effectiveness, as require
intangible value of information systems. The cost of re-creating the data or information could be more than the
important data, or the denial of services at a crucial time could result in substantial "costs" that are not measurabl
premature or partial information relating to investigations, budgets, or contracts could be highly embarrassing to

Asset valuation should include all computing-associated tangible assets, including computer hardware, special eq
since
backup copies should be available.

The starting point for asset valuation is the LAN inventory. A composite summary of inventory items, acquisitio
provide a reasonable
basis for estimating cost-effectiveness for safeguards. It should be noted that if a catastrophic loss were to occu
exact model equivalents. Instead, newer substitute items currently available would probably be chosen, due to t

3.3 THREATS TO LAN SECURITY

A threat is an identifiable risk that has some probability of occurring.

A useful framework for introducing the discussion of threats is depicted in Figure 3-1, Security Threats. People t
who make errors and omissions, and employees who are disgruntled or dishonest.

People threats are costly. Employee errors, accidents, and omissions cause some 50 to 60 percent of the annual
percent. These insider threats are estimated to account for over 75 percent of the annual dollar loss experienced
5 percent. Physical threats, mainly fire and water damage, add
another 20 percent. It should be noted that these figures were published in 1988, and since that time
there has been a dramatic increase in virus incidents, which may significantly enlarge the dollar loss
from outsider threats, particularly in the LAN environment.

In this paper, threats are grouped in three broad areas: People threats, virus threats, and physical
threats. LANs are particularly
susceptible to people and virus related threats because of the large number of people who have access
rights.

3.3.1 People Threats

People threats include the following:

System Administration Error: all human
errors occurring in the setup, administration, and operation of LAN systems, ranging from the failure to properly
backups. The
possible consequences include loss of data confidentiality, integrity, and system availability, as well as possible e

PC Operator Error: all human errors occurring in the operation of PC/LAN systems, including
improper use of logon/passwords, inadvertent deletion of files, and inadequate backups. Possible consequences
erasure of critical programs or data).

Software/Programming Error: all the "bugs," incompatibility issues, and related problems that occur in developing, installing, and maintaining software on a LAN. Possible consequences include degradation, inte

Unauthorized Disclosure: any release of sensitive information on the LAN that is not sanctioned by proper autho consequences are violations of law and policy, abridgement of rights of individuals, embarrassment to individual

Unauthorized Use: employment of government resources for purposes not authorized by the Agency and the use of non-government resources on the network (such as using personally-owned software at the office). P violations for use of unlicensed software. (See DHHS AISSP Handbook for policy guidance).

Fraud/Embezzlement: the unlawful deletion of government recorded assets through the deceitful manipulation o consequences include monetary loss and wrongful contract/grant awards.

Modification of Data: any unauthorized changing of data, which can be motivated by such things as personal gai Possible consequences include the loss of data integrity and potentially flawed decision making. A high risk is t

Alteration of Software: any unauthorized changing of software, which can be motivated by such things as disgru include all kinds of processing errors and loss of quality in output products.

Theft of ADP Assets: the unauthorized/unlawful removal of data, hardware, or software from government facilities. Possible consequences for the loss of hardware can include the loss of important data and vicinity.

3.3.2 Viruses and Related Threats

"Computer viruses are the most widely recognized example of a class of programs written to cause some form of computer virus performs two basic functions: it copies itself to other programs, thereby infecting them, and it exe instructions the author included in it. Depending on the author's motives, a program infected with a virus may c occurred, such as a particular time or date. The damage can vary widely, and can be so extensive as to require t rapidly to other programs and systems, the damage can multiply geometrically."

"Related threats include other forms of destructive programs such as Trojan horses and network worms. Collecti masquerade as useful programs, so that users are induced into copying them and sharing them with their friends. [frequently] authored and [often] initially spread by individuals who use systems in an unauthorized manner. Th addressed as a part of virus prevention."14

3.3.3 Physical Threats

Electrical power problems are the most frequent physical threat to LANs, but fire or water damage is the most se

Electrical Power Failures/Disturbances: any break or disturbance in LAN power continuity that is sufficient to ca Possible consequences range from minor loss of input data to temporary shutdown of systems.

Hardware Failure: any failure of LAN components (particularly disk crashes in PCs). Possible consequences include loss of data or data integrity, loss of processing time, and interruption of services; may also

Fire/Water Damage: the major catastrophic destruction of the entire building, partial destruction within a zone, LAN room fire, water damage from sprinkler system, and/or smoke damage. The possible consequences include loss of the entire system for extended periods of time.

Other Physical Threats: Environmental failures/mishaps involving air conditioning, humidity, heating, liquid le
riot/civil disorders, bomb threats, and vandalism. Natural disasters include flood, earthquake, hurricane, snow/i

3.4 VULNERABILITIES

Vulnerabilities are flaws in the protection of LANs/WANs that can be exploited, partially or fully, by threats resu
vulnerabilities are specific weaknesses in a given LAN environment. Vulnerabilities are precluded by safeguard
a comprehensive list of LAN safeguards is discussed in Section 3.5, "Safeguards." Of paramount
importance is the most basic safeguard: proper security awareness and training.

A LAN exists to provide designated users with shared access to hardware, software, and data. Unfortunately, the
include the PC, passwords, LAN server, and internetworking.

3.4.1 PC

The PC is so vulnerable that user awareness and training are of paramount importance to assure even a minimum

Access Control. Considerable progress has been made in security management and technology for large-
scale centralized data processing environments, but relatively little attention has been given to the protection of s
mechanisms that would provide users with security-related systems functions. Without such hardware features
memory protection), it is virtually impossible to prevent user programs from accessing or modifying parts of the

PC Floppy Disk Drive. The floppy disk drive is a major asset of PC workstations, given its virtually unlimited s
However, the disk drive also provides ample opportunity for sensitive government data to be stolen on floppy dis
points. This problem is severe in certain sensitive data environments, and the computer industry has responded
advantage of diskless PCs is that they solve certain security problems, such as the introduction of unauthorized s
disadvantage is that the PC workstation becomes a limited, network-dependent unit, not unlike the old "dumb" m

Hard Disk. Most PCs have internal hard disks ranging from 10 to 160 or more megabytes of on-line storage cap
modification, or destruction. Even if PC access and LAN access are both password protected, some PCs may be
from a floppy disk that bypasses the password, permitting access to unprotected programs and files on the hard d
provide increasing degrees of security for data on hard disk drives, ranging from password protection for enterin

"Erasing" hard disks is another problem area. An "erase" or "delete" command does not actually delete
a file from the hard disk. It only alters the disk directory or address codes so that it appears as if deletion or eras
"erased" when DOS eventually writes new files over the old "deleted" files. This may take some time, dependi
on the available space on the hard disk. In the meantime, various file recovery programs can be used
to magically restore the "deleted" file. There are special programs that really do erase a file and these should be
have a copy of the sensitive file, and a user may or may not have erase privileges for the server files.

Repairs. Proper attention must be given to the repair and disposition of equipment. Commercial repair staff sh
on sensitive PC/LAN equipment. Excess or surplus hard disks should be properly erased prior to releasing the e

3.4.2 The PC Virus

PCs are especially vulnerable to viruses and related malicious software (e.g., Trojan horse, logic bomb, worm).
things in memory
or on disk. For example, when DOS activates an application program on a PC, it turns control over to the progr
access by application programs. There is no block between an application program and the direct usage of syste

etc.). Once the application program is running, it has complete access to everything in the system.

Virus-infected software may have to be abandoned and replaced with uninfected earlier versions. Thus, an effec
important, it is essential to determine the source of the virus and the system's vulnerability and institute appropria

A PC LAN is also highly vulnerable, because any PC can propagate an infected copy of a program to other PCs a

3.4.3 LAN Access

Access Control. A password system is the most basic and widely used method to control access to LANs/WAN
its services) for access to each major application on the LAN, and to other major systems interconnected to the L
LAN logon/password sequence. While passwords are the most common form of network protection, they are als
organizations have found that passwords have many weaknesses, including: poor selection of passwords by users
password guidance, no requirement to change passwords regularly),
and the recording of passwords in easily detected formats (on calendar pads, in DOS batch files, and even in logo
vulnerable to misuse.

Dial-in Access. Dial-in telephone access via modems provides a unique "window" to LANs, enabling anyone w
into the
system. Hackers are noted for their use of dial-in capabilities for access, using commonly available user IDs an
time limitations and locations, call back devices, port protectors, and strong LAN administration are ways to pro

UNIX. UNIX is a popular operating system that is often cited for its vulnerabilities, including its handling of "s
everything on
the system. NIST Interagency Report 4453 states that UNIX was not really designed with security in mind. "T
years, making security
even more difficult to control. Perhaps the most problematic features are those relating to networking: remote l
and electronic mail. All of these features have increased the utility and usability of UNIX by untold amounts. H
systems to the Internet
and other networks, have opened up many new areas of vulnerabilities to unauthorized abuse of the system."

3.4.4 Internetworking

Access Control. Internetworking is the connection of the local LAN server to other LAN/WAN servers via vari
e-mail system, for example, could not exist without this interconnectivity. Each additional LAN/WAN interconn
servers and network devices can function
as "filters" to control traffic to and from external networks. For example, application gateways may be used to e
balance connectivity requirements with security requirements.

Wireless LANs. Wireless LANs use infrared light waves or radio frequencies (RF) to transmit signals and data
wired and wireless capabilities. Increasingly, portable computers, laptops, and palmtops will have wireless conn
vulnerable to the
interception of data and passwords. Security planning, careful selection of security features (e.g., data encryptio

Organizational Teamwork. The effective administration of LANs/WANs requires inter-organizational coordinat
integrated security requires the combined efforts of many personnel, including the administrators and technical s
personnel, users, and management.

E-mail. E-mail messages are somewhat different from other computer applications in that they can involve "sto

recipient, often from one computer to another over a WAN. When messages are stored in one place and then fo
to multiple locations, they become vulnerable to interception or can carry viruses and related malicious software.

Figure 3-2 highlights LAN vulnerabilities.

3.5 SAFEGUARDS

Safeguards preclude or mitigate LAN vulnerabilities and threats, reducing the risk of loss. No set of safeguards
reduce risks
to a reasonable level, as determined by management. To make this guide as useful as possible, safeguards will b
plans. Most of these safeguards also apply to applications.

3.5.1 General Safeguards

Assignment of LAN Security Officer. The first safeguard in any LAN security program is to assign
the security responsibility to a specific, technically knowledgeable person. This person must then take the neces
the AISSP Handbook. Also, the Handbook requires that a responsible owner/security official be assigned to eac

Security Awareness and Training. Security training is mandated by the Computer Security Act of 1987. All Fed
acquisition, maintenance or operation of a LAN must be aware of their security responsibilities and trained in ho
Program (AIS-STOP) Guide for detailed guidance on security training programs.

Technical training is the foundation of security training. These two categories of training are so interrelated that
class. Proper technical training is considered to be perhaps the single most important safeguard in reducing huma

Personnel Screening. Personnel security policies and procedures should be in place and working as part of the p
designate sensitive positions and screen incumbents, following the guidance in DHHS Instruction 731-1, Personn
1988, for individuals involved in the management, operation, security, programming, or maintenance of the syste
abuse was often committed by authorized government/contractor users (not outsiders), and "it was also determin

The personnel screening process should also address LAN repair and maintenance activities, as well as janitorial

Separation of Duties. People within the organization (insider people threats) are the largest category of risk to t
fraud or abuse
difficult without collusion. For example, setting up the LAN security controls, auditing the controls, and manag

Preventive Maintenance. Hardware failure is an ever present threat, since LAN physical components
wear out and break down. Preventive maintenance identifies components nearing the point at which they could
affected.

Written Procedures. It is human nature for people to perform tasks differently and inconsistently, even if the sa
potential for an unauthorized action (accidental or intentional) to take place on a LAN. Written procedures help

Procedures should be tailored to specific LANs and addressed to the actual users, to include the "do's" and "don't
(e.g., password
content), handling of floppies, copyrights and license restrictions, remote access restrictions, input/output contro

3.5.2 Technical Safeguards

These are the hardware and software controls, as basically defined in OMB Bulletin 90-08, to protect the LAN fi
for LAN applications.

User Identification and Authentication. User identification and authentication (verification) controls
are used to verify the identity of a station, originator, or individual prior to allowing access to the system, or spec
name
by which the user is known to the system (e.g., a user identification code). This identifying name or number is
it is used to provide authorization/access and to hold individuals responsible for their subsequent actions.
Authentication is the process of "proving" that the individual is actually the person associated with the identifier.
accountability in a system. There are three basic authentication methods for establishing identity:

- o Something known by the individual: Passwords are presently the most commonly used method of controlling access to systems. Passwords are a combination of letters and numbers (or symbols), preferably six or more characters, that should be known only to the accessor. Passwords reusable, should provide for secrecy (e.g., non-print, non-display feature, encryption), and should limi conform to a set of rules established by management.

  In addition to the password weaknesses cited earlier in Section 3.4.3, passwords can be misused. For channel may also be able to "read" or identify a password and later impersonate the sender. Popular such abuses. Encryption authentication schemes can overcome such problems.

- o Something possessed by an individual: such as a magnetically encoded card (e.g., smart cards) or a ke with card devices to further enhance their security.

  Dial back is a combination method where users dial in and identify themselves in a prearranged metho predetermined number. There are also devices to determine, without the call back, that a remote devi

  Other security devices, at the point of logon and validatio include port-protection devices and random number generators.

  o Something about the individual: these include biometric physical attribute of a person (e.g., fingerprints, voiceprints, signatures, or retinal patterns) and transm major factor for these techniques.

  Authorization/Access Controls. These are hardware or software features used to detect and/or permit Authorization/access
controls include controls to restrict access to the operating system and programming resources, limits on access t
internetwork access.

In general, authorization/access controls are the means whereby management or users determine:

- o who will have
- o what modes of access to
- o which objects and resources

The who may include not only people and groups but also individual PCs and even modules within an applicatio
programs, servers, and internetwork devices. The objects that are candidates for authorization control include:

programs, etc.), input/output devices (printers, tape backups), transactions, control data within the applications, r
devices.

Integrity Controls. Integrity controls are used to protect the operating system, applications, and information in t
assurance
to users that data have not been altered (e.g., message authentication). Integrity starts with the identification of

- The foundations of integrity controls are the identification/authentication and authorization/access controls. These controls include careful selection of and adherence to vendor-supplied LAN administrative and security controls. Additionally, the use of software packages to automatically check for viruses is effective for integrity control.
- Data integrity includes two mechanisms that are at the heart of fraud and error control: the well-formed transaction and segregation of duties among employees. A well-formed
- transaction has a specific, constrained, and validated set of steps (and programs) for handling data with automatic logging of all data modifications so that actions can be audited later. The most basic segregation of duty rule is that a person creating or certifying a well-formed transaction may not be permitted to execute it.
- Two cryptographic techniques provide integrity controls for highly sensitive information:
    1. - Message Authentication Codes (MACs) are a type of cryptographic checksum that can protect against unauthorized data modification, both accidental and intentional. See FIPS PUB 113, Computer Data Authentication, May 20, 1985 and NBS Special Publication 500-156, Message Authentication Code (MAC) Validation System: Requirements and Procedures, May 1988.
    2. - Digital signatures authenticate the integrity of the data and the identity of the author. NIST is in the process of issuing a Digital Signature Standard that is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and sender authentication.

Audit Trail Mechanisms. Audit controls provide a system monitoring and recording capability to retain
or reconstruct a chronological record of system activities (e.g., system log files). These audits records help to establish accountability when something happens or is discovered. Audit controls should be implemented as part of a planned LAN security program. LANs have varying audit capabilities, which include:

- Exception logs record information relating to system anomalies such as unsuccessful password or logon attempts, unauthorized transaction attempts, PC/remote dial-in lockouts, and related matters. Exception logs should be reviewed and retained for specified periods.
- Event records identify transactions entering or exiting the system, and journal tapes are a backup of the daily activities.

Confidentiality Controls. These controls provide protection for data that must be held in confidence and protect
the user site, at a computer facility, in transit, or some combination of these (e.g., encryption).

- Confidentiality relies on the totality of LAN security (similar to integrity), and additional protection may include encryption.
- Encryption is a means of encoding (scrambling) data so that they are unreadable. When the data are received, the reverse scrambling takes place. The scrambling and descrambling requires an encryption capability at either end and a specific key, either hardware or software to code and decode the data. Encryption allows only authorized users to have access to applications and data. The NIST-sponsored Data Encryption Standard (DES) "is mandatory for all Federal agencies, including defense agencies, for the protection of sensitive unclassified information when the agency or department determines that cryptographic protection is required."
- The use of cryptography to protect user data from source to destination (end-to-end encryption) is a powerful tool for providing network security. This form of encryption is typically applied at the transport layer of the network (layer 4). End-to-end encryption cannot be employed (to maximum effectiveness) if application gateways are used along the path between communicating entities. These gateways must, by definition, be able to access protocols at the application layer (layer 7), above the

layer at which the encryption is employed. Hence the user data must be decrypted for processing at the application gateway and then re-encrypted for transmission to the destination (or another gateway). In such an event the encryption being performed is not really end-to-end.

- There are a variety of low-cost, commercial security/encryption products available that may provide adequate protection for unclassified use, some with little or no maintenance of keys. Many commercial software products have security features that may include encryption capabilities, but do not meet the NIST-required encryption standards. WordPerfect is an example of a product that automatically encrypts files when they are password protected (and the encrypted files can be stored on diskettes), but the encryption does not meet the requirements of the DES.

3.5.3 Operational Safeguards

Operation safeguards are the day-to-day procedures and mechanisms to protect LANs, as basically defined in OM

Backup and Contingency Planning. The goal of an effective backup strategy is to minimize the number of workdays that can be lost in the event of a disaster (e.g., disk crash, virus, fire). A backup strategy should inc

- the type/scope of backup: complete system backups, incremental system backups (changes), file/data backups, and even dual backup disks (disk "mirroring").
- the frequency of the backups: AM/PM, nightly, weekly, monthly.
- the time period for which the backup copies are kept: daily backups may be kept for a week, weekly backups may be kept for a month, monthly backups may be kept for a year.
-

Contingency/Disaster Recovery Planning consists of workable procedures for continuing to perform essential fu plans should be coordinated with the back-up and recovery plans of any installations and networks used by the a emergency, backup and contingency plans and procedures should be in place and tested regularly to assure the co users and coordinated with them.

Offsite storage of critical data, programs, and documentation is important. In the event of a major disaster such as fire, or even extensive water damage, backups at offsite storage facilities may be the only way to requirement for Level 2 and 3 (and 4) protection requirements.

Physical and Environmental Protection. These are controls used to protect against a wide variety of physical an hazards, and utility outages or breakdowns. Several areas come within the direct purview of the LAN/security s and possibly additional air conditioning. Surge protection and backup power will be discussed in more detail.

Surge suppressors that protect stand-alone equipment may actually cause damage to computers and other periphe (UPS) can
actually divert dangerous electrical surges into network data lines and damage equipment connected to that netw volt power systems, making them dangerous to delicate electronic components and data as they search for paths neutral and ground wires, where they are assumed to flow harmlessly to earth. The extract below summarizes th

> Computers interconnected by datalines present a whole new problem because network (and modem) datalines use the powerline ground circuit for signal voltage reference. When a conventional surge protector diverts a surge to ground, the surge directly enters the datalines through the ground reference. As [NIST's Francois] Martzloff explained in "Protecting Computer Systems Against Power Transients," this causes high surge voltages to appear across datalines between computers, and dangerous surge currents to flow in these datalines. Data Communications reported in December 1990 that "Most experts now agree that TVSSs (Transient Voltage Surge Suppressors) based on conventional diversion designs should not be used for networked equipment." LAN Times commented in May 1990 "Surge protectors may contribute to LAN crashes by diverting surge pulses to ground thereby contaminating the reference used by data cabling." This problem was first discovered by a team of NIST researchers led by Martzloff in 1988.

To avoid having the ground wire act as a "back door" entry for surges to harm a computer's low-voltage circuitry, network managers should consider power-line protection that:

- Provides low let-through voltage (under 250 volts peak is harmless).
- Does not use the safety ground as a surge sink and preserves it for its role as voltage reference.
- Attentuates the fast rise times of all surges, to avoid stray coupling into computer circuitry.
- Intercepts all surge frequencies, including internally generated high-frequency surges.

The use of an UPS for battery/backup power can make the difference between a "hard or soft crash." "Hard crashes" are the sudden loss of power and the concurrent loss of the system, including all data and work-in-progress in the servers' random-access-memory (RAM). An UPS provides immediate backup power to permit an orderly shutdown or "soft crash" of the LAN, thus saving the data and work-inprogress. The UPS protecting the server should include software to alert the entire network of an imminent shutdown, permitting users to save their data. LAN servers should be protected by UPSes, and UPS surge protectors should avoid the "back door" entry problems described above.

Production and Input/Output Controls. These are controls over the proper handling, processing, storage, and disposal of input and output data and media, including: locked storage of sensitive paper and electronic media, and proper disposal of materials (i.e., erasing/degaussing diskettes/tape and shredding sensitive paper material).

Audit and Variance Detection. These controls allow management to conduct an independent review of system records and activities in order to test for adequacy of system controls, and to detect and react to departures from established policies, rules, and procedures. Variance detection includes the use of system logs and audit trails to check for anomalies in the number of system accesses, types of accesses, or files accessed by users.

Hardware and System Software Maintenance Controls. These controls are used to monitor the installation of and updates to hardware and operating system and other system software to ensure that the software functions as expected and that an historical record is maintained of system changes. They may also be used to ensure that only authorized software is allowed on the system. These controls may include hardware and system software configuration policy that grants managerial approval to modifications, then documents the changes. They may also include virus protection products.

Documentation. These documentation controls are in the form of descriptions of the hardware, software, and policies, standards, and procedures related to LAN security, to include vendor manuals, LAN procedural guidance, and contingency plans for emergency situations. They may also include network diagrams to depict all interconnected LANs/WANs and the safeguards in effect on the network devices.

3.5.4 Virus Safeguards

Virus safeguards include good security practices cited above (e.g., backups, use of only agency approved softwa
prevention

and protection program, including the designation and training of a computer virus specialist (and backup). Eac

considered, as needed, such as:

- Use of anti-virus software to prevent, detect, and eradicate viruses
- Use of access controls to more carefully limit users
- Review of the security of other LANs before connecting
- Limiting of electronic mail to non-executable files
- Use of call-back systems for dial-in lines
-

Additionally, "Five common-sense tips for safer computing" are provided below:

- If the software allows it, apply write-protect tabs to all program disks before installing new software.

If it does not, write protect the disks immediately after installation.

- Do not install software without knowing where it has been.
- Make executable files read-only. It won't prevent virus infections, but it can help contain those that attack executable files (e.g., files that end in ".exe" or ".com"). Designating executable files as read-only is easier and more effective on a network, where system managers control read/write access to files.
- Abolish "SneakerNet." Boot sector viruses are especially pernicious. The most common virus, "Stoned," travels in the boot sector of floppy disks, which are passed from user to user and PC to PC. If an infected floppy disk is left in the A: drive and the user turns on the PC, the virus will spread to the hard disk as quickly as the "non-system disk" error appears onscreen. Transferring data files via networks, E-mail, or direct modem connections will minimize the possibility of spreading boot sector viruses.
- Back-up files. The only way to be sure the files will be around tomorrow is to back them up today.

3.6 METHOD OF ANALYSIS

3.6.1 Formal versus Informal

OMB Circular No. A-130 states that methodologies may range from informal reviews of small office automation security review can be used for systems with Level 1 security designations. Formal risk assessments are require Section 4 below for further discussion of levels of protection.

3.6.2 Automated Risk Assessment

There are a considerable number of automated risk assessment packages, of varying capabilities and costs, availa facilities, applications, office automation, and even LANs to some extent. Regrettably, there appears to be no au general analyses of
network vulnerabilities applicable in part to LANs, and many PC assessment protocols include questions relating adequate coverage of LAN administration, protection of file servers, and PC/LAN backup practices and procedu

3.6.3 Questionnaires and Checklists

The key to good security management is measurement - knowing where one is in relation to what needs to be do

Questionnaires are one way to gather relevant information from the user community. A PC/LAN
Questionnaire can be a simple, quick, and effective tool to support informal and formal risk assessments. For sm assessment tool. A checklist is another valuable tool for helping to evaluate the status of security. Section 4 di appendices.

A customized, DHHS version of an automated questionnaire and assessment package is being made
available to the Department. This PC-based product, MicroSecure Self Assessment from Boden
Associates, prompts the user to respond to a series of PC and LAN questions, which are tailored on-line to the us practices
and safeguards. Designed for the average PC user, the product functions as a risk assessment tool.

A questionnaire/checklist may be a useful first step in determining if a more formal/extensive risk assessment ne

4. LAN SECURITY IMPLEMENTATION

This section provides a step-by-step approach for implementing cost-effective LAN security.

4.1 DETERMINE/REVIEW RESPONSIBILITIES

The first step in LAN security implementation is to know who is responsible for doing what. LAN security is a
AISSP Handbook cites responsibilities for Departmental security, including:

- Managers of AIS Facilities and Information Technology Utilities (ITUs) (which include LAN/WANs)
- Managers of AISs and Application Systems (which run on LANs)

In addition to the AISSP Handbook requirements, every area network requires a LAN/WAN
Administrator and an Information Systems Security Officer (ISSO) whose specific duties include the implementa
security), and operational controls (e.g., backups and contingency planning). In general, the ISSO is responsib
including the Computer Systems

Security Plan. The LAN Administrator is responsible for the proper implementation and operation of security fe

4.2 DETERMINE WHAT PROTECTIONS ARE REQUIRED

The second step is to understand the type and relative importance of protection needed for a LAN. 4.2.1Protectio
As stated in Section 3, a LAN may need protection for reasons of confidentiality, integrity, and availability. For
level of security needed: High, Medium, or Low.

Rank the security objectives for the LAN being reviewed, using the following matrix:

Table 4-1: Security Objectives and Levels

Security Objectives	Level of Protection Needed
High (Level 3)	
Medium (Level 2)	
Low (Level 1)	
Confidentiality	
Integrity	
Availability	

The result is an overall security designation of low (Level 1), medium (Level 2), or high (Level 3). In all instan
highest security level designation of any data it processes or systems it runs.

This security level designation determines the minimum security safeguards required to protect sensitive data file refer to the DHHS AISSP Handbook, Chapter II, Security Level Designations for additional details.

4.2.2 DHHS Security Level Requirements

The following minimum security requirements have been extracted from the DHHS AISSP Handbook, Chapter III, Security Level Requirements:

Level 1 Requirements: The controls required to adequately safeguard a Level 1 system are considered good management practices. These include, but are not limited to:

a. AIS security awareness and training
b. Position sensitivity designations.
c. Physical access controls.
d. A complete set of AIS documentation.

Level 2 Requirements: The controls required to adequately safeguard a Level 2 system include all of the

a. A detailed risk management program (to be included in the AISSP).
b. Record retention procedures.
c. A list of authorized users.
d. Security review and certification procedures.
e. Clearance (i.e., appropriate background checks) for persons in sensitive positions, and for all contra
f. A detailed fire/catastrophe plan.
g. A formal written contingency plan. h. A formal risk analysis.
i. An automated audit trail.
j. Authorized access and control procedures. k. Secure physical transportation procedures. l. Secure telecommunications.
m. An emergency power program.

Level 3 Requirements: The controls required to adequately sa
all of the requirements for Levels 1 and 2, plus the following:

a. More secure data transfer, maybe including encryption.
b. Additional audit controls.
c. Additional fire prevention requirements.
d. Provision of waterproof covers for computer equipment.
e. Maintenance of a listing of critical-sensitive clearances.

There is also a set of Level 4 Requirements for classified information that comes under National Security policie DHHS LAN.

4.2.3 Sample Table of Mandatory/Optional Safeguards

The following table provides a quick (but not exhaustive) summary of mandatory and optional safeguards for Le Handbook, Exhibit
III-A: Matrix of Minimum Security Safeguards.

Table 4-2: Examples of Mandatory/Optional Safeguards

(Level 2 protection of LANs)
Safeguards

Mandatory

Optional

1.General Safeguards:

Security officer

X

Security training

X

Screen personnel

X

Risk analysis

X

2.Technical Safeguards:

Passwords/log-on

X

Limit log-on attempts

X

Access rights lists/profiles

X

Dial-back

X

Message authentication

X

Audit trail mechanisms

X

Encryption

X

3.Operational Safeguards:

Backups

X

Contingency plan

X

Offsite storage

X

Audit and variance detection

X

Maintenance controls

X

Physical/environmental controls

X

Handling/storage controls

X

Documentation

X

Virus prevention measures

X

4.2.4 Determine Detailed Security Protections

Table 4-2 is still general. Specific, detailed security protections must be determined, starting with who gets wha
users, must determine the detailed security protections. Procedures for maintaining these protections must be fo
departed personnel).

4.3 DEVELOP AN INTEGRATED SECURITY APPROACH

4.3.1 Role of the PC/LAN Questionnaire

Security programs require the gathering of a considerable amount of information from managers,
technical staff, and users. Interviews are one way, and these are often used with technical staff. Another way t
for reaching
a reasonable segment of the user community, quickly and efficiently. With minor updating, these surveys can be

We recommend using a PC/LAN questionnaire for Level 1 reviews and to support Level 2 and 3 risk assessment

assessment and can be a major element in a formal risk assessment. A PC/LAN questionnaire, for example, can

- Identify applications and general purpose systems.
- Identify sensitivity and criticality
- Determine specific additional security needs, relating to:
    1. -Security Training
    2. -Access controls
    3. -Backup and recovery requirements
    4. -Input/output controls
    5. -And many other aspects of security
    6.

Appendix C contains a sample PC/LAN questionnaire to illustrate this methodology. This questionnaire can be
experienced), asking them to take 15-20 minutes to fill out the form. The aggregated results of this questionnair
of PC computing practices within the LAN/WAN environment.

4.3.2 Role of the Computer System Security Plan

Develop a Computer Systems Security Plan (CSSP) for Level 2 and Level 3 LANs and WANs. CSSPs
are currently outlined in OMB Bulletin No. 90-08 and are an effective tool for organizing LAN security. The CS
CSSP is to be used
as the risk management plan for controlling all recurring requirements, including risk updates, personnel screeni
required for all Level 2 LANs and WANs.

See Appendix D, Sample Security Plan, for an example of a LAN Computer System Security Plan.

See Appendix F, LAN/WAN Security Plan Checklist, for a method to review security plans for
compliance with OMB guidance.

4.3.3 Risk Assessment

As required by the AISSP Handbook, risk assessments include: identification of informational and other

assets of the system; threats that could affect the confidentiality, integrity, or availability of the system; system vu
identification of protection requirements to control the risks; and selection of appropriate security measures.

Risk assessment for general purpose systems, including LANs/WANs, are required at least every five
years, or more often when there are major operational, software, hardware, or configuration changes. Section 3, "
See also appropriate NIST publications (e.g., FIPS PUB 65, Guideline for Automatic Data Processing Risk
Analysis).

4.3.4 The Contingency Plan

In view of the importance of contingency planning, Appendix E contains a sample Contingency Plan that can be
requirements of the DHHS AISSP Handbook, OMB Circular No. A-130, and FIPS PUB 87, Guidelines for ADP
Planning, March 1981. For additional guidance, see also: Information Technology Installation Security, Federal
1988.

4.3.5 An Annual Review & Training Session

An ideal approach would be to conduct a yearly LAN meeting where LAN management, security, and end-user p
meetings are an ideal way to satisfy both the security needs/updates of the system and the training/orientation ne
as simple as reviewing the CSSP,
item by item, for additions, changes, and deletions. General discussion on special security topics such as planne
agenda. A summary
of the meeting is useful for personnel who were unable to attend, for managers, and for updating the managemen

An often overlooked fact is that "LAN security" is only as good as the security being practiced. Information and
and monitored to ensure good security practices.

4.3.6 Update Management/Budget Plan

The management/budget plan is the mechanism for getting review and approval of security requirements in term
plan should be updated yearly to reflect the annual review findings.

APPENDIX A: DEFINITIONS

Accreditation. The authorization and approval, granted to an ADP system or network to process sensitive data i
designated technical personnel of the extent to which design and implementation of the system meet prespecified

Application System. An application system is a software package that processes, transmits, or disseminates info
is run at an automated information system facility. A word processor usually runs only one application system.

Automated Information System (AIS). An AIS is the organized collection, processing, transmission, and dissem

Automated Information System (AIS) Facility. An AIS facility is an organizationally defined set of personnel, h
operation of an automated information system(s) and an application system(s). AIS facilities range from large c
personal computers and word processors. 3

Certification. A technical evaluation made as part of and in support of the accreditation process, that establishes
implementation meet a prespecified set of security requirements. 1,2

Computer Security. Computer Security is the protection of a computer system against internal failures, human e
modification, destruction, or denial of service. 1,2

Computer System Security Plan (CSSP). This plan is a document describing the security and privacy requireme

Information Technology Utility (ITU). An ITU is an organizationally defined set of personnel,
hardware, software, and physical facilities, a primary function of which is to coordinate the operation of geograp
system facilities. ITUs range in size from wide area networks covering widely dispersed geographical areas to lo

Local Area Network (LAN). A data network, located on a user's premises, within a limited geographic region.
however, communication across the network boundary may be subject to some form of regulation. 6

Personnel Security. Personnel security refers to a program that determines the sensitivity of positions
and screens individuals who participate in the design, operation, or maintenance of automated information syste

Physical Security. Physical security refers to the combination of devices that bar, detect, monitor, restrict, or oth
measures to protect a facility that houses AIS assets and its contents from damage by accident, malicious intent,

Sensitive Information. Sensitive information is any information, the loss, misuse, disclosure, or unauthorized ac
conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, Unite
under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of nationa

Wide Area Network (WAN). A WAN is an arrangement of data transmission facilities that provides communica

---

1 FIPS Pub 102, Guideline for Computer Security Certification and Accreditation, September 1983.
2 DHHS IRM Circular # 10, "Automated Information Systems Security Program," September 30, 1991
3 DHHS Automated Information Systems Security Program Handbook, February 1, 1991
4 OMB Circular No. A-130, Management of Federal Information Resources, Appendix III, "Security of Federal Automated Information Systems," December 12, 1985.
5 OMB Bulletin No. 90-08, "Guidance for the Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information," July 9, 1990.
6 FIPS PUB 11-3, Dictionary for Information Systems, 1991 (ANSI X3.172-1990)
7 Computer Security Act of 1987, January 8, 1988, P.L. 100-235

APPENDIX B: REFERENCES

"Federal Legislation, Regulations, Standards, and Guidelines"