25X1 [redacted]

ICSR

NATIONAL FOREIGN INTELLIGENCE BOARD C011 17-SR
WASHINGTON, D C. 20505

25X1

NFIB 9.11/2
27 October 1988

MEMORANDUM FOR NATIONAL FOREIGN INTELLIGENCE BOARD PRINCIPALS

FROM: Executive Secretary

SUBJECT: Coordination of Threat to Intelligence Community Automated Information Systems and Networks, 1988-89 [redacted] 25X1

The above-cited document (attached) is forwarded at the direction of Deputy Director of Central Intelligence Gates for your coordination. Please provide any comments to [redacted] and certify your coordination to the Secretariat [redacted] by noon on 10 November 1988. If the Secretariat has not heard from you by that time, or received a request for more time for consideration, the Secretariat will take that you concur with the document as drafted. [redacted]

25X1 25X1 STAT

25X1 [redacted]

Attachment:
As Stated

25X1 [redacted]

25X1 [redacted]

~~SECRET~~

SUBJECT: Coordination of Threat to Intelligence Community Automated Information Systems and Networks, 1988-89 [redacted] 25X1

Distribution: NFIB 9.11/2

Copy 1 - DCI
2 - DDCI
3 - Executive Registry
4 - DDI
5 - DIRNSA
6 - D/DIA
7 - D/INR/State
8 - DoE
9 - FBI
10 - Treasury
11 - SAFSS
12 - Army DCSINT
13 - DNI
14 - Air Force ACSI
15 - USMC
16 - ES/NFIB
17 - NFIB Subject
18 - NFIB Chrono
19 - D/ICS - DD/ICS - DD/R&E/ICS
20 - ICS Registry

25X1 ES/NFIB/[redacted] (27 Oct 88)

25X1 [redacted]

THREAT TO INTELLIGENCE COMMUNITY AUTOMATED INFORMATION SYSTEMS AND NETWORKS 1988-1989

SENIOR EXECUTIVE PANEL MEMBERSHIP (Alphabetical Listing):

	Baker, Dr. Lara H.	Los Alamos National Laboratory
	Bayse, William A. Mr.	Federal Bureau of Investigation
	Bush, Mr. James O.	Planning Research Corporation
	Davis, Dr. Ruth M.	The Pymatuning Group, Inc., Chairman
	Deskin, Mr. George W.	Deskin Research Group
25X1	[redacted]	National Security Agency
		Intelligence Community Staff
	Lockwood, Mr. Earl F.	Betac Corporation
25X1	[redacted]	National Security Agency
		Central Intelligence Agency
		Defense Intelligence Agency

THREAT TO INTELLIGENCE COMMUNITY AUTOMATED INFORMATION SYSTEMS AND NETWORKS 1988-1989

DRAFTING GROUP MEMBERSHIP (Alphabetical Listing):

	Baker, Dr. Lara H.	Los Alamos National Laboratory
25X1	[redacted]	Central Intelligence Agency
		National Security Agency
		National Security Agency
		Defense Intelligence Agency
25X1	[redacted] Special Agent Paul D.	Federal Bureau of Investigation
	Hausman, Dr. Robert, Jr.	Los Alamos National Laboratory
25X1	[redacted]	Intelligence Community Staff
	McNulty, Mr. Lynn	Department of State
25X1	[redacted]	Central Intelligence Agency
	Schwalm, Mr. Roger	US Secret Service
25X1	[redacted]	Central Intelligence Agency

REGRADE AS CONFIDENTIAL WHEN
SEPARATED FROM ATTACHMENT

25X1 [redacted]

SECRET

25X1 [redacted]

DRAFT

THREAT TO INTELLIGENCE COMMUNITY AUTOMATED INFORMATION SYSTEMS AND NETWORKS 1988-1989

WARNING:

The contributing organizations view the contents of this document as extremely sensitive. A strict adherence to the need-to-know principle is required.

This document, in part or in its entirety, is not releasable to foreign nationals.

Fall 1988

25X1
25X1
[redacted]

[redacted]

SECRET

[redacted]

25X1 [redacted]

DCI'S THREAT TO AUTOMATED INFORMATION SYSTEMS (AIS)
AND NETWORKS 1988

SENIOR EXECUTIVE PANEL

25X1

Lara H Baker
Dr. Lara Baker
Drafting Group Liaison
Los Alamos National Laboratory

Will A. Bayse
Mr. William A. Bayse
Assistant Director
Technical Services Division
Federal Bureau of Investigation

25X1

James O. Bush
Mr. James O. Bush
Vice President, Planning
Emhart PRC

25X1

Ruth M. Davis
Dr. Ruth M. Davis, Panel Chairman
President
The Pymatuning Group, Inc.

25X1

George W Deskin
Mr. George W. Deskin
Chairman of the Board
Deskin Research Group

25X1

25X1 [redacted]
Director, National Computer
Security Center

[redacted]
ICS Liaison
Intelligence Community Staff

Mr. Earl F. Lockwood
President and CEO
Betac Corporation

[redacted]
Chief, National Information
Security Assessment Center
National Security Agency

[redacted]
Deputy Director for Physical and
Technical Security
Office of Security
Central Intelligence Agency

[redacted]
Deputy Director for Information
Systems
Defense Intelligence Agency

[redacted]

25X1 [redacted]

PREFACE [redacted] 25X1

The Threat to Intelligence Community Automated Information Systems and Networks 1988-1989 addresses the threat to intelligence information through computers and networks of computers. This document provides a comprehensive treatment of the computer-related threat to classified and unclassified intelligence information and it includes the basic thinking and judgments that guide the Intelligence Community in understanding the threat to its systems. [redacted] 25X1

25X1 25X1 25X1 The Senior Executive Panel would like to acknowledge the efforts the following individuals who contributed to this report: [redacted] of the Central Intelligence Agency (CIA), [redacted] [redacted] of the National Security Agency (NSA), [redacted] of the Defense Intelligence Agency (DIA), Special Agent Paul D. FitzGerald of the Federal Bureau of Investigation, Dr. Robert F. Hausman, Jr., of Los Alamos National Laboratory, Mr. Lynn McNulty of the Department of State, [redacted] [redacted] of CIA, Mr. Roger Schwalm of the US Secret Service, [redacted] [redacted] of CIA, and [redacted] of NSA. [redacted] 25X1 25X1 25X1 25X1

Government organizations and employees should consult the computer security element of their agencies for further information and guidance. Contractors and their employees should consult the appropriate contracting officers technical representative for further information. [redacted] 25X1

Next 86 Page(s) In Document Denied

APPENDIX A

GLOSSARY [redacted] 25X1

ACCREDITATION

Accreditation is the specific management authorization for operation of an AIS or network and is based on the certification process as well as on other management considerations. The accreditation statement affixes security responsibility with the accrediting authority and shows due care has been taken for security. By extension, it also covers AISs that are interconnected or that participate cooperatively in a network. [redacted] 25X1

The formal declaration by a designated authority that an AIS or network is approved to operate (a) in a particular security mode, (b) with a prescribed set of technical and nontechnical security safeguards, (c) against a defined threat, (d) in a given operational environment, (e) under a stated operational concept, (f) with stated interconnections to other AISs or networks, (g) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility. [redacted] 25X1

Systems processing intelligence will require a joint accreditation with an appropriate IC official when such systems are under the operational control of a US Government official not connected with the IC. [redacted] 25X1

AUTOMATIC DATA PROCESSING (ADP) SYSTEM

The assembly of computer hardware, firmware, and software used to categorize, sort, calculate, compute, summarize, store, retrieve, control, process, and/or protect data with a minimum of human intervention. [redacted] 25X1

ADP systems include, but are not limited to, process control computers, embedded computer systems that perform general purpose computing functions, supercomputers, personal computers, intelligent terminals, word processors, office automation systems, firmware, and other implementations of AIS technologies as may be developed; they also include application and operating system software. [redacted] 25X1

ASSOCIATED DATA COMMUNICATIONS

Associated data communications play many roles for an AIS and for connections among multiple AISs. The simplest is that of connecting geographically nearby users (direct users) and geographically remote users (indirect users) to a stand- alone AIS, and also interconnecting various components (e.g., multiple host computers) of the central AIS equipment. Such associated data communications will be considered in the accreditation of the AISs using the requirements in Section III. [redacted] 25X1

Associated data communications also facilitate the interconnection of multiple AISs as part of a separately accredited network. In effect, such a separately accredited network (including local area networks [LANs]) provides specialized common-carrier data communications to a limited subscriber community. It may be of limited geographic extent (a LAN), of metropolitan area size (tens of kilometers), or wide area (hundreds of kilometers, national, worldwide). Separately accredited networks must provide for network security in the form of access safeguards and controls. [redacted] 25X1

Unless they have already been accredited as part of a national telecommunications network, associated data communications, which handle intelligence in unencrypted form, must be included in the accreditation of the AIS or network to which they are attached. In this context, associated data communications include items such as protected wire distribution systems, concentrators, multiplexors, and network access devices. [redacted] 25X1

AUTOMATED INFORMATION SYSTEM (AIS)

An AIS is an assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information. An AIS will typically consist of automatic data processing (ADP) system hardware, operating system and applications software associated peripheral devices, and associated data. [redacted] 25X1

Examples include information storage and retrieval systems, personal computers (PCs) and workstations, office automation systems, and automated message processing systems (AMPS.) In addition, those supercomputers and process control systems (e.g., embedded computer systems) <u>that perform general-purpose computing functions</u> are included. [redacted] 25X1

AUTOMATED INFORMATION SYSTEM SECURITY

All security features needed to provide an acceptable level of protection for hardware; software; and classified, sensitive unclassified, or critical data, material, or processes in the system. It includes:

- All hardware and software functions, characteristics, and features.
- Operational procedures.
- Accountability procedures.
- Access controls at all computer facilities (including those housing mainframes, terminals, minicomputers, or microcomputers).
- Management constraints.
- Physical protection.
- Control of compromising emanations (TEMPEST).
- Personnel and communications security (COMSEC).
- Other security disciplines. [redacted] 25X1

BOUNDARY OF AN AIS

For the purpose of identifying the mode of operation of an AIS to be accredited, the AIS has a conceptual boundary that extends to all intended users of a system, both directly and indirectly connected, who receive output from the system without a manual security review by an appropriately cleared authority. The location of such a review is commonly referred to as "an air gap." The perimeter of the AIS, which encompasses all the components of the AIS to be accredited, excludes separately accredited networks to which the AIS is connected. [redacted] 25X1

BOUNDARY OF A NETWORK

For purposes of identifying the mode of a network to be separately accredited (including a local area network,) the boundary of a network extends to (but does not include) the AISs or other separately accredited networks that attach thereto. [redacted] 25X1

CERTIFICATION

The comprehensive evaluation of the technical and nontechnical security features of an AIS or network and other safeguards, made as part of and in support of the accreditation process, that establishes the extent to which a particular design and implementation meets a set of security requirements. [redacted] 25X1

COMMUNICATIONS SECURITY (COMSEC)

The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information. [redacted] 25X1

COMPUTER SECURITY (COMPUSEC)

The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized access, disclosure, acquisition, manipulation, modification, or loss of information contained in a system. [redacted] 25X1

DATA

1. A representation of facts, concepts, information, or instructions in a manner suitable for communication, interpretation, or processing by humans or by an AIS. [redacted] 25X1

2. Information with a specific physical representation. [redacted] 25X1

INFORMATION

Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape. [redacted] 25X1

INFORMATION SYSTEM

The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. [redacted] 25X1

INFORMATION SYSTEMS SECURITY

The protection afforded to information systems in order to preserve the availability, integrity, and confidentiality of the systems and information contained within the systems. Such protection is the application of the combination of all security disciplines that will, at a minimum, include COMSEC, TEMPEST, COMPUSEC, personnel security, industrial security, resource protection, and physical security. [redacted] 25X1

NETWORK

A network comprises communications media and all attached components whose responsibility is the transfer of information among a collection of AISs or workstations. Network components include packet switches, front-end computers, network and technical control devices. [redacted] 25X1

25X1 [redacted]

APPENDIX E

THREATS TO COMPUTER NETWORKS [redacted] 25X1

The threats to a network define the misuses of the system stemming from user, operator, and maintenance activities that are executed either purposefully or accidentally to exploit network vulnerabilities. Network threats and vulnerabilities are discussed below. [redacted] 25X1

THREATS [redacted] 25X1

Network threats can be summarized into several generic classes as follows:

- Leaks
- Adulteration
- Physical damage
- Denial of service
- Misuse of network connectivities (connectivity-related threats) [redacted] 25X1

The first class of threat, leaks, involves the compromise of sensitive information by delivering information into the hands of a person not authorized to receive it. The second, adulteration, involves injection of undesired material into a network to render information or network resources unusable for the intended purpose. The third, physical damage, involves accidental or deliberate physical damage resulting from accidents and improper operation, environmental phenomena, deterioration, or sabotage. The fourth, denial of service, involves deliberate degrading of network system performance or even making a network temporarily unusable through modification of components, overloading, or crashing of the network. It also includes intentional disruption of information exchange between network components. Finally, the threat of misuse of network connectivities involves deliberate or accidental misuse of information and network resources made possible by connections to remote terminals or processes. This class is actually basic to the previous four classes of threat to the extent that connections are involved in carrying them out. [redacted] 25X1

25X1 [redacted]

The general threat categories may be further broken down into specific threats or means of attack. The list of possible attacks arising from the various classes of threat include both single computer and network attacks. Attacks common to both include:

- Sabotage
- Spoofing
- Confusing
- Hacking
- Software implants
- Hardware implants
- Microcode implants [redacted] 25X1

Those attacks related primarily to networking and telecommunications include:

- Jamming
- Cryptanalysis
- Passive monitoring (interception of plain text, traffic analysis, compromising emanations)
- Tapping
- Unauthorized connections (transactions, sessions)
- Message diversion (misrouting)
- System spillage
- Changing address tables (message, session)
- Aborting network security controls
- Critical node failures
- Sabotage of remote facilities [redacted] 25X1

VULNERABILITIES [redacted] 25X1

Vulnerabilities offer the opportunity for threats to be executed. Threats can only be carried out because hardware, software, or procedural deficiencies, i.e., vulnerabilities, make unauthorized accesses to network components possible. These vulnerabilities represent an inability of the network to restrict user, operator, and maintainer accesses to only those components necessary to satisfy their needs and responsibilities. There are two basic categories of vulnerabilities:

- Vulnerabilities in the network hardware and software components that permit an attacker to successfully carry out a threat.

- Unpredictable hardware failures (including protection mechanisms) and human operational failures that permit attacks to be conducted. Such vulnerabilities are never completely eliminated but can be reduced by fault detection, isolation, and automatic error recovery. [redacted] 25X1

In the first category, the vulnerabilities in the network components are fundamentally the access paths to system components that facilitate their misuse. They stem from design and implementation errors introduced during

25X1 [redacted]

system development and make the network susceptible to attack. Design and implementation errors include both missing and inadequate protection mechanisms for preventing unauthorized access of system components. For example, a design error would be the failure to include a protection mechanism in a network for preventing unauthorized access. An implementation defect would be the misinterpretation of a design specification that led to an operational malfunction and failure defect, eventually resulting in unauthorized access and subsequent misuse of network resources. [redacted] 25X1

In the second category, hardware failures in protection mechanisms and related hardware elements are probably the most common. Access control mechanisms in the hardware can fail and support either accidental or deliberate attacks. Errors in communications devices may cause the misrouting of information and thereby support attacks. Thus, it is desirable to have fault detection, isolation, and automatic error recovery capabilities for components posing such vulnerabilities. [redacted] 25X1

While the threats may be identified and enumerated, the identification and characterization of the system penetration vulnerabilities that support successful attacks is a far more complex and difficult problem. [redacted] 25X1

CONNECTION VARIABLES [redacted] 25X1

Networks are inherently distributed, both functionally and geographically. They also range in complexity from the simplest networks in which two systems are connected with a pair of wires (i.e., a communications channel), to more complex connections involving message switches as well as communications channels, and finally to the situations whereby services are moved out of the network hosts and located in dedicated processors within the network. [redacted] 25X1

This distributed and complex nature of networks gives rise to many connectivity-related threats. Connectivity threats involve the misuse of network resources through network connections. A network connection may be defined in terms of the components, bandwidth, and services provided. Thus, a network connection between terminal-host, host-host, and terminal-terminal components, may accommodate a diverse array of data rates and data classifications/compartments (bandwidth), and provide numerous services such as virtual terminal, fine transfer, and electronic mail. [redacted] 25X1

When dealing with connectivity threats, it is useful to view the network as composed of a number of separate computer systems, interconnected by solely passive communications media. Threats relating to the passive communications media are considered to be outside the scope of this discussion; in particular the threats pertaining to hardware and software systems involved in providing end-to-end encryption. Also, if end-to-end encryption is used, all portions of the network protected by the encryption are treated as "passive communications media." [redacted] 25X1

Connectivity threats vary according to the characteristics described above, i. e., type of subscriber components connected to the network, the bandwidth involved, and the type of service provided by the network. For example, given several interconnected component hosts providing interprocess communications service, connections may vary considerably in terms of bandwidth and associated threats. Thus, connection A between two multilevel secure (MLS) systems, has a bandwidth that is both high volume and supports multiple classifications/compartments. Connection B is a low-volume, single classification and compartment connection between an MLS system and a dedicated mode system. Without the proper access controls, accountability and audit trails, Connection B with the dedicated system poses a much greater threat of information loss than Connection A. However, if adequate controls are present in both, Connection A, with its broad bandwidth, is under greater threat of attack because of the potentially greater loss of information. Specific examples are discussed below. [redacted] 25X1

25X1 Components. [redacted]

Network subscribers may include:

- Remote users
- Remote terminals
- Remote personal computers
- Remote networks
- User hosts
- User processes on a user host
- Switchable terminals
- Dial-up hosts
- Network nodes
- Gateways [redacted] 25X1

Generally, connections with remote networks, gateways, personal computers, and switchable terminals are under greater threat of attack because access here could initiate access in all the other networks/components to which they connect (cascade effect). [redacted] 25X1

25X1 Bandwidth. [redacted]

Bandwidth, as used in this report, refers to the level of connectivity with regard to data rate (bits per second) and data security level. Security level reflects both the classification level (Top Secret, Secret) and SCI access level (compartments), as well as the number of classifications/compartments involved. The bandwidth of a connection may involve any combination of these two factors: high-volume, multilevel, multicompartmented use; or low-volume, single-level, single-compartmented use, and so forth. Generally, the threat of attack increases with volume and security level. A one-way, low-volume connection between a remote terminal and dedicated host is less subject to attack than a high-volume conduit between network hosts carrying multiple classifications and compartments of information. [redacted] 25X1

Services. [redacted] 25X1

Many networks provide some or all of the following services:

- Virtual Terminal (Requires open/close connection)--In a virtual terminal connection a user already attached to the network connects to a host at some other point on the network. The user wishes to interact with the remote host in the same way as if he/she were attached directly to that host as a terminal.

- File Transfer--In a file transfer connection, a user wishes to transfer information, usually in files (real or virtual), between separate hosts.

- Electronic Mail--In mail, information is transferred between hosts, as in file transfer, but the user normally specifies a particular user or group of users on remote hosts without authenticating himself/herself on the remote hosts. The remote hosts have some mechanism for storing the mail until it is read by the users on the remote systems.

- Message Routing/Dissemination--Requires no open/close connections. [redacted] 25X1

When describing connectivity threat scenarios, it is important to identify the subscriber components, bandwidth, and types of service involved. [redacted] 25X1

UNDERLYING PROBLEMS [redacted] 25X1

Because network connections involve the union of communications and autonomous computers, certain technical problems and inconsistencies may occur from their interactions. These technical problems include:

- Inconsistency in the end-to-end use of naming parameters and conventions.

- Inability to reliably synchronize security state information end-to-end.

- Inconsistent security policy and protection mechanisms at various networked stations.

- Inadequate end-to-end error detection, isolation, and recovery mechanisms.

- Inconsistent auditing standards and tools for audit reduction.

- Independence of resource management strategies end-to-end [redacted] 25X1

These underlying technical problems give rise to the general connectivity threats addressed in subsequent paragraphs. [redacted] 25X1

CONNECTIVITY THREAT SCENARIOS [redacted] 25X1

Basic Problem: User-Level Connections [redacted] 25X1

The basic connectivity threat occurs at the user level when a user seeks access via a session or dial-up to a network resource. Unless a network has global control over users, information leaks may arise due to the large number of persons operating from different terminal stations at different sites with different authorizations for different resources, each of which has different classifications and compartments. [redacted] 25X1

For example, a user/process on host A wishes to communicate with processes/users on host B. The user logs into host A at clearance level x and establishes a virtual terminal connection to host B. If the user logs into B at a higher level than accredited for on A, then information may appear on the user's terminal that is at a higher level than the terminal is cleared for. If the user logs into B at a lower level, unless host A and/or the network can be trusted not to copy host A internal information (including files) to host B, there is a potential for unauthorized disclosure of information to B from host A. [redacted] 25X1

Normally, most user-level access to the network must be through the operating system of the host on which the user is working. Thus it appears that host B must decide at what level to allow the user to log-in. If B permits the user to log-in at a lower level, then host A could be compromised. If B permits the user to log-in at a higher level, then B could be compromised. B must only permit the log-in at the same clearance level as the user currently has at A. Otherwise, there is the potential of copying information from the user's higher level terminal to the lower level processes on B. A, on the other hand, must trust B to operate correctly. Such a security level mismatch may go unrecognized because it is conducted over cryptographically secured communications lines. [redacted] 25X1

Host Connections to Network [redacted] 25X1

Connectivity threats also occur at the network level when unauthorized hosts are allowed to connect to the network, in violation of a networkwide security policy (this aspect is discussed under the following heading, Propagation of Local Risk). OR, when authorized connections are established between host systems at many security levels, increasing the risk of information leaks due to inadequate access and authentication mechanisms. For example, hosts that are multilevel secure to the highest level sensitivity of information carried on the network could be connected directly to the network. Other network hosts must have some mechanism for protecting the network from the host, usually in the form of a network interface unit. [redacted] 25X1

Propagation of Local Risk [redacted] 25X1

Sometimes, an unevaluated host is connected to a trusted network; or operational needs of a system may lead to the accreditation of a system for multilevel operation that would not meet the requirements for the recommended class. This exposes all users of all other systems connected to the network to the additional risk. Misuse may occur if the connections are two-way, or if there is no manual review of transmissions. [redacted] 25X1

Nth Party Connectivities [redacted] 25X1

In a networking environment, in the case where a subscriber is a subnet or gateway host, the question of how far to extend the access controls becomes an issue. Nth party threats involve unauthorized access to information and misuse of network resources since one site may operate on behalf of another, which itself is operating on behalf of yet another, but in all cases for some ancestral user who initiated the request. This may result in several conditions that render the access and authentication mechanisms inadequate and increase the risk of unauthorized information disclosure:

- o The identification of the original requesting device/person may be needed but no longer available, jeopardizing the network security policy.
- o Information that should be carried at each stage of the chained requests is omitted, which also jeopardizes the network security policy. At a minimum, each stage should know of the previous stage; at a maximum, a trail of all previous stages should be carried. [redacted] 25X1

Cascade Threat [redacted] 25X1

The cascade problem exists when an unauthorized user can take advantage of network connections to compromise information across a range of security levels that is greater than the accreditation range of any one of the component systems that he must defeat to do so. [redacted] 25X1

For example, consider two hosts, A and B. Host A processes Secret and Top Secret information, and all users are cleared to at least Secret. Host B processes Confidential and Secret information, and all users are cleared to at least Confidential. While the risk of compromise in both hosts is small enough to justify their use with two levels of information, the system as a whole has three levels of information, increasing the potential harm that could be caused by compromise. When they are connected so that Secret data can pass from one to the other, an unauthorized user could defeat the access control to make Top Secret information available at the Confidential level. 25X1

[redacted]

Remote Diagnostics [redacted] 25X1

Vendor-supplied software is often maintained using a remote diagnostic capability. By its very nature, a diagnostic capability must bypass all access controls to allow the maintenance personnel access to data and software not normally available to users. When such a capability is remote the potential for information leaks is even greater. [redacted] 25X1

Incompatibilities [redacted] 25X1

Very-low-level details may have to be considered to make network connections safe and preserve the existing security properties of each. For example, suppose two identical multilevel hosts #1 and #2 process Unclassified through Top Secret data and have two compartments A and B. In System 1, bit 0, of the compartment field of the communications protocol represents compartment A and bit 1 represents compartment B, while in System 2 it is the other way around. Even though both systems are multilevel secure, when they are connected the data will not be protected unless the bit mapping is taken into account. [redacted] 25X1

Physical Damage/Denial of Service [redacted] 25X1

While these threats are generic classes in themselves, they relate to the distributed nature of networks and increase in importance as the network complexity increases. For example, remotely located connections may afford saboteurs the opportunity to vandalize a network with less chance of detection. If the vandalized resource is essential, such as a power supply, a network can be totally disabled. Or, if a network is functionally distributed, and perhaps draws on operational information collected automatically by remote sensors and relayed back, disruption of the vital connections initiates disruption in all the components that depend on it. The more complex the network and the more vital the interdependency of its components, the greater the threat of denial of service/operational failures related to connectivities. In fact, the easiest way to disable a network may be to disrupt some component or some other network upon which it depends. [redacted] 25X1

Management Complexity [redacted] 25X1

As data, functionality, and control become increasingly distributed, management becomes more complex. Loss of management control of data and resources may result. [redacted] 25X1