NCSC-TG-011
VERSION-1

NATIONAL COMPUTER SECURITY CENTER

TRUSTED NETWORK INTERPRETATION ENVIRONMENTS GUIDELINE

GUIDANCE FOR APPLYING THE TRUSTED NETWORK INTERPRETATION

1 August 1990

NCSC-TG-011
Library No. S-235,465
Version 1

FOREWORD

The National Computer Security Center is issuing the *Trusted Network Interpretation Environments Guideline* as part of our Technical Guidelines Program, through which the "Rainbow Series" is produced. The Technical Guidelines Program ensures that the features of the *Trusted Computer Systems Evaluation Criteria* (DOD 5200.28-STD) are discussed in detail and that guidance is provided for meeting each requirement. The National Computer Security Center, through its Trusted Product Evaluation Program, analyzes the security features of commercially produced and supported computer systems. Together, these programs ensure that organizations are capable of protecting their important data with trusted computer systems.

The *Trusted Network Interpretation Environments Guideline* is a companion to the *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria* (NCSC-TG-005), published 31 July 1987. The *Trusted Network Interpretation Environments Guideline* provides insight into the issues relevant when integrating, operating, and maintaining trusted computer networks. This document identifies the minimum security protection required in different network environments such that network certifiers, integrators, and accreditors can determine what protection mechanisms and assurances are minimally required in specific network environments.

This document parallels *Computer Security Requirements — Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments* (CDC-STD-003-85) and its technical rationale (CSC-STD-004-85). It also provides a descriptive presentation of the security issues that exist in networked computer systems as the networked computer system environment is inherently more complex and requires additional protection considerations over stand-alone computer systems.

As the Director, National Computer Security Center, I invite your suggestions for revising this document. We plan to review this document as the need arises.

PATRICK R. GALLAGHER, JR.
Director
National Computer Security Center

1 August 1990

ACKNOWLEDGMENTS

The National Computer Security Center extends special recognition and acknowledgment for their contributions to this document to Dr. Marshall D. Abrams, Renee Child, Annabelle Lee, Dr. Jonathan K. Millen, Samuel I. Schaen, and Dr. Martin W. Schwartz, of The MITRE Corporation, as authors; Richard Wilmer, also of The MITRE Corporation, as technical editor; and to Alfred Arsenault, David Chizmadia, and Rick Siebenaler of the National Computer Security Center, who managed the effort and participated in the development.

Special thanks are extended to the many members of the computer security community who enthusiastically gave their time and expertise in reviewing the material and providing valuable comments and suggested changes. Special thanks are extended to James P. Anderson of James P. Anderson Co., Donald L. Brinkley of Gemini Computers, Inc., Dr. Eric Roskos of The Institute for Defense Analysis, Dr. Tien Tao of Gemini Computers, Inc., and Dr. John M. Vasak of The MITRE Corporation for their extensive suggestions and recommendations.

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, DC 20402

TABLE OF CONTENTS

TABLE OF CONTENTS (Concluded)

LIST OF FIGURES

LIST OF TABLES

1 Introduction

This Trusted Network Interpretation (TNI) Environments Guideline (TNIEG) addresses many issues in determining the security protection required in different network environments. It complements the TNI, just as the Trusted Computer System Evaluation Criteria (TCSEC) Environments Guideline [1] complements the TCSEC. The TNI interprets the TCSEC for networks; it contains all of the criteria in the TCSEC, adding interpretation and rationale to applying trust technology to network systems. In the same way that the TCSEC Environments Guideline provides guidance on applying the TCSEC, this TNIEG provides guidance on the use of the TNI. The TCSEC and its Environments Guideline constitute the foundation on which the TNI and TNIEG add network applicability.

1.1 Background

The National Computer Security Center (NCSC) is responsible for establishing and maintaining technical standards and criteria for the evaluation of trusted computer systems. As part of this responsibility, the NCSC is developing guidance on how new security technology should be used. Two objectives of this guidance are:

- Establishing a metric for categorizing systems according to the security protection they provide, and
- Identifying the minimum security protection required in different environments.

The TCSEC [2] helps to satisfy the first objective by categorizing computer systems into hierarchical classes based on evaluation of their security features and assurances. The TCSEC Environments Guideline [1] helps to satisfy the second objective by identifying the minimum classes appropriate for systems in different risk environments. These two documents, however, apply to stand-alone computer systems.

The TNI [3] satisfies the first objective by interpreting the TCSEC for networks. The TNI also provides guidance for selecting and specifying other security services (e.g., communications integrity, denial of service, transmission security). The TNIEG is the first step toward addressing the second objective.

1.2 Trusted Network Technology Publications

The NCSC has decided to provide guidance concerning security in networks and distributed Automated Information Systems (AISs)[1] in a series of publications. The subject area is collectively identified as Trusted Network Technology (TNT). The TNI is the first TNT publication. This TNIEG is the second TNT publication. It contains the best guidance that is available at this time; as technology advances and more experience is gained in implementing trusted networks, more specific guidance will be provided. This TNIEG provides elaboration and clarification on the TNI. Guidance concerning Interconnected AIS which initially appeared in the TNI, Appendix C, has been revised and incorporated into this document (see Section 6 and Appendix A). This document does not address all of the security issues that are excluded from the TNI. Other topics, such as composing a trusted system from evaluated components, will be discussed in future TNT publications.

1.3 Purpose

The overall purpose of this TNIEG is to assist program managers, integrators, certifiers, and Accreditors with identifying the minimum security protection needed for different trusted computer network environments. For brevity, this audience is referred to as security managers. Not all questions can be answered at this time. The NCSC invites suggestions for topics to be addressed in future TNT publications.

This guideline is not a tutorial on security and networking; it is assumed that the reader will have some background in both areas. Suggested background references are identified in Appendix B. This guideline is designed to be self contained; a fair amount of background information that can be found in the TNI is also included here. The interested reader may consult the TNI and other documents referenced in this guideline for further detail.

1.4 Scope

This document describes an environmental assessment process that helps determine the minimum level of trust recommended for a specific network operational environment. The primary focus of this document (and also of the TNI) is on the AIS

[1]Definitions of terms particularly important to this document are given in Section 2.

hardware, firmware, and software aspects of security; therefore, neither this guideline nor the TNI address all the security requirements that may be imposed on a network. Depending on the particular environment, communications security (COMSEC), emanations security (TEMPEST), physical security, personnel security, administrative security, and other information security (INFOSEC) measures or safeguards are also required. This document applies to networks that are entrusted with the processing of information, regardless of whether that information is classified, sensitive, or otherwise relevant to national security.

1.5 Structure of the Document

Section 2 of this document defines terms and Section 3 discusses Network Security Architecture and Design. Section 4 guides security managers in applying Part I of the TNI; Section 5 does the same for Part II. Section 6 addresses security issues that arise when AIS are interconnected. Appendix A discusses the Cascade Condition in greater detail; Appendix B provides tutorial and background references on network security; and Appendix C discusses encryption and encryption mechanisms.

[This page intentionally left blank.]

2 Terminology

Many of the terms used in the TNI are drawn from diverse specialization areas. Their special meaning in context may differ from common English usage. In this section we explain how such terms are used in the TNI and how these definitions have been refined in this document. Terms are printed in boldface when they are defined.

2.1 Automated Information System

An **AIS** is defined in DODD 5200.28 as "an assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information" [4]. This is both a broad definition and a new one, since DODD 5200.28 was published after the TNI. The TNI states that "...automatic data processing (ADP) systems, referred to in this [TNI] document as Automated Information System (AIS)...", and equates AIS and ADP. We will use the DODD 5200.28 definition since it is broader and more authoritative. We also note that DODD 5200.28 tends to pluralize AIS as AISs while the TNI considers AIS to be a collective noun. We have followed the latter convention.

2.2 Network Trusted Computing Base

The **Network Trusted Computing Base** (NTCB) is the totality of protection mechanisms within a network system[2]—including hardware, firmware, and software—the combination of which is responsible for enforcing a security policy. The NTCB is the network generalization of the trusted computing base (TCB). An **NTCB Partition** is the totality of mechanisms within a single network subsystem[3] for enforcing the network policy, as allocated to that subsystem; it is the part of the NTCB within a single network subsystem.

---

[2]The distinction between a system and a subsystem is a matter of the viewpoint of the observer. One observer's system may be another observer's subsystem. For example, the vendor of a local area network may regard his product as a system, while the customer's network architect may consider it to be a subsystem along with hosts, workstations, etc.

[3]The TNI uses component in the definition of NTCB Partition. We use subsystem to be consistent in this document.

2.3 System and Component

The terms system and component need to be related to each other. Unfortunately, the TNI is not completely consistent in its use of these terms. We will first cite the relevant sections from the TNI; then we will reconcile them as used in this guideline. As discussed below, we define the relationship as follows: A component is a physical unit contained within a system.

2.3.1 TNI Introduction (definition not used in TNIEG)

The TNI Introduction states (emphasis added):

> A *network system* is the entire collection of hardware, firmware, and software necessary to provide a desired functionality. A *component* is any part of a system that, taken by itself, provides all or a portion of the total functionality required of a system. A *component* is recursively defined to be an individual unit, not useful to further subdivide, or a collection of components up to and including the entire system.

2.3.2 TNI - Appendix A (definition not used in TNIEG)

Appendix A of the TNI presents the view:

> ... a trusted network represents a composition of trusted *components*.... The approach to evaluation of a network suggested by this view is to partition the system into components, rate each component to determine its security-relevant characteristics, and then evaluate the composition of the components to arrive at an overall rating class for the network. This approach ... allows for the evaluation of components which in and of themselves do not support all the policies required by the TCSEC, ... contribute[s] to the overall evaluation of any network which uses them and allows for the reuse of the evaluated component in different networks without the need for a re-evaluation of the component.

Appendix A goes on to state that:

> The set of policy-related features to be supported by the component need not be the complete set required for a stand-alone system: features not supplied by one component for the system are supplied by another.

2.3.3 Discussion

We see a difference between the Introduction and Appendix A of the TNI. We will use the definition of component as an individual unit that *does not* provide a complete set of end-user services. As a consequence, a subsystem can operate on its

own and a component will require an external connection to perform a useful function. Appendix C of the TNI uses *component*, as follows, where we would use *subsystem*:

> Any AIS that is connected to other AIS must enforce an "Interconnection Rule" that limits the sensitivity levels of information that it may send or receive. Using the component connection view, each component responsible for maintaining the separation of multiple levels of information must decide locally whether or not information can be sent or received.

A *component* may support all the policy and accountability requirements: M, D, I, and A[4]; however, as defined above, this is not applicable to determining whether an individual unit is a component. A component which supports some part of the security policy contains an NTCB partition. In the extreme, a component may not have any security-relevant function; in this case it doesn't support any TCSEC policy and doesn't contain an NTCB partition.

2.3.4 Definitions

To summarize the previous discussions, following are definitions for component and system/subsystem.

- **Component**: An individual physical unit that does **not** provide a complete set of end-user services.
- **System/subsystem**: A collection of hardware, firmware, and software necessary configured to collect, create, communicate, compute, disseminate, process, store, and/or control data and information [4].

2.4 Evaluation

NCSC-evaluation refers specifically to the process in which the NCSC determines whether a commercial-off-the-shelf (COTS) product satisfies the TCSEC. Application of the TCSEC to a particular product may be assisted by an interpretation guideline such as the TNI [5]. In such a case, the guideline clarifies the meaning of the TCSEC's language with regard to a particular type of product, but in no case circumvents or grants exception to the requirements of the TCSEC. The purpose of an NCSC-evaluation is as follows:

[4]Mandatory access control, discretionary access control, identification and authentication, and audit, respectively.

> The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems. This goal is realized, in large measure, through the NCSC's Commercial Product Evaluation Program. This program is focused on the technical evaluation of the protection capabilities of off-the-shelf, commercially produced and supported systems that meet the computer security needs of government departments and agencies. This product evaluation culminates in the publication of an Evaluated Products List (EPL) report... [6].

An NCSC-evaluation places a product in one of four divisions: D, C, B, or A. Division D is for systems that have been evaluated but fail to meet the requirements for a higher NCSC-evaluation rating. Division C has two classes: C1 and C2, which require discretionary (need-to-know) protection. Division B has three classes: B1, B2, and B3, which require support for sensitivity labels and increasing robustness of system architecture. Division A has only class A1, which requires additional assurance through formal verification methods.

2.5 Certification

Certification is defined as "the technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular system's design and implementation meet a set of specified security requirements" [7]. In this definition, the word *evaluation* is used in the generic sense and should not be confused with NCSC-evaluation. The primary distinction is that certification is an evaluation with respect to specified requirements, and NCSC-evaluation is an evaluation against the TCSEC (and the TNI).

Certification is conducted in support of the accreditation decision. For most systems, the hardware, system software, applications software, communications equipment, and the operational facility must be configured and tested during certification. Certification should be performed by technical personnel independent of the development organization, according to an acceptable methodology. Certification should identify the level of security protection with regard to a procedure, program, or system. Certification results in the issuance of the Certification Statement, which states whether system security requirements are met, describes all known remaining vulnerabilities, and advises the Accreditor relative to the accreditation decision. If requirements are not met, the Certification Statement lists problem areas and identifies suggested solutions (if known). A certification documentation package, called the

Certification Report of Findings, submitted to the Accreditor includes the Certification Statement, certification analysis, results of Security Test and Evaluation, and results of Operational Test and Evaluation.

2.6 Accreditation

Accreditation is "the managerial authorization and approval granted to an ADP system or network to process sensitive data in an operational environment, made on the basis of a certification by designated technical personnel..." [3]. Accreditation is a management decision to operate a system or network employing specific safeguards, against a defined threat, at an acceptable level of risk, under a stated operational concept, with stated interconnections, in a specific operational environment, with a specific security mode of operation. Other terms have been used to identify the formal managerial approval for operation; in this document we use the term Accreditation. FIPS PUB 102 defines Accrediting Officials as "the agency officials who have authority to accept an application's security safeguards and issue an accreditation statement that records that decision. The Accrediting Officials must also possess authority to allocate resources to achieve acceptable security and to remedy security deficiencies" [7]. The ultimate responsibility for system security rests with the Accreditor. DODD 5200.28 employs the term Designated Approving Authority (DAA) to refer to the same officials or officers [4].

All AIS must be accredited before they may process or use sensitive or classified information, unless a written waiver is granted by the Accreditor. Accreditation is based on a technical investigation and a formal review of the certification Report of Findings. Before authorizing an AIS to operate, the Accreditor must ensure that satisfactory security measures have been installed and that any residual risk is within acceptable limits. Often, the Accreditor must weigh the technical shortcomings of an AIS against operational necessity. Lacking other ways to accomplish an operational mission, the Accreditor may determine that it is preferable to accept a residual security risk than to preclude the mission. To ensure that the accreditation goals and objectives are adequately met, the Accreditor must be involved throughout the system life cycle.

2.7 Two Types of Networks

A network may be defined as either an interconnection of accredited AIS or as a Unified Network. When it is not necessary to differentiate in this guideline, the term network is used.

2.7.1 Unified Networks

The TNI defines a Network Single Trusted System while DODD 5200.28 Enclosure (5) defines a Unified Network; this TNIEG conforms to the latter usage. The section of Enclosure (5) that addresses **Unified Networks** is brief and instructive[5]:

> Some networks may be accredited as a whole without prior accreditation of their component AIS. It is necessary to treat a network as unified when some of its AIS subsystems are so specialized or dependent on other subsystems of the network for security support that individual accreditation of such subsystems is not possible or meaningful with respect to secure network operation. In order to be accredited, a Unified Network shall possess a coherent network architecture and design, and it should be developed with an attention to security requirements, mechanisms, and assurances commensurate with the range of sensitivity of information for which it is to be accredited.
>
> The recommended approach for accrediting a Unified Network is to apply Enclosure 4 to the entire network to derive an evaluation class. Requirements to meet that evaluation class then are obtained from an applicable interpretation of DoD 5200.28-STD [the TCSEC], such as NCSC-TG-005 [the TNI].

2.7.2 Interconnected Accredited AIS

Enclosure (5) of DODD 5200.28 also discusses **Interconnected Accredited AIS**:

> If a network consists of previously accredited AIS, a Memorandum of Agreement[6] [MOA] is required between the DAA of each DOD Component AIS and the DAA responsible for the network ... The network DAA must ensure that interface restrictions and limitations are observed for connections between DOD Component AIS. ... In particular, connections between accredited AIS must be consistent with the mode of operation of each AIS, the specific sensitivity level or range of sensitivity levels for which each AIS

---

[5] As mentioned in the introduction and the definitions, this TNIEG differs from DODD 5200.28 and the TNI in the usage of AIS and the definition of component. This quotation has been slightly edited to conform to the usage in this guideline.

[6] The content of a Memorandum of Agreement is discussed in Section 3.2

is accredited, any additional interface constraints associated with the particular interface device used for the connection, and any other restrictions required by the MOA.

2.8 Network Security Architecture and Design

Network Security Architecture and Design (NSAD) applies to all networks. The NSAD identifies how the NTCB is partitioned and how the trusted system requirements are met. Security engineering, including the development of the NSAD, is a specialty area within systems engineering. The security engineer is responsible for ensuring that the system being built meets the security requirements of the organization. The security engineer ensures that the AIS security conforms to applicable regulations and policy, and implements the system security requirements [8].

The *security policy* includes the set of laws, rules, and practices that govern how an organization manages, protects, and distributes sensitive information (including classified information). The overall security policy is addressed in a family of related documents consisting of a system security policy, a security policy model, and security requirements. The system security policy is developed first, followed by the other two. A system security policy interprets and applies regulations to systems. The security policy model defines subjects and objects and the accesses between the two. The security requirements document identifies evaluatable user requirements for a secure system.

The *security architecture* is that part of the system architecture that describes the required security services and features. The security architecture shows how the required level of assurance for the system is to be met. A mapping of security requirements to functional elements is documented in the security architecture; therefore, the security architecture is used to document security design decisions.

2.9 Protocol Layer Approach

This guideline discusses networks in terms of the Open System Interconnection (OSI) reference model [9] because that model provides a well-understood terminology and is used in the TNI. This guideline, however, is independent of the actual protocol reference model used.

274-353 0 - 90 - 2 : QL 3

An NTCB implementation need not include all protocol layers. The precise security services and their granularity will depend on the highest protocol layer at which an NTCB partition is implemented.[7] For example, in a Unified Network where layer 3 (the network layer) is the highest layer that implements the NTCB, the network will be able to enforce mandatory access control (MAC) and discretionary access control (DAC) decisions on the granularity of network addresses[8]. The network system being evaluated knows only about the range of classifications that the host (or other network) is permitted to handle and the hosts (or other networks) that are permitted to communicate with each other. Finer distinctions must be made by the hosts (or other networks) involved. When a trusted network provides all seven layers, the network is aware of and enforces MAC and DAC at the granularity of individual users.

A network device might not provide a complete set of end-user services through layer 7. Products that do not provide all system services through layer 7 may be NCSC-evaluated as components and subsequently used with other components to compose a network.

2.10 Part II Security Services

The terms *functionality*, *strength of mechanism*, and *assurance* are used to rate TNI Part II services. Their meanings in that context are described below.

Functionality refers to the objective and approach of a security service; it includes features, mechanism, and performance. Alternative approaches to achieving the desired functionality may be more suitable in different applications environments.

Strength of mechanism refers to how well a specific approach may be expected to achieve its objectives. In some cases the selection of parameters, such as number of bits used in a checksum or the number of permutations used in an encryption algorithm, can significantly affect strength of mechanism. With regard to inadvertent threats, strength refers to the ability to operate correctly during natural disasters, emergencies, operator errors, and accidents. Inadvertent threats are particularly

[7]Since the publication of the TNI, the policy environment has changed. "User", as defined in DODD 5200.28, and peer-entity, as defined in the OSI reference model, are comparable. Therefore, the TNIEG applies to all layers of the OSI architecture.

[8]A network address refers to either a host or another network.

critical to prevention of denial of service. As an example, for communications line outages, strength of mechanism may refer to the number of alternate routes that may be used to bypass the outage. The misdelivery of messages is an example of an inadvertent threat that may disclose information to unauthorized individuals. Encryption can be used to prevent the unintended recipient from seeing the information.

Assurance refers to a basis for believing that the functionality will be achieved; it includes tamper resistance, verifiability, and resistance against circumvention or bypass. Assurance is generally based on analysis involving theory, testing, software engineering, validation and verification, and related approaches. The analysis may be formal or informal.

[This page intentionally left blank.]

3 Network Security Architecture and Design (NSAD)

Every network should have a Network Security Architecture and Design (NSAD). This section helps the security manager in establishing the NSAD for the network.

The NSAD, produced as part of the risk management process, documents the security services. As mentioned in Section 1, the primary focus of this TNIEG is on the AIS aspects of security. Depending on the particular environment, communications security (COMSEC), emanations security (TEMPEST), physical security, personnel security, administrative security, and other information security (INFOSEC) measures or safeguards are also incorporated in the NSAD. An NSAD results from a series of tradeoffs among cost, effectiveness, technical risk, mission requirements, and risk management.

While the architecture part of the NSAD may be somewhat abstract, the design part should be quite concrete. The design maps the selected security services to system functional elements[9]. Next, these functional elements are assigned to components and subsystems.

3.1 Composing an NSAD

The security manager is responsible for ensuring that an NSAD is defined that applies to all the components or subsystems that constitute the network. The NSAD for a network must address the applicable security-relevant policies and may incorporate the NSADs of its constituent components or subsystems. In some cases, such as when a component provides part of the functionality of the network (e.g., a local area network (LAN) providing OSI layer three communication services), the NSAD of the component may be incorporated with little or no change into the NSAD for the network. The component NSAD will probably require some modification to address the applicable policy and environment constraints.

A typical network configuration will include multiple vendor's products. When the network is created, the security manager must reconcile the diverse NSADs of the constituents into a coherent NSAD for the configured network and identify any

[9]Sections 4 and 5 of this document should guide the security manager in selecting those security services and safeguards that are appropriate for the given operational environment.

restrictions or new security services and assurance that must be added. The NSAD must implement national, service, and command policies for the environment in which the network will operate. The same process applies when previously accredited AIS are to be interconnected to support the exchange of information.

In contrast to the networks described above, when a network is created from scratch, the NSAD may be established before any devices are selected and may be included as part of the criteria for selecting the network devices.

Note that the network may include components that are not security-relevant and, therefore, do not have a component NSAD. The design decisions that result in the inclusion of non-security-relevant components are documented in the NSAD.

AIS may be combined into a network under conditions of a hierarchical relationship of their security managers. In this case the NSAD of the subordinate system must conform to the governing NSAD. For example, when a host computer connects to a common user network, the host computer must conform to the NSAD established by the security manager of the common user network, who has a responsibility to the security managers of all other connected AIS to maintain the network's trustworthiness. As discussed below, this conformance is recorded in a Memorandum of Agreement (MOA).

AIS whose security managers are not hierarchically related may also be combined to form a network. In this case, the security managers come to agreement on the NSAD for the network; this agreement is also recorded in an MOA.

3.2 Memorandum of Agreement

If a network consists of previously accredited AIS, a MOA is required between the Accreditors for each subsystem. This MOA is part of the documentation of the NSAD. The MOA discusses the accreditation requirements for each subsystem that is to be interconnected to form the network [4], i.e., defines all the terms and conditions of the security arrangements that will govern the operation of the network [10]. The objective of the MOA is to document the interconnection requirements and identify any requirements that may be necessary to provide *overall* security safeguards for the entire network. This network includes all the interconnected subsystems, the communications devices, the users, and the data stored in the subsystem [10]. A Memorandum of

Record (MOR) is used when the subsystems have the same Accreditor. A comprehensive MOA[10] could constitute the entire NSAD for a network; alternatively, the MOA could contain high level agreements, with the details spelled out in supporting documents. Following is a list of suggestions for the contents of the MOA and supporting documents. The items towards the top of the list are more likely to occur in the MOA; those towards the end of the list are more likely to occur in supporting documents.

- A general description of the information that will be transmitted to the network by each subsystem
- A summary discussion of the trusted behavior that is expected from each subsystem
- The details of the overall security plan for the network and the assignment of responsibility for producing and accepting the plan
- A description of the overall network security policy
- A description of additional security training and assignment of training responsibility
- Specification of the security parameters that are to be transmitted between communicating subsystems
- A discussion of security details that are relevant to the exchange of information among the subsystems.
- A description of the user community, including the lowest clearance of any user who will have access to the network
- Any special considerations for dial-up connections to any subsystem in the network, including potential security threats and the safeguards that will be used.
- A description of the security protections provided by the data communications, both local to a subsystem and between communicating subsystem

[10]In this guideline, MOA is used to identify the agreement between Accreditors and includes the MOR.

- A description of the information that each subsystem will log in the audit trail, and how the audit trail tasks will be divided among the subsystems
- A description of the information security services to be offered to the network by each subsystem, including:
  - The types of processing provided by each subsystem, e.g., file query, individual user, general processing
  - The modes of operation of all the subsystems, e.g., dedicated, system high, multilevel
  - The sensitivity levels processed on all subsystems

4 TNI Part I Security Requirements

This section assists the security manager in determining the recommended minimum security requirements based on TNI Part I and Appendix A, which interprets the TCSEC for networks.

The procedure for determining the minimum security requirements for a network parallels the procedure for a stand-alone system, whereby the highest classification of data and the lowest clearance among system users are used in computing a risk index. The risk index is used to determine which NCSC-evaluation rating is required of the system to provide adequate security. To emphasize, these are the minimum requirements. The TCSEC Environments Guideline does not address environmental factors such as the number of users and the percentage of users at different classification levels. These factors may become more significant in a network environment. Communications security risk in a network is addressed by the National Security Agency (NSA) and other cognizant organizations and results in a set of recommendations for the appropriate equipment or security procedures. Other factors, such as the number of connections, the physical distance between devices, the number of subsystems, the presence of encryption, and the possible presence of intervening systems between the resources being used and the ultimate user may result in more or less stringent requirements.

4.1 Risk Management

Risk management is a methodology used to identify, measure, and control events which adversely affect security; it involves cost-benefit analyses to ensure appropriate cost-effectiveness of security safeguards. A risk management program is mandated by Enclosure (3) of DODD 5200.28.

The literature on risk management is quite extensive. It is not the purpose of this document to survey the field. The interested reader is referred to FIPS PUB 65 [11]. The literature is constantly growing; a recent high-level introduction to general concepts and terminology can be found in Bell [12] and in the Proceedings of the First Invitational Workshop on Computer Security Risk Management [13].

DODD 5200.28 Enclosure (4) mandates the use of a methodology, extracted from the TCSEC Environments Guideline, to determine the recommended evaluation class

(or requirements of an evaluation class) based on a specific environment. Enclosure (5) of the Directive also recommends this method to determine minimum computer-based requirements in a network. This guideline also uses that method. Use of a different method requires prior approval of the Assistant Secretary of Defense (ASD) Command, Control, Communications, and Intelligence (C^3I).

DODD 5200.28 Enclosure (4) contains six major steps in the risk assessment procedure. These steps are listed below. DODD 5200.28 Enclosure (4) applies in all steps.

Step 1. Determine system security mode of operation.

Step 2. Determine minimum user clearance or authorization rating.

Step 3. Determine maximum data sensitivity rating.

Step 4. Determine risk index.

Step 5. Determine minimum security evaluation class for computer-based controls.

Step 6. Determine adjustments to computer security evaluation class required.

An elaboration of step six given in Migues [14], involving a detailed analysis of both environmental and architectural risk factors, is based on Landwehr and Lubbes [15]. It presents a method which incorporates analysis of the applications environment. This analysis includes such factors as whether the system allows programming, or whether it is restricted to a limited set of applications. This more detailed information supports a finer determination of the level of trust required.

4.2 Determination of Network Risk

To apply the TCSEC Environments Guideline guidance, the security manager must determine the following:

- minimum clearance or authorization of the network users (see Table 1[11]),

[11]Tables 1 and 2 are adapted from DODD 5200.28 (Enclosure 4).

Table 1
Rating Scale for Minimum User Clearance (Rmin)

Minimum User Clearance	Rmin
Uncleared OR Not Authorized (U)	0
Not Cleared but Authorized Access to Sensitive Unclassified Information (N)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS) and/or current Background Investigation (BI)	4
TS and/or current Special Background Investigation (SBI)	5
One Category (1C)	6
Multiple Categories (MC)	7

- maximum sensitivity of data processed by the network (see Table 2) (the TCSEC Environments Guideline distinguishes between an open system and a closed system based on whether application development was done by cleared or uncleared users; the distinction was dropped in DODD 5200.28 and is not used here either).

The number derived from Table 1 is used for Rmin; the one derived from Table 2 is used for Rmax. A risk index for the network is calculated using the following formula:

$$\text{Risk Index} = R_{max} - R_{min}$$

Table 2
Rating Scale for Maximum Data Sensitivity (Rmax)

Maximum Sensitivity Ratings without categories	Rating (Rmax)	Maximum Data Sensitivity with categories[1,2]	Rating (Rmax)
Unclassified (U)	0	N/A[3]	
Not Classified but Sensitive (N)[4]	1	N with one or more Categories	2
Confidential (C)	2	C with one or more Categories	3
Secret (S)	3	S with one or more Categories only one Category containing S S with two or more Categories containing S	4 5
Top Secret (TS)	5[5]	TS with one or more Categories only one Category containing S or TS TS with two or more Categories containing S or TS	6 7

1 Where the number of categories is large or where a highly sensitive category is involved, a higher rating might be warranted.

2 The only categories of concern are those for which some users are not authorized access. When counting the number of categories, count all categories regardless of the sensitivity level associated with the data. If a category is associated with more than one sensitivity level, it is only counted at the highest level. Systems in which all data are in the same category are treated as without categories.

3 Unclassified data by definition may not contain categories.

4 Examples of N data include financial, proprietary, privacy, and mission-sensitive data. In some situations (e.g., those involving extremely large financial sums or critical mission-sensitive data), a higher rating may be warranted. This table prescribes minimum ratings.

5 The rating increment between the Secret and Top Secret data sensitivity levels is greater than the increment between other adjacent levels. This difference derives from the fact that the loss of Top Secret data causes EXCEPTIONALLY GRAVE damage to U.S. national security, whereas the loss of Secret data causes SERIOUS damage.

Table 3
Security Risk Index

Risk Index	Security Mode	Minimum Security Class[4]
0	Dedicated[5]	No Minimum Class[1,2]
0	System High	C2[2]
1	Multilevel, Partitioned	B1[3]
2	Multilevel, Partitioned	B2
3	Multilevel	B3
4	Multilevel	A1
5	Multilevel	*
6	Multilevel	*
7	Multilevel	*

1 Although there is no prescribed minimum class, the integrity and denial of service requirements of many systems warrant at least class C2 protection.

2 Automated markings on output must not be relied on to be accurate unless at least class B1 is used.

3 Where an AIS handles classified or compartmented data and some users do not have at least a Confidential clearance, or when there are more than two types of compartmented information being handled, at least a class B2 is required.

4 The asterisk (*) indicates that computer protection for environments with that risk index is considered to be beyond the state of current computer security technology.

5 Most embedded systems and desk top computers operate in the dedicated mode.

Table 3[12] is used, along with the Risk Index calculated above, to determine a minimum NCSC-evaluation rating for the system. Note that some terms that appear in the TCSEC Environments Guideline are no longer defined in DODD 5200.28. (*Limited Access Mode*, and *Compartmented Mode* fall under the heading of *Partitioned Mode*. *Controlled Mode* comes under the heading *Multilevel*. The previously used terms referred to the equivalent of the B1 and B2 evaluation classes. In DODD 5200.28, *Partitioned Mode* is used in place of *Compartmented Mode*.)

[12]Table 3 is adapted from the TCSEC Environments Guideline

[This page intentionally left blank.]

5 TNI Part II Security Requirements

This section contains a discussion of TNI Part II which describes qualitative evaluations of security services in terms of functionality, strength of mechanism, and assurance. Part II of the TNI describes additional security concerns and services that arise in conjunction with networks, but that do not normally arise in stand-alone computers.

Part II of the TNI focuses on those threats that occur between end systems (hosts) on the network. These security services include protection against compromise, denial of service, and unauthorized modification. In discussing these services, the TNI borrows heavily from the International Standards Organization (ISO) OSI Basic Reference Model [9] and Security Architecture [16]. The services discussed are closely related to those found in the latter reference. The TNI goes beyond the OSI Security Architecture in several respects. First, the OSI document does not address the relative strengths of different mechanisms nor the assurances that they operate as intended. Second, the protection against denial of service threats is not specifically addressed by OSI but is an important consideration in the TNI.

5.1 Relationship of TNI Part II Services to Part I and Appendix A

The Part II services are not as well understood as the features in TNI Part I. The fact that Part II services have not been supported by equally well developed theories and detailed evaluation criteria should not be interpreted to imply that their security problems do not have to be evaluated as rigorously as TNI Part I and Appendix A services. Some Part II services may not be part of the NTCB. For example, to make the NTCB as small as possible, some of the protocol software may be outside the NTCB. Therefore, the protocol-based protection against denial of service is likely to be outside the NTCB. Nonetheless, it must rely on some of the fundamental NTCB assurances since the protocols invoke portions of the subsystem's operating system.

It is important to recognize that many Part II security services depend on (embedded) AIS. These AIS should be evaluated using Part I and Appendix A of the TNI. Encryption systems, for example, are highly dependent upon AIS; they are addressed in Appendix B of the TNI and Appendix C of this guideline. Appendix C presents some considerations concerned with applying Tables 1, 2, and 3 to encryption systems.

For security services that do not depend strongly on AIS, a qualitative evaluation approach is used. For functionality, a question and answer format is presented in Section 5.4.3. For strength of mechanism and assurance, the concept of a risk index is used in Sections 5.4.1 and 5.4.2.

5.2 Specification and Evaluation of Security Services

Specifying and evaluating Part II security services is quite different from a TNI Part I evaluation even though both parts are concerned with the same three aspects of security services or capabilities: functionality, strength of mechanism, and assurance. For clarity these terms are defined as follows:

Functionality refers to the objective and approach of a security service.

Strength of mechanism refers to how well a specific approach may be expected to achieve its objectives.

Assurance refers to a basis for believing that the functionality will be achieved.

5.3 Evaluation Ratings

Part II evaluations are qualitative, as compared with the hierarchically-ordered ratings (e.g., C1, C2, ...) from the TCSEC. The results of a Part II evaluation for offered services are generally summarized using the terms *none, minimum, fair,* and *good*. For some services, functionality is summarized using *none* or *present* because gradations are not meaningful. The term *none* is used to mean the security service fails to distinguish the strength of mechanism. The term *not offered* is used when a security service is not offered. For example, if a certain network did not include non-repudiation as one of its security services, that network would be rated *not offered* with respect to non-repudiation. Table 4 represents the evaluation structure of Part II as a matrix. It identifies a set of security services. It also shows the possible evaluation ranges for each service in terms of its functionality, strength of mechanism, and assurance.

5.4 Selecting Security Services

Part II enumerates representative security services that an organization may choose to employ in a specific situation. Not all security services will be equally important for a specific environment, nor will their relative importance be the same

Table 4
Evaluation Structure for Network Security Services

Network Security Service	Criterion	Evaluation Range
Communications Integrity Authentication	Functionality Strength Assurance	None | present None - good None - good
Communications Field Integrity	Functionality Strength Assurance	None - good None - good None - good
Non-repudiation	Functionality Strength Assurance	None | present None - good None - good
Denial of Service Continuity of Operations	Functionality Strength Assurance	None - good None - good None - good
Protocol Based Protection	Functionality Strength Assurance	None - good None - good None - good
Network Management	Functionality Strength Assurance	None | present None - good None - good
Compromise Protection Data Confidentiality	Functionality Strength Assurance	None | present Sensitivity level None - good
Traffic Flow Confidentiality	Functionality Strength Assurance	None | present Sensitivity level None - good
Selective Routing	Functionality Strength Assurance	None | present None - good None - good

among different environments. Selecting security services is a management decision, with assistance provided by this guideline.

Ordinarily, the security manager would first determine whether a particular service is required and what functionality is needed (if there are distinctions) through a series of questions provided in Section 5.4.3. A separate set of questions is provided for each service shown in Table 4.

274-353 0 - 90 - 2 : QL 3

Once the functionality has been determined, the strength of mechanism and appropriate level of assurance must be determined. The process is similar to the determination of Part I risk in Section 4 of this guideline. Since the strength of mechanism and assurance determination do not differ for the various services, these topics are addressed first.

5.4.1 Strength of Mechanism

Determination of strength of mechanism for each service has two components. The inadvertent threat and the malicious threat should be analyzed separately. In many cases, the malicious threat will dominate the inadvertent threat; malicious users can often duplicate the circumstances of an inadvertent threat. The required strength of mechanism is determined using a risk index similar to that used in Part I.

For inadvertent threats, traditional risk management techniques are used. While some countermeasures may be the same for inadvertent and malicious threats, others may be effective only against the former. The security manager must determine the likelihood of a particular threat, the dollar cost of a countermeasure, and the residual risk if the countermeasure is put into effect. The manager concerned with these inadvertent threats is referred to the references on risk assessment previously cited.

For malicious threats, we consider the most sensitive information contained on the system and the lowest clearance of user who can gain *physical* access to some device in the system, including access to wireless transmissions. Some devices in the system may be physically protected in buildings that require a clearance for admittance. Other devices in the system, such as long-haul transmission lines, may have no physical protection.

Protection of the information in the network system is a combination of physical, administrative, procedural, and technical protections. The TNI is concerned only with the AIS hardware, firmware, software, and configuration management protections. Various service or agency regulations describe methods for implementing the other protections.

The various devices in the system must be considered separately; for each device, the risk index will be based on the most sensitive information on the network system and the minimum clearance to gain physical access to the device. Note that this is

different from the Part I risk index calculation (where the lowest cleared *user* is of concern). For some devices in the system (e.g., the communications media), the clearance of individuals with physical access may be lower than that for authorized users. For convenience, all the necessary tables are included here. Table 5, Minimum Clearance for Physical Access, is identical to Table 1. For each device in the system, the lowest clearance of individuals with physical access to that device is used. Table 6 for Maximum Data Sensitivity is identical to Table 2.

Table 5
Minimum Clearance for Physical Access

Minimum User Clearance	Rmin
Uncleared OR Not Authorized (U)	0
Not Cleared but Authorized Access to Sensitive Unclassified Information (N)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS) and/or current Background Investigation (BI)	4
TS and/or current Special Background Investigation (SBI)	5
One Category (1C)	6
Multiple Categories (MC)	7

Table 6
Maximum Data Sensitivity

Maximum Sensitivity Ratings without Categories	Rating (Rmax)	Maximum Data Sensitivity with Categories[1,2]	Rating (Rmax)
Unclassified (U)	0	N/A[3]	
Not Classified but Sensitive (N)[4]	1	N with one or more Categories	2
Confidential (C)	2	C with one or more Categories	3
Secret (S)	3	S with one or more Categories only one Category containing S S with two or more Categories containing S	4 5
Top Secret (TS)	5[5]	TS with one or more Categories only one Category containing S or TS TS with two or more Categories containing S or TS	6 7

1 Where the number of categories is large or where a highly sensitive category is involved, a higher rating might be warranted.

2 The only categories of concern are those for which some users are not authorized access. When counting the number of categories, count all categories regardless of the sensitivity level associated with the data. If a category is associated with more than one sensitivity level, it is only counted at the highest level. Systems in which all data are in the same category are treated as without categories.

3 Unclassified data by definition may not contain categories.

4 Examples of N data include financial, proprietary, privacy, and mission-sensitive data. In some situations (e.g., those involving extremely large financial sums or critical mission-sensitive data), a higher rating may be warranted. This table prescribes minimum ratings.

5 The rating increment between the Secret and Top Secret data sensitivity levels is greater than the increment between other adjacent levels. This difference derives from the fact that the loss of Top Secret data causes EXCEPTIONALLY GRAVE damage to U.S. national security, whereas the loss of Secret data causes SERIOUS damage.

Table 7 now gives the strength of mechanism requirement based on the risk index calculated as

$$\text{Risk Index} = R_{max} - R_{min}$$

Table 7
Minimum Strength of Mechanism Requirement

Risk Index	Strength of Mechanism
0	None
1	Minimum
2	Fair
>2	Good

5.4.2 Assurance

Assurance is a very important concept in the TCSEC and TNI. This section discusses the need for assurance and the ways in which it may be achieved.

One salient property of trusted systems is the reliance on a TCB. Similarly, trusted network systems rely on an NTCB. In addition to its other responsibilities, the NTCB prevents unauthorized modification to objects within the network system. In particular, the NTCB maintains the integrity of the programs which provide security services, thus ensuring that their assurance is continued. The NTCB provides an execution environment that is extremely valuable in enhancing the assurance of security services. Discretionary and mandatory access controls can be employed to segregate unrelated services. Thus, service implementation that is complex and error-prone or obtained from an unevaluated supplier can be prevented from degrading the assurance of other services implemented in the same device. Furthermore, an NTCB ensures that the basic protection of the security and integrity information entrusted to the network is not diluted by various supporting security services.

The relationship of the risk index to the required assurance is expressed in Table 8.

Table 8
Minimum Assurance Requirements

Risk Index	Part II Assurance Rating
0	None
1	Minimum
2	Fair
>2	Good

Assurance of the design and implementation of Part II mechanisms is also related to the assurance requirements in Part I because service integrity depends on protection by the NTCB or TCBs. Table 9 expresses this dependency. The second column identifies the minimum Part I evaluation which supports the Part II assurance requirement. Note that Table 9 is applicable only to those Part II services not strongly dependent on AIS; the AIS implementing those services can be directly evaluated under Part I and Appendix A of the TNI.

Note that the Evaluation Class calculation in Part I will not necessarily be the same as the Minimum Part I Evaluation in Table 9. This is because the R_{min} for Part II may be different from that of Part I since the Part II protections are oriented towards outsiders (those with physical access) rather than towards users. Depending on the particular environment, either the Part I requirement or the Part II requirement may dominate. The latter would be the case if a system were operated in the system high mode—where all users were cleared to see the most sensitive information—but the network was exposed to lower clearance individuals.

5.4.3 Functionality

This section asks questions about each of the security services contained in Part II of the TNI. These questions are designed to help the security manager identify the functionality required for each security service. The questions should be answered in sequence, unless the answer to one question contains an instruction to skip ahead.

Authentication

1. Is there a requirement to determine what individual, process or device is at the other end of a network communication? If yes, document this requirement.

Table 9
Part II Assurance Rating

Part II Assurance Rating	Minimum Part I Evaluation
Minimum	C1
Fair	C2
Good	B2

If no, skip to Communications Field Integrity.

2. Do you have a requirement to identify and authenticate the specific hardware device at the distant end-point involved in the network communication?

   If yes, then you have a functionality requirement for authentication. This functionality may be implemented at one or more protocol layer. For example, a specific control character, ENQ (enquiry or who-are-you) may be used to return immediately a stored terminal identifier.

3. Do you have a requirement to identify and authenticate the location of the hardware at the distant end-point or in any intermediate system involved in the network communication?

   If yes, then you have a functionality requirement for authentication at protocol layer 2, the Link Layer or layer 3, the Network Layer.

4. Do you have a requirement to identify and authenticate the specific operating system or control program at the distant end-point or in any intermediate system involved in the network communication?

   If yes, then you have a functionality requirement for authentication at protocol layer 4, the Transport Layer.

5. Do you have a requirement to identify and authenticate the subject (process/domain pair) at the distant end-point involved in the network communication?

   If yes, then you have a functionality requirement for authentication at protocol layer 4 or above.

6. Do you have a requirement to identify and authenticate the application or user at the distant end-point involved in the network communication?

   If yes, then you have a functionality requirement for authentication above protocol layer 7, the Applications Layer. The Applications Layer provides an interface to the application. Authentication information may pass over this interface. Authentication of a user is addressed in Part I of the TNI. Application process authentication is outside the scope of the OSI Security Architecture, but does fall within the scope of TNI Part II Security Services.

   Have you chosen to use some mechanism other than encryption to provide authentication? If so, your strength of mechanism is shown in Table 7.

   If your authentication mechanism is encryption based, see the appropriate encryption authority (e.g., NSA). Even if encryption is used, some supporting processes may need to satisfy the strength of mechanism shown in Table 7 (depending on the architecture). For example, a database that relates encryption keys to specific users may need to be trusted.

Communications Field Integrity

1. Do you have a requirement to protect communication against unauthorized modification?

   If no, skip to Non-Repudiation.

2. Are your protection requirements the same for all parts of the information communicated?

   If no, then you should identify the separate parts and answer the rest of the questions in this section separately for each part. Each part is known as a field.

   There are two major fields: protocol-information, wherein the network is informed of the destination of the information and any special services required; and user-data. Not every protocol data unit (PDU) contains user-data, but protocol-information is necessary. Each of these fields may be divided into additional fields; depending on your application, protection requirements for fields may differ.

3. Do you have a requirement for detecting unauthorized modification to part or all of a PDU?

   If yes, you have a requirement for at least minimum functionality.

4. Do you have a requirement for detecting any of the following forms of message stream modification: insertion, deletion, or replay?

   If yes, you have a requirement for at least fair functionality. In addition, your functionality must be incorporated in a connection oriented protocol.

5. Do you require that, if message stream modification is detected, recovery (correction) should be attempted?

   If yes, you have a requirement for good functionality. In addition, you must implement integrity in a reliable transport (layer 4) mechanism.

Non-repudiation

1. Do you have a requirement to be able to prove (to a third party) that a specific message transfer actually occurred?

   If no, skip to Denial of Service.

2. Do you have a requirement for proving that a specific message was sent? *Specific message* means that the identity of the subject sending the message, the host computer and/or mail agent/server, time and date, and contents are all uniquely and unalterably identified.

   If yes, then you have a functionality requirement for non-repudiation with proof of origin.

3. Do you have a requirement for proving that a specific message was received? *Specific message* means that the identity of the subject to which the message was delivered, the host computer and/or mail agent/server, time and date, and contents are all uniquely and unalterably identified.

   If yes, then you have a functionality requirement for non-repudiation with proof of delivery.

Denial of Service

1. Do you have a requirement to assure the availability of communications service or to determine when a *Denial of Service* (DOS) condition exists? A DOS condition is defined to exist whenever throughput falls below a pre-established threshold, or when access to a remote entity is unavailable, or when resources are not available to users on an equitable basis. For a DOS condition to occur, the user must have priority to access the system or resources.

   If no, skip to Data Confidentiality.

2. Do you have a requirement to detect conditions that would degrade service below a pre-selected minimum and to report such degradation to the network operators?

   If yes, you have a requirement for at least minimum denial of service functionality.

3. Could failure of the system to operate for several minutes lead to personal injury or large financial loss?

   If yes, you have a requirement for at least fair denial of service functionality.

4. Do you have a requirement for service resiliency that would continue—perhaps in a degraded or prioritized mode—in the event of equipment failure and/or unauthorized actions?

   If yes, you have a requirement for at least fair denial of service functionality.

5. Could failure of your system to operate for several minutes lead to loss of life?

   If yes, you have a requirement for good denial of service functionality.

6. Do you have a requirement for automatic adaptation upon detection of a denial-of-service condition?

   If yes, you have a requirement for good denial of service functionality.

Protocol Based DOS Protection

1. Do you want advanced knowledge of unavailability of service?

   If no, skip to Network Management.

   If yes, do you want to implement alternatives?

   If yes, you should employ this alternative basis and skip to Network Management.

2. In general, ordinary protocol mechanisms don't provide protection against malicious attacks or bizarre errors. Do you have a requirement to detect a DOS condition which cannot be met by the protocols used as part of normal communications?

   If no, you do not have a functional requirement for protocol-based DOS protection and should skip to Network Management.

3. The TNI suggests the following protocol-based mechanisms:

   a. Measure the transmission rate between peer entities under conditions of input queuing, and compare the measured transmission rate with a rate previously identified as the minimum acceptable;

   b. Employ a request-response polling mechanism, such as "are-you-there" and "here-I-am" messages, to verify that an open path exists between peer entities.

   If you have identified any additional mechanisms, include them in your list of required mechanisms.

Network Management

1. Do you have a requirement for (at least) detecting a denial of service condition that affects more than a single instance of communication, or attempted communication?

   If no, skip to Data Confidentiality.

   If yes, you have a functional requirement for network management denial of service protection.

Data Confidentiality

1. Do you have a requirement to protect any part of transmitted data from disclosure to unauthorized persons?

   If no, skip to Traffic Flow Confidentiality.

2. Is your requirement for confidentiality limited to selected field of user-data within a PDU?

   If no, then you require confidentiality for the entire data portion of each PDU. Continue with Traffic Flow Confidentiality.

3. Is there a reason to encrypt only selected fields (e.g., cost savings, legal requirements)?

   If yes, you require selected field confidentiality. If no, you require full confidentiality on the data portion of each PDU.

Traffic Flow Confidentiality

1. Do you have a requirement to prevent analysis of message length, frequency, and protocol components (such as addresses) to prevent information disclosure through inference (traffic analysis)?

   If no, skip to Selective Routing.

   If yes, you have a functional requirement for traffic flow confidentiality.

Selective Routing

1. Do you have a requirement to choose or avoid specific networks, links, relays, or other devices for any reason at any time?

   If yes, you have a functional requirement for selective routing.

6 Interconnecting AIS

The definition of Interconnected Accredited AIS recognizes that parts of a network may be **independently** created, managed, and accredited. AIS in different security domains[13] generally operate under different security policies, consequently, it is difficult to combine them into a Unified Network. For example, AIS operated by the U.S. DOD and NATO cannot be combined into a Unified Network, since they enforce different policies and do not have a common authority.

Interconnecting systems that support different security domains (e.g., classified, sensitive unclassified) adds additional complexity. Exchange of information among these different security domains requires identification of the markings and protection given to information when transmitted to another domain. For example, several evolving approaches to the protection of sensitive unclassified information [17] consider "that sensitive information is not part of the same hierarchy as classified information".

There are technical criteria for judging the trustworthiness of Interconnected Accredited AIS: an Interconnection Rule, which ensures that information conveyed between subsystems is labeled properly, and risk factors such as *propagation of local risk* and the *cascading problem*. These criteria are examined in some detail below.

6.1 Agreement Between Accreditors

Interconnection of AIS between security domains requires a documented agreement identifying the interconnection requirements and all safeguards. This agreement will have many similarities to the MOA discussed in Section 3.2. It will probably have to reconcile different security policies and philosophies of protection, identifying the conditions under which specified classes of information can be exchanged among domains. In addition to the information included in the MOA, this agreement between managers of different security domains should address the mappings of policy and countermeasures between the domains. In many ways this agreement takes on the character of an NSAD for the agreed upon information exchange between domains.

[13]A security domain is a collection of AIS under the control of a single administrator that enforces or operates under a specified policy. There can be sub-domains, (e.g., Army and Air Force are sub-domains under the Department of Defense.)

6.1.1 Accreditation Range

An accreditation designates a system's mode of operation and range of data sensitivity levels. The *accreditation range* reflects the Accreditor's judgment on the subsystem's ability to exchange information within an acceptable level of risk, with respect to its network connections, and in accord with the designated sensitivity levels.

The range must be a single level in the case of a system high or dedicated device[14]. If the accreditation range comprises more than a single level, the system is trusted to reliably segregate data by level within its accreditation range, and label it accurately for transmission over multilevel interfaces. The accreditation range will be specified in the MOA. The accreditation range is used in determining whether communication between systems is permitted.

Figure 1
Information Levels and Accreditation Ranges

C2	Evaluation Class	B3
S	Accreditation Range	TS-C
SH	Operating Mode	MLS

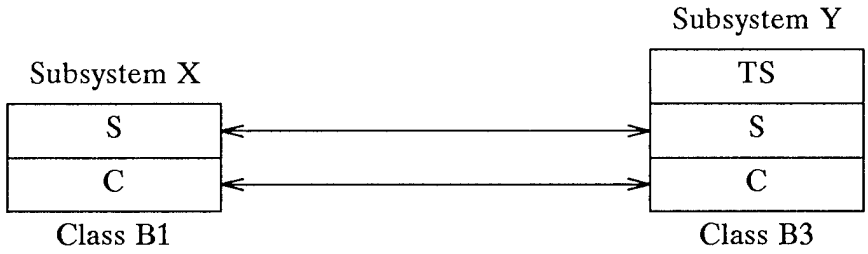
As shown in Figure 1, an AIS may contain information at levels that are below its accreditation range. For example, a C2 host which contains Secret (S) and Confidential (C) information, is not trusted to segregate this Confidential and Secret information. Therefore, it is accredited to operate in system high (SH) mode at Secret (the highest sensitivity level of information on the system), and its accreditation range is the single level Secret. All exported information must be labeled with the system high sensitivity label until there is a manual review to assign the information a lower

[14]Often in the discussion it is not appropriate to distinguish between a component and a subsystem; in that case we use the term device.

classification level. In contrast, a B3 multilevel secure (MLS) host, which contains Top Secret (TS), Secret, and Confidential information could be assigned an accreditation range equal to the entire set of levels processed. In this case, the label of the exported data is equal to the *actual level* of the exported data, unless unclassified data is to be exported.

Figure 2 illustrates the accreditation ranges of two interconnected subsystems. Although Subsystem Y is able to separate its three levels of information, it may exchange information with Subsystem X *only* at the S and C levels.

Figure 2
Accreditation Ranges of Two Interconnected Subsystems



In a network, an accreditation range bounds the sensitivity levels of information that may be sent (exported) to or received (imported) from each interconnected subsystem[15]. For example, if a network consists of only dedicated and system high subsystems, each subsystem will be assigned single-valued accreditation ranges (i.e., an accreditation range consisting of one sensitivity level).

When the same communications channel processes information at different levels, the data must be labeled through some protocol agreed upon by the communicating systems.

[15]Note that information exported or imported to a subsystem having a single-level accreditation range is implicitly labeled at that level. It is also possible for a subsystem with a multilevel accreditation range to employ network interface devices with single-level ports, in which case the data transferred over such ports is also implicitly labeled.

DODD 5200.28 Enclosure (5) also addresses AIS that have not been accredited:

> Untrusted, unaccredited AIS ... may be components of a network.... Only unclassified information, which does not include sensitive unclassified information, may be sent to and from untrusted, unaccredited AIS.

This trust requirement is satisfied by restricting the accreditation range of the untrusted, unaccredited AIS to Unclassified (U).

6.1.2 Device Range

A network subsystem is typically connected to another subsystem through some kind of I/O network interface or device (see Figures 3-6) and the same device may provide connection to multiple subsystems.

Although an I/O device is part of a subsystem, it may be designated to process a more restricted set of sensitivity levels than the accreditation range of the subsystem as a whole. This leads to the concept of a *device range*. Each I/O device in a subsystem that is used to communicate with other subsystems in the network must have a device range. The device range may be single level, or it may be a set of levels (in which case the device is referred to as multilevel), and it must be included within the subsystem accreditation range. The TCSEC states that "systems that have been evaluated at classes B2 and above must support minimum and maximum security labels for all multilevel I/O devices". The purpose of device labels is to document the constraints placed on the security levels of information authorized for the devices.

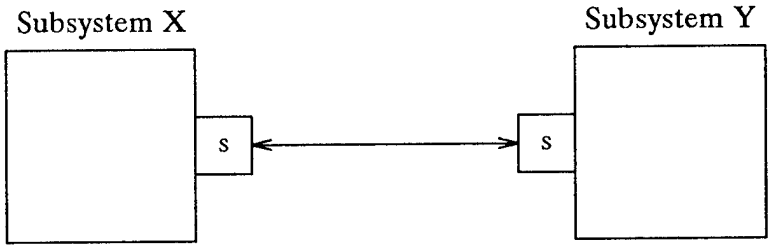
Each physically attached multilevel system (if any) has a minimum and maximum sensitivity level associated with it. A B1 or higher system interconnected to a second system must ensure that both imported and exported information is contained within appropriate sensitivity levels.

6.1.3 Information Transfer Restrictions

The following points summarize the discussion on the restrictions imposed on information transfer between interconnected devices.

Information exported or imported using a single-level device is labeled implicitly by the security level of the device. As shown in Figure 3, any information transferred between the single-level (S) devices on Subsystems X and Y is implicitly labeled S.

Figure 3
Implicit Labeling



Information exported from one multilevel device and imported at another multilevel device must be labeled through an agreed-upon protocol, unless it is labeled implicitly by using a communications link that always carries a single level. For instance, in Figure 4, Secret and Confidential information may be transferred between the multilevel devices.

Figure 4
Protocol Labeling

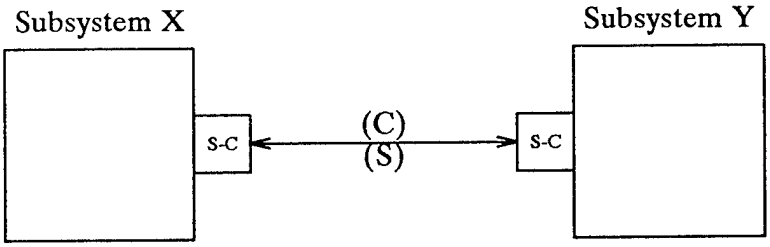
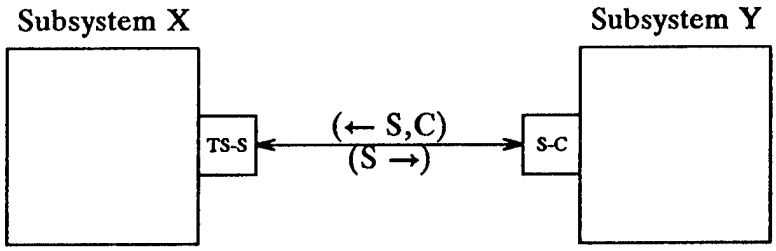
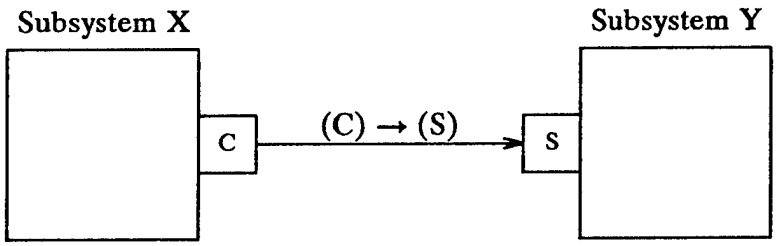


Figure 5
Compatibility Labeling



Information exported at a given security level can be sent only to an importing device whose device range contains that level or a higher level. In Figure 5, Subsystem X is allowed to export only Secret information to Subsystem Y's multilevel device. Subsystem Y is allowed to export Secret and Confidential information to Subsystem X, because the device range Subsystem X is TS-S. If the importing device range dominates the exported level, the information is implicitly or explicitly relabeled upon receipt at a higher level within the importing device range.

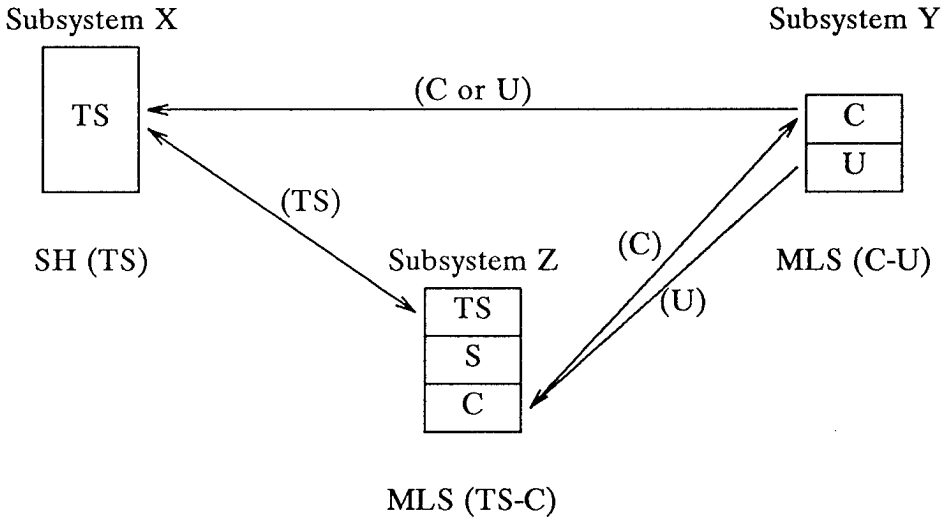
Figure 6
Relabeling



In Figure 6, Subsystem Y relabels information imported from Subsystem X. The information transfer restrictions also permit one-way communication (i.e., no acknowledgments) from one device to another whose ranges have no level in common, as long as each level in the sending device range is dominated by some level in the receiving device range. It is never permitted to send information at a given level to a device whose range does not contain a dominating level.

In most interconnected subsystems, the bidirectional flow of information is permitted. In this environment, the sensitivity level of any transmitted message must be within the accreditation range of both the sending and receiving systems. In some networks, an additional restriction on information flow may be *unidirectional communications*. This restriction may enhance security. The following discussions refer to Figure 7.

Figure 7
Bidirectional and Unidirectional Information Flow



The system high mode is usually assigned to AIS that are unevaluated or are NCSC-evaluated in class C. These AIS do not employ explicit labels because they cannot be trusted to differentiate between sensitivity levels. All information within these AIS is implicitly labeled. When exported on a single level channel, by default the information is labeled implicitly by the level of the channel. Human-readable output must be labeled at the system high level; it may be manually downgraded by an authorized reviewer.

Explicit labels are required on a multilevel channel. In order to export explicit labels, Subsystem X would normally be expected to be NCSC-evaluated at B1 or above, or employ an I/O device, such as those shown in Figure 6, NCSC-evaluated at B1 or above. Also, Subsystem X or the I/O device should be used as specified in Section 4

of this guideline. Lacking such NCSC-evaluation, the MOA between the Accreditors would have to specifically address these labels.

Subsystem X can import a message from Subsystem Y, but cannot acknowledge receipt of that message, because an exported acknowledgment (labeled TS) cannot be imported by Subsystem Y, which can only receive C or U information. Transmitting an acknowledgment from Subsystem X to Subsystem Y would constitute a write-down (i.e., writing information at a lower sensitivity level—generally a security violation.)

Subsystems Y and Z can exchange information at C since this level is in the accreditation range of each subsystem. When only unidirectional communication (no acknowledgment) is utilized between two subsystems, write up is permitted if each sensitivity level in the source subsystem is dominated by a sensitivity level in the destination subsystem. The receiving subsystem must change the sensitivity level of the message when the message is received. For instance, U information sent from Subsystem Y will be labeled C by Subsystem Z.

6.2 Interconnection Rule

The Interconnection Rule states that each device in the network must be separately accredited to operate in an approved security mode of operation and with a specific accreditation range. The device is accredited to participate in the network at those levels and only those levels. This means that information exported at a given sensitivity level can be sent only to an importing device whose accreditation range contains that level or a higher level. Information is relabeled, implicitly or explicitly, upon reception at a higher level within the importing device accreditation range only if the original level is not in that range.

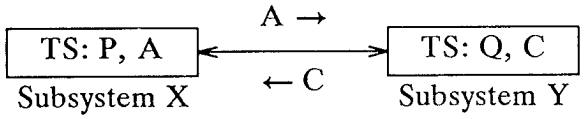
According to the Interconnection Rule, a multilevel network may contain devices with different operating modes: dedicated, system high, partitioned, and multilevel. Also the devices may differ in the sensitivity levels and categories which they process, and the formal access approvals of their users (some users may not have access to all information).

Figure 7 illustrates the flexibility of the Interconnection Rule. For example, the Interconnection Rule will allow, with certain restrictions, a multilevel subsystem to communicate with a single-level subsystem and with another multilevel subsystem (and

the two MLS subsystems may have different accreditation ranges). It also allows for one-way communication to a higher-level system. It is intended to be a non-restricting rule and yet ensure that each system receives only information that it can properly mark and handle. Interconnection in the context of the Interconnection Rule means only *direct* connections, that is, without any intermediate accredited subsystem.

The Interconnection Rule alone does not guarantee that classified information will not be exposed to greater risks in a network than in a stand-alone environment. One problem in networks that is dealt with at some length below is the cascading problem.

Figure 8
A Complex Interconnection



6.2.1 A Complex Example

The Interconnection Rule and device range allow for some rather challenging situations. Consider, for example, the connection depicted in Figure 8. The system on the left processes TS information of two types: categories A and P (where P is the union of categories C and D, P = C ∪ D). The system on the right processes the categories C and Q (where Q is the union of categories A and B, Q = A ∪ B). The two devices have no sensitivity levels in common. Yet this is a legitimate connection as long as only TS,A and TS,C information is transferred. Any information sent must be relabeled upon receipt. Information in category A is relabeled Q when received on the right, and information in category C is relabeled P when received on the left.

6.3 Risk Factors

There are two global considerations that affect the interconnection of systems. The first is called *propagation of local risk* and the second is the *cascading problem*. Before discussing these considerations, the concepts of subsystem connection view and global network view need to be introduced.

As discussed in the previous section, any subsystem that is connected to other subsystems must enforce the Interconnection Rule. Using the subsystem connection

view, each subsystem responsible for maintaining the separation of multiple levels of information must decide locally whether or not information can be sent or received. This view, then, does not require a subsystem to know the accreditation ranges of all other subsystems on the network; only of those with which it can communicate without an intermediary.

The Interconnection Rule applies to communication between any two (or more) accredited systems. However, even when the Interconnection Rule is followed, there may be other potential security problems that will require the implementation of additional constraints on the network. In order to address these problems, it is necessary to adopt a global view of the network. This view requires a knowledge of the accreditation ranges of all the subsystems in the network. That is, it is no longer determinable locally whether or not a constraint is being satisfied. These accreditation ranges are taken into account when determining whether or not a subsystem should be allowed to connect to the network. In this way, the potential damage that can occur when information is compromised or modified can be limited to an acceptable level.

Two global concerns are discussed below. One concern is the propagation of local risk; the other is the cascading problem.

6.3.1 Propagation of Local Risk

The term *Propagation of Local Risk* comes from the notion of jeopardizing the security of a system as a result of weaknesses in other systems to which it may be connected. Table 3 in Section 4 recommends minimum classes of trusted systems for specific environments. Unfortunately, in many cases, operational needs have led to the accreditation of systems for multilevel operation that would not meet the requirements of the recommended class. While this increased risk may be accepted by the Accreditor of a particular system, connection of such a system to a network exposes users of all other subsystems in the network to the additional risk. Consequently, when an unevaluated system, or one that does not meet the class recommended for its accreditation, is proposed for connection to a network, constraints should be considered, such as one-way connections, manual review of transmissions, cryptographic isolation, or other measures to limit the risk it introduces.

In the special case of a common user network such as DDN, it may be necessary to provide communications capabilities among systems that do not conform to the security requirements established by the network Accreditor (i.e., a system meeting no security requirements may be connected to a network.) One common way to provide network service to these non-conforming systems while still protecting the other, conforming, systems would be to segregate the non-conforming systems into closed communities that could not directly communicate with conforming systems. This approach is discussed in detail in the *Defense Data Network Security Architecture* [18].

6.3.2 The Cascading Problem

One of the problems that the Interconnection Rule does not address is the *cascading problem*, discussed in Appendix C of the TNI. The cascading problem exists when an attacker can take advantage of network connections to reduce the nominal system resistance against leaking information across a range of sensitivity levels. Most multilevel systems, evaluated or not, are vulnerable to some risk that information can be leaked from a higher to a lower level supported on the system. The accreditation range of a subsystem represents a judgment that the risk is acceptable for that range of classifications. The size of the range is one indication of the attractiveness of the system as a target, so larger ranges call for more care in system design and management. In particular, Section 4 of this guideline discusses computation of a risk index calculation based on the accreditation range, and recommends a minimum evaluation class for a given risk index.

The cascading problem results from the observation that subsystems may be connected in such a way that the network covers a larger sensitivity level range than the individual systems are accredited to handle. Depending on the actual topology of the interconnection and the characteristics of the installations, the amount of effort required for an attacker to take advantage of residual vulnerabilities may be less than what is required for the network sensitivity range.

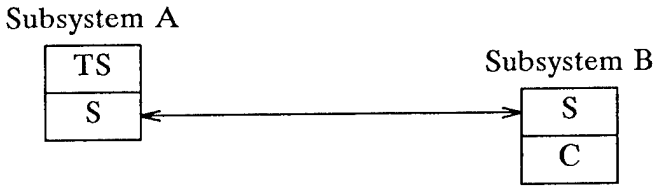
To see how this is possible, consider two systems, each of which is accredited to handle two adjacent classifications of information, as shown in Figure 9. Subsystem A processes Secret and Top Secret information, and all users are cleared to at least the Secret level. Subsystem B processes Confidential and Secret information, and all users are cleared to at least the Confidential level.

The network as a whole has three levels of information. However, the leakage resistance of the network is only that offered by two systems qualified for only two levels. To make Top Secret information available to Confidential users, an attacker might attempt to:

1. Install a Trojan horse in Subsystem A to leak some Top Secret information to Secret
2. Send that information across the network link to Subsystem B
3. Install a Trojan horse in Subsystem B to leak the original Top Secret information, now labeled Secret, to Confidential.

The path from Top Secret in Subsystem A to Confidential in Subsystem B is referred to as a cascading path, with three steps. Step 1 is from TS to S in Subsystem A, Step 2 is the network link, and Step 3 is from S to C in Subsystem B. Steps (1) and (3), the downgrading steps, offer resistance commensurate with strictly smaller ranges. Step (2), the network link, offers no additional resistance, given that the two Trojan horses have been written and installed.

Figure 9
Cascading Problem



The question is, whether subverting two systems qualified for two levels of information is as hard as defeating one system qualified for three levels of information. In some cases it might be. Lee [19] gives an argument that if two systems have probabilistically independent flaw sources, "...the resistance to threat of a cascade of two B2 systems is approximately the same as, or even better than, that of a B3 system."

But Lee also remarks that demonstrating effective independence of flaw sources in a practical case is not easy, and that two systems may have the same or equivalent flaws, particularly if their TCBs are the same, or are separate implementations of a

single flawed design. Exploitation of the flaws on two or more systems does present additional resistance to the attacker, but it should be kept in mind that physical access to all interconnected systems is not necessary to send untrusted software to them, as our experience with viruses shows unmistakably.

6.3.2.1 Tests for Cascading. For a relatively large and complex interconnection of systems, it might not be obvious whether a cascading problem exists. Appendix C of the TNI includes three approaches, with different degrees of complexity and precision, for recognizing a potential cascading problem. These range from a simple test that is rather pessimistic, called the *nesting condition*, to a complex procedure. Appendix A of this TNIEG reviews the nesting condition, and presents additional information concerning tests for the cascading problem.

Whichever test for cascading is employed, its result is to focus attention on certain subsystems and their network connections that might potentially be subject to a cascading threat. The next step is to determine whether the systems involved are actually vulnerable to the multiple coordinated attack that is necessary for cascading, and, if so, to consider countermeasures.

6.3.2.2 Solutions. There are several ways to tackle a cascading problem. Since cascading depends on cooperative action by malicious software on the participating subsystems, one approach is to institute configuration controls to prevent installation of unscrutinized software, or perhaps isolating it from network usage.

Another solution is to use a more trusted subsystem at appropriate nodes in the network, so that an attacker will be forced to overcome a protection mechanism commensurate with the seriousness of the potential compromise. In Figure 9, for example, if either subsystem A or subsystem B is NCSC-evaluated at class B3, which is sufficient according to Table 3 in Section 4 of this guideline for a range of Top Secret to Confidential, then the attacker is presented with an acceptable level of difficulty.

A cascading threat can also be interdicted by eliminating certain network connections, to break paths by which an attacker could compromise information with insufficient resistance. This solution is practical only when the links to be eliminated are not needed for operational reasons. Sometimes end-to-end encryption can be used

to address a cascading threat while preserving necessary connectivity, by reducing the level of information available to intermediate systems on a communication path.

APPENDIX A

Tests for the Cascading Problem

The cascading problem was discussed in Section 6. This appendix reviews the approaches presented in Appendix C of the TNI for testing whether a cascading problem exists in an interconnection of accredited subsystems. Three criteria are given there: the nesting condition, the cascade condition, and a heuristic procedure. The nesting condition is a simple but pessimistic test that can, in some cases, dismiss the possibility of a cascading problem. When it fails, there is not necessarily a cascading problem; other, more accurate, tests should then be applied to confirm and locate it. This appendix first summarizes the nesting condition, and then discusses other approaches briefly. A forthcoming report will provide further guidance on computational approaches for the cascading problem.

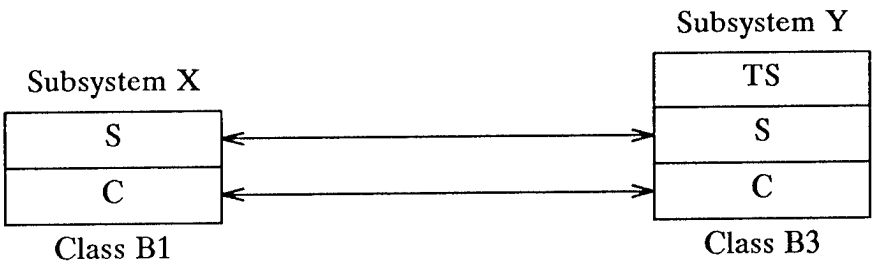
A.1 Nesting Condition

The nesting condition is evaluated solely on the basis of the accreditation ranges of the subsystems. *In the form given both here and in the TNI, it is applicable only when all sensitivity levels are totally ordered* — that is, if they can be placed in order such that each one is higher than the one before it. This is true, in particular, if they are pure classifications, with no categories or compartments.

The nesting condition is satisfied, by definition, if the accreditation ranges of each pair of subsystems are either disjoint or nested. A pair of accreditation ranges is disjoint if they have no levels in common. They are nested if one range is included (as a subset) in the other. All possible pairs (not just those of adjacent subsystems) must be considered, but some pairs may be nested while others are disjoint.

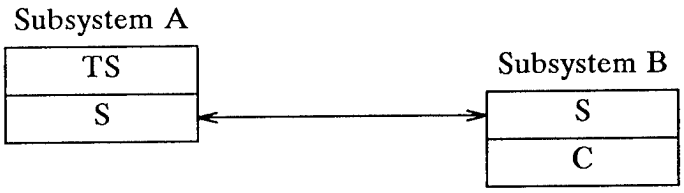
If the nesting condition is satisfied, there is no cascading problem. Because the nesting condition does not take into account which network subsystems are actually connected to one another, it can sometimes give a pessimistic result, i.e., there are cases when the nesting condition fails, but there is actually no cascading problem.

Figure A-1
Accreditation Ranges of Two Interconnected Subsystems



Example 1: Consider the situation illustrated in Figure A-1. The accreditation range of Subsystem X is nested within that of Subsystem Y (i.e., C-S is completely contained within C-TS). Therefore, the nesting condition is satisfied, and there is no cascading problem.

Figure A-2
Cascading Problem



Example 2: Consider the situation illustrated in Figure A-2. The accreditation ranges of Subsystem A and Subsystem B are not disjoint; neither is one completely contained within the other. Therefore, the nesting condition fails, and a cascading problem is possible. Note, however, that the nesting condition would still fail even if the two subsystems were not connected to one another, yet in that case there would be no cascading problem.

The situation is more complex when sensitivity levels are drawn from a partially ordered set, so that the accreditation ranges of some subsystems have sensitivity levels that are incomparable. Two sensitivity levels are incomparable when neither is greater than or equal to the other. Sensitivity levels with category sets are, in general, incomparable. An extended form of the nesting condition has been devised that applies to partially ordered sensitivity level sets . [20]

A.2 Other Approaches

Appendix C of the TNI contains two other criteria for the cascading problem: the cascade condition, which is a mathematical characterization of the problem, and a heuristic procedure. These criteria have been superseded by improved methods since the publication of the TNI. The new approach is described in a separate report, in order to give adequate scope to the presentation of background and context necessary to apply it appropriately.

The need for a new approach arose from a recognition of the limitations of the existing criteria. The cascade condition is accurate but it is not, in itself, a computational procedure. It is limited by its assumption that all of the interconnected subsystems have been given evaluation classes. The heuristic procedure is believed to provide a conservative approximate test for cascading, but only when applied to interconnections in which all communication paths are two-way, i.e., capable of both sending and receiving. A simpler procedure is now available.

[This page intentionally left blank.]

APPENDIX B

Background References

Neither the TNI nor this TNIEG contain tutorial information on security and networking; it is assumed that the reader will have some background in both areas. There is considerable literature available. Following are some references that provide background and related information concerning security in networks:

1 M. D. Abrams and H. J. Podell, *Computer and Network Security, a Tutorial*, IEEE Computer Society Press 1987.

2 D. W. Davies and W. L. Price, *Security for Computer Networks*, John Wiley & Sons 1984.

3 D. E. Denning, *Cryptography and Data Security*, Addison-Wesley 1983.

4 M. Gasser, *Building a Secure Computer System*, Van Nostrand Reinhold Company 1988.

5 International Standards Organization, *Information Processing Systems - Open System Interconnection - Basic Reference Model*, 15 October 1984. International Standard 7498.

Part 2: *Security Architecture*, February 1989. ISO 7498-2-1988(E).

6 Charles P. Pfleeger, *Security in Computing*, Prentice-Hall 1989.

7 Andrew S. Tanenbaum, *Computer Networks, Second Edition*, Prentice-Hall 1988.

[This page intentionally left blank.]

APPENDIX C

Encryption

Many networks today use or plan to use encryption as a fundamental mechanism for providing security services. The encryption devices provide a security perimeter at the protocol layer at which they provide service (typically the Network or Transport Layer). This section presents some information on how an encryption system can be part of the NSAD. It discusses MAC and DAC, use of encryption to reduce the number of AIS, and the risk index of the encryption system.

C.1 Use of Encryption

As indicated in the TNI, an encryption mechanism is evaluated differently than other mechanisms. Evaluating encryption mechanisms has a long history predating the TNI. Evaluation of an encryption mechanism is part of COMSEC. Generally, encryption mechanisms receive a rating of the highest level of classified information which may be protected using that mechanism. Therefore, the only rating applicable to an encryption mechanism is the classification level of the information that is to be protected. This classification level also establishes the requirement.

In general, organizations using the TNI and this document select their encryption mechanisms from a list provided by an organization which is responsible for evaluating such mechanisms. In many cases, that organization is the NSA.

A more complicated situation exists when encryption is employed above the Link Protocol Layer, layer 2. At layers 3 and 4 the protocols are concerned with the end systems or intermediate devices (e.g., hosts, network switches) that the links connect. Higher layers are concerned with other peer entities. Traditionally, encryption applied above layer 2 has been termed *end-to-end encryption*, or E^3.

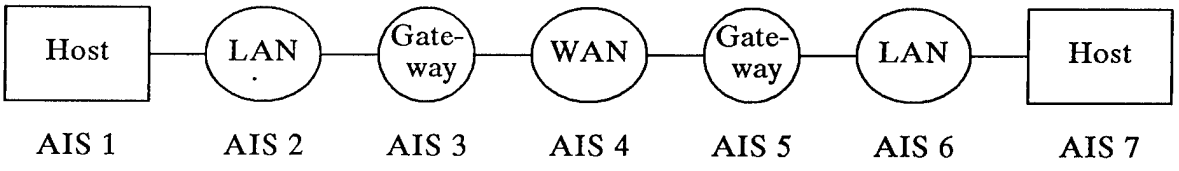
An E^3 system may be provided as (part of) an NTCB. When the E^3 system is integral to the NTCB, the use of the E^3 system requires evaluation under the TCSEC with interpretations in the TNI. The evaluation must consider (1) the accreditation

range of the user interface, (2) the risk index for the bypass in the E^3 device, and (3) the risk index between the highest sensitivity data and the lowest clearance of user on the network.

Depending on the design, devices of an E^3 system may satisfy all requirements for a system evaluated under Part I of the TNI. MAC may be provided either explicitly or implicitly. Explicit MAC is provided if the packets sent by the encryption device include a security label. Implicit MAC is provided if the security level must be inferred from the encryption key used to protect the data. All data protected by that key must be classified at a single security level.

DAC is often provided in an E^3 system as well. Typically, keys for exchanging data are provided to the E^3 devices only after DAC has been applied. The encryption devices can provide identification and authentication. While identification is generally done explicitly (by transmitting an identifier), authentication can be done implicitly (i.e., by the use of a unique key). The encryption devices may perform certain types of auditing as well. Typically, a device collects information and forwards it to another device for storage. Information collected may include: connections established, connections refused, packets with inappropriate labels, and misrouted packets. The granularity provided by these E^3 mechanisms is determined by the protocol layer at which the service is offered.

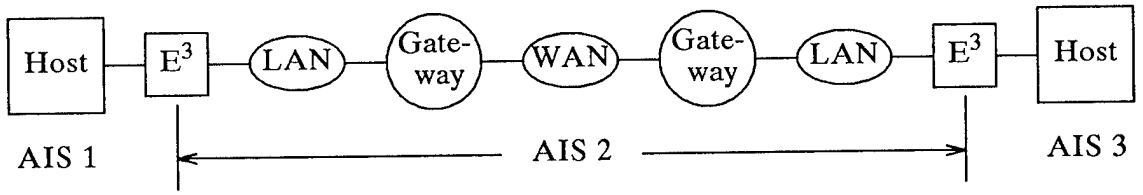
Figure C-1
Typical Interconnected AIS



In a typical network there will be a number of AIS. For example, two hosts are often attached to separate local networks connected by a wide area network (WAN). As shown in Figure C-1, the path between the hosts (without E^3) may involve 7 separate interconnected AIS.

E^3 can help reduce the number of AIS. By placing E^3 devices between each host and the LAN to which it is connected and incorporating suitable key distribution components, the LANs and WAN collapse into a single network system and the path now traverses only three AIS, as shown in Figure C-2. AIS 2 provides security services to the hosts, therefore, it may be part of the NTCB.

Figure C-2
Using End-to-End Encryption to Reduce Number of AIS



There may be a hierarchy of trusted system views. For example, E^3 may be provided at protocol layers 3, 4, and 7. Depending on the architecture, the layers of E^3 could constitute a single NTCB or each could be a separate NTCB. In the latter case, the devices supporting different layers would be part of different AIS and the interconnection rules would be applied between higher and lower protocol layers.

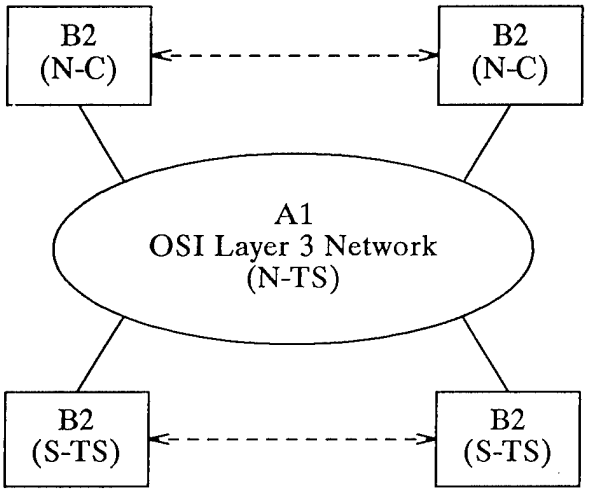
In general, an AIS at a higher protocol layer encompasses more devices than one at a lower protocol layer. The granularity of services offered is also finer at the higher protocol layer.

In a situation where the higher protocol layer encryption system also has a higher evaluation class, the lower protocol layers might be considered less trusted just as current E^3 designs treat the subnetwork as untrusted. Continuing the analogy, just as certain physical security requirements are imposed on the untrusted subnetwork, the higher protocol layer encryption might rely on characteristics of the lower protocol layers.

However, one may be faced with a dilemma that the higher-protocol-layer E^3 system has a lower security evaluation than the lower-protocol-layer trusted system. For example, a WAN with E^3 at layer 3 might be evaluated A1. The system might also provide E^3 at layer 4, but an NTCB that includes layer 4 might only be rated B2. In

this case, treating the subsystems constituting the separate layers as separate AIS and using the Interconnection Rule to accredit the network as a whole could prove advantageous, as illustrated in Figure C-3.

Figure C-3
Separate Layers Treated as Separate AIS



C.2 Encryption Mechanisms

In a trusted AIS, the recommended evaluation class is determined using a risk index based on the highest data classification and the lowest user clearance. In considering an E^3 subsystem in a network, three separate indexes must be considered [21]:

1. **The subscriber's range of sensitivity levels.** The cleartext side of the encryption subsystem must be sufficiently trusted to maintain separation among the cleartext data streams sent and received by the subscriber attached to the encryption subsystem. A risk index is based on the highest and lowest sensitivity levels sent or received by the subscriber through this encryption subsystem.
2. **The bypass.** In an E^3 system, protocol control information must be sent around the encryption unit through a bypass. The software and hardware to

implement the bypass must be trusted not to send user data through the bypass. A risk index can be computed based on the difference between the sensitivity level of the cleartext information and the sensitivity level of the untrusted subsystems of the network.

3. **The range of sensitivity levels across the network.** This risk index is concerned with the difference between the highest level of information on any host attached to the network and the lowest clearance of a user that could potentially get access to that information. Depending on the characteristics of the network, this risk index could be larger than either 1. or 2. above. The worst case scenario occurs when some users have lower clearances than the level at which the network backbone is physically protected. For example, there are currently plans to allow some uncleared users on the DISNET segment of the DDN [22] which will be physically protected at the Secret level. In that case, the risk index for the bypass works the opposite of the normal case: the ciphertext side will be the higher of the two ratings.

The subsystem which performs access control and key distribution must also be concerned with this risk range since improper key distribution could lead to compromise across the entire network. An erroneous distribution could potentially permit the lowest cleared user to access the highest classification of information.

[This page intentionally left blank.]

LIST OF REFERENCES

1. Department of Defense Computer Security Center, *Computer Security Requirements — Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments*, 25 June 1985. CSC-STD-003-85
2. Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, 15 August 1983. Department of Defense 5200.28-STD
3. National Computer Security Center, *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, Version 1*, July 1987. NCSC-TG-005
4. Department of Defense, *Security Requirements for Automative Data Processing (ADP) Systems*, March 1988. Department of Defense Directive 5200.28
5. National Computer Security Center, *Trusted Product Evaluation, A Guide for Vendors*, draft 1 March 1988 (or most recent edition). NCSC-TG-002, Version-1
6. National Security Agency, *Information Security Products and Services Catalogue*, (quarterly updates).
7. National Institute of Standards and Technology, United States Department of Commerce, *Guideline for Computer Security Certification and Accreditation*, 27 September 1983. FIPS PUB 102
8. V. A. Ashby, Thomas Gregg, and Annabelle Lee, "Security Approach for Rapid Prototyping in Multilevel Secure Systems," *Fifth Annual Computer Security Applications Conference*, December 1989.
9. International Standards Organization, *Information processing systems — Open Systems Interconnection — Basic Reference Model*, 15 October 1984. International Standard 7498
10. Defense Intelligence Agency, *Security Manual for the Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U), Supplement to Director of Central Intelligence Directive (DCID) 1/16 (U), SECRET*, 19 July 1988.
11. National Institute of Standards and Technology, United States Department of Commerce, *Guideline for Automatic Data Processing Risk Analysis*, August 1979. FIPS PUB 65
12. T. E. Bell, "Managing Murphy's Law: Engineering a Minimum-Risk System," *IEEE Specrtum*, pp. 24-27, June 1989.
13. National Computer Security Center, *Proceedings of the 1988 Computer Security Risk Management Model Builders Workshop*, Fort Meade, MD, May 1988.
14. Sammy Migues, "A Guide to Effective Risk Management," *Third Aerospace Computer Security Conference Proceedings*, December 1987.
15. Carl E. Landwehr and H.O. Lubbes, *An Approach to Determining Computer Security Requirements for Navy Systems*, 13 May 1987.

16. International Standards Organization, *Information Processing Systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*, October 1988 . International Standard 7498-2-1988(E)

17. Ingrid M. Olson, Eugene F. Troy, Milan S. Kuchta, and Brian W. McKenney, "Disclosure Protection of Sensitive Information," *13th National Computer Security Conference Proceedings*, 1-4 October 1990.

18. Robert W. Shirey, "Defense Data Network Security Architecture," *Computer Communication Review*, April 1990.

19. T. M. P. Lee, "Statistical Models of Trust: TCB's vs. People," *IEEE Symposium on Security and Privacy*, 1989.

20. Jonathan K. Millen and Martin W. Schwartz, "The Cascading Problem for Interconnected Networks," *Fourth Aerospace Computer Security Applications Conference Proceedings*, December 1988.

21. R. W. Shirey and S.I. Schaen, "ARCHWAY Program Preliminary Planning," MTR-87W00093-02, The MITRE Corporation, December 1987. Not currently in the public domain.

22. G. R. Mundy and R. W. Shirey, "Defense Data Network Security Architecture," *MILCOM '87 Proceedings*, 21 October 1987.

ACRONYMS

ADP	Automatic Data Processing
AIS	Automated Information System
ASD	Assistant Secretary of Defense
AUTODIN	Automated Digital Network
BI	Background Investigation
C	Confidential
C&A	Certification and Accreditation
COMPUSEC	Computer Security
COMSEC	Communications Security
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CSS	Central Security Service
C^3I	Command, Control, Communications, and Intelligence
CSSI	Computer Security Subsystem Interpretation
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DCA	Defense Communications Agency
DDN	Defense Data Network
DIA	Defense Intelligence Agency
DISNET	Defense Integrated Secure Network
DOD	Department of Defense
DODD	Department of Defense Directive
DOS	Denial of Service
E^3	End-to-end Encryption
ENQ	Enquiry
EPL	Evaluated Products List
FIPS PUB	Federal Information Processing Standards Publication
GOSIP	Government OSI Profile
I&A	Identification and Authentication
INFOSEC	Information Security
IPC	Inter-Process Communication
ISO	International Standards Organization
ISSO	Information System Security Officer
JCS	Joint Chiefs of Staff
LAN	Local Area Network
MAC	Mandatory Access Control

MLS	Multilevel Secure
MOA	Memorandum of Agreement
MOR	Memorandum of Record
N	Not Classified but Sensitive
NACSI	National Communications Security Instruction
NCSC	National Computer Security Center
NDI	Non-Development Item
NIU	Network Interface Unit
NSA	National Security Agency
NSAD	Network Security Architecture and Design
NSAP	Network Service Access Point
NTCB	Network Trusted Computing Base
OSI	Open System Interconnection
OT&E	Operational Test and Evaluation
PDS	Protected Distribution System
PDU	Protocol Data Unit (a.k.a. packet, datagram)
POSIX	Portable Operating System Interface for Computer Environments
RFP	Request for Proposal
RI	Risk Index
S	SECRET
SBI	Special Background Investigation
SCI	Special Compartmented Information
SDNS	Secure Data Network System
SH	System High
SIOP-ESI	Single Integrated Operational Plan-Extremely Sensitive Information
ST&E	Security Test and Evaluation
STS	Single Trusted System
TCB	Trusted Computing Base
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TEMPEST	(Not an acronym)
TNI	Trusted Network Interpretation
TNIEG	TNI Environments Guideline
TS	TOP SECRET
TSAP	Transport Service Access Point
WAN	Wide Area Network

U.S. GOVERNMENT PRINTING OFFICE : 1990 0 - 274-353 : QL 3

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION **UNCLASSIFIED**	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT **UNLIMITED DISTRIBUTION**
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) **NCSC-TG-011**	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION **National Computer Security Center** 6b. OFFICE SYMBOL (*If applicable*) **C8**	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (*City, State and ZIP Code*) **ATTN: C81** **9800 Savage Road** **Ft. George G. Meade, MD 20755-6000**	7b ADDRESS (*City, State and ZIP Code*)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (*If applicable*)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (*City, State and ZIP Code*)	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT NO.
11. TITLE (*Include Security Classification*) **Trusted Network Interpretation Environments Guideline**	
12 PERSONAL AUTHOR(S)	
13a. TYPE OF REPORT **Final** 13b. TIME COVERED FROM ____ TO ___	14. DATE OF REPORT (*Yr, Mo., Day*) **900801** 15. PAGE COUNT **75**
16. SUPPLEMENTARY NOTATION **Library No.: S235,465**	

17. COSATI CODES			18. SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUB. GR.	**NCSC; TCSEC; TNI; TNIEG; Network Security; TCB; NSAD; AIS; Cascading; Interconnection**

19. ABSTRACT (*Continue on reverse side if necessary and identify by block number*)

The Trusted Network Interpretation Environments Guideline -- Guidance for Applying the Trusted Network Interpretation provides insight into the issues relevant when integrating, operating, and maintaining trusted computer networks. The TNIEG identifies the minimum security protection required in different network environments such that network certifiers, integrators, and accreditors can determine what protection mechanisms and assurances are minimally required in specific network environments.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED DISTRIBUTION	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED	
22a. NAME OF RESPONSIBLE INDIVIDUAL **BLAINE W. BURNHAM**	22b. TELEPHONE NUMBER (*Include Area Code*) **(301)859-4463**	8b. OFFICE SYMBOL **C81**

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE