Reference Guide for Security in Networks

This reference guide is provided to aid in understanding security concepts and their application in various network architectures. It should not be used as a template for network security plans or network security approvals. It is not a compliance document.

This reference guide discusses security concerns of networks by type and mode of operation. The level of security applied in a network should be determined by the mode of operation and complexity of the network. While examples of methodology and devices for securing networks are provided, these are in no way intended to represent the only acceptable methods for securing a network.

A. NETWORK SECURITY CONCEPTS

1. Types of Networks . Networks are accredited either as a Unified Network or as an Interconnected Network.

   a. Unified Network . A Unified Network is a collection of ISs or network systems that are accredited as a single entity. A unified network should :

      (1) Have a readily understandable network security architecture and design.

      (2) Have a single security policy.

      (3) Represent a single security domain.

      (4) Be administered by a single authority (ISSO).

      (5) Have a well defined perimeter encompassing all its hardware, software, and attached devices.

      (6) Have a well understood boundary that includes all its users.

      (7) Have an overall mode of operation.

   Special-purpose components, such as guards and filters, (Controlled Interfaces) may be applied to improve the security of a unified network. Its hosts should be physically protected in accordance with the sensitivity of information processed, and its links should be physically protected (See NSTISSI 7003) or encrypted, with NSA grade encryption products.

   b. Interconnected Network. An Interconnected Network is comprised of separately accredited ISs and/or unified networks, each of which maintains its own intra-IS services and controls, protects its own resources, retains its individual accreditation, and has its own ISSO. The interconnected network must have an identifiable Security Support

Structure (SSS) capable of adjudicating the different security policy (implementations) of the participating ISs or unified networks (e.g., each may handle security labels differently). An interconnected network requires accreditation—even if so simple as an addendum to the MOU/MOA.

(1) A network of interconnected ISs or unified networks should have an understandable approach to security across the interconnected whole. That understanding should be documented in an MOU/MOA (or addendum thereto), if required, between/among the accreditors of the contributing (separately accredited) systems which have agreed to exchange classified information, or a Network Security Profile if DSS is the Accreditor.

(2) There are two basic approaches to the interconnection of networks. Either they are **directly** connected or **indirectly** connected.

(a) If they are **directly connected**, there are three basic architectural choices for the SSS needed to adjudicate the security policy and implementation differences between or among them.

i. The SSS may be separately identifiable hardware, software and firmware which is dedicated to the sole function of providing the secure interconnection of the contributing systems. This would be seen as a gateway, or Controlled Interface (CI); it might be as simple as a network server (all of whose users are independently accredited systems or unified networks).

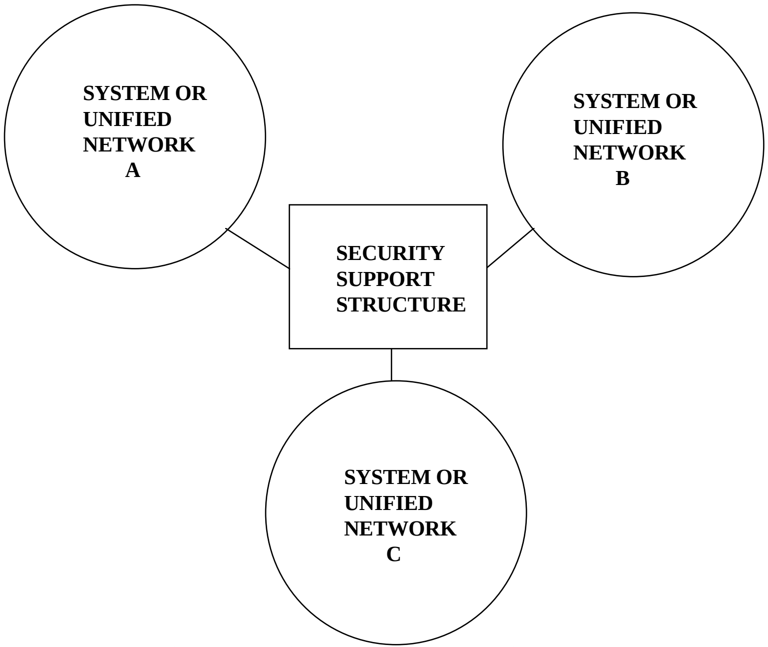
SYSTEM OR UNIFIED NETWORK A
SYSTEM OR UNIFIED NETWORK B
SECURITY SUPPORT STRUCTURE
SYSTEM OR UNIFIED NETWORK C

Figure 1. Separate Security Support Structure

ii. The SSS may be a (sub)set of the trusted computing base of one of the contributing systems (“non-distributed”).

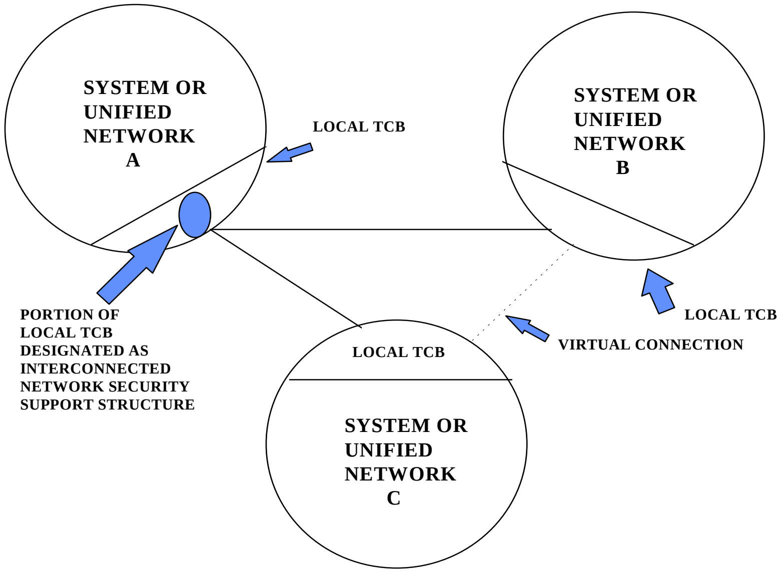
SYSTEM OR UNIFIED NETWORK A
LOCAL TCB
SYSTEM OR UNIFIED NETWORK B
PORTION OF LOCAL TCB DESIGNATED AS INTERCONNECTED NETWORK SECURITY SUPPORT STRUCTURE
LOCAL TCB
LOCAL TCB
VIRTUAL CONNECTION
SYSTEM OR UNIFIED NETWORK C

Figure 2.   SSS function provided by one member

iii. The SSS may be a (sub)set of the trusted computing base of more than one of the contributing systems (distributed).

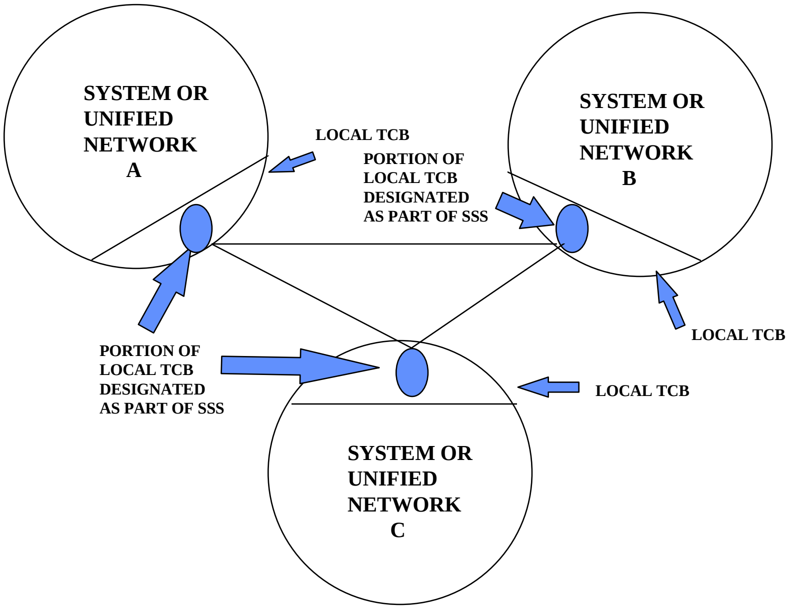
SYSTEM OR UNIFIED NETWORK A
LOCAL TCB
PORTION OF LOCAL TCB DESIGNATED AS PART OF SSS
SYSTEM OR UNIFIED NETWORK B
LOCAL TCB
PORTION OF LOCAL TCB DESIGNATED AS PART OF SSS
LOCAL TCB
SYSTEM OR UNIFIED NETWORK C

Figure 3. Distributed Security Support Structure

(b) In any case the SSS should be documented and separately accredited (from the contributing systems); that documentation and accreditation may be as simple as the data in an MOU/MOA between accrediting authorities for the contributing systems (or an attachment thereto), or could be a very complex SSP, depending on the situation.

(c) If unified networks and/or ISs are indirectly connected (to form an interconnected network), some intermediate information system (a Separately Accredited Network (SAN)) is providing interconnection service (see figure 4). In this case the accreditors of the systems intending to share data and resources through the intermediate network should:

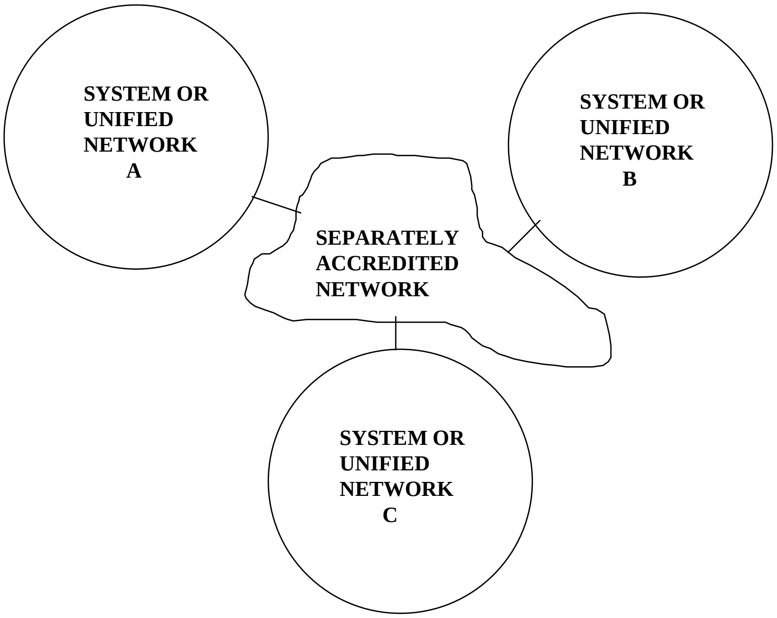
SYSTEM OR UNIFIED NETWORK A
SYSTEM OR UNIFIED NETWORK B
SEPARATELY ACCREDITED NETWORK
SYSTEM OR UNIFIED NETWORK C

Figure 4. Use of Separately Accredited Network

i. Execute an MOU/MOA documenting their intentions, necessary data exchange and access restrictions and mechanisms, and appropriate agreements concerning mutual notification of security relevant events.

ii. Independently satisfy the accreditor of the <u>intermediary</u> system that their systems satisfy the intermediate SAN requirements (e.g. the SIPRNET or other Defense Information Systems Agency network) for connection; this should be formally documented.

(d) In an interconnected network, the SSS is either a subset of one or both (or all) of the client unified networks or ISs which are <u>using</u> the SAN as a medium of convenience.

(e) For purposes of examining the security of the overall interconnected network, the SAN is considered a subset of the interconnected whole and is limited to those components required for network operations (e.g., transmission medium, network interface components of a host computer, packet switches, access control centers, technical control devices, and gateways).

i. A SAN has a prescribed perimeter and boundary and is separately accredited for a specified mode of operation.

ii. In contrast to an IS or unified network, the SAN's mode is defined solely by the sensitivity of the data to be introduced into the SAN by its subscriber ISs. For example, a PL-1 or PL-2 mode SAN transmits information at a maximum classification level (such as TOP SECRET) along with any specific compartments and special access programs. Each attached IS or network sends or receives information to or from the SAN at the same level of sensitivity or classified level. A PL-1 mode SAN may have any combination of PL-1, PL-2 or PL-3 mode IS subscribers attached to it as long as they are only transmitting the same level of data.

iii. A SAN should transmit data accurately and in a timely fashion, not disturb the security parameters attached to data, and not disturb the association of the security parameters with the data to which they are attached. The SAN security policy will be agreed upon by the DAA of the SAN and the DAA of each subscriber IS.

2. Security Architecture and Design—A network should possess an understandable security architecture and design that addresses the security services of the network. The architecture and design documentation should specify the types of components in the network, which ones are trusted, and in what way they will cooperate to support network security objectives. Depending on the particular environment, communications security (COMSEC), emanations security (TEMPEST), physical security, personnel security, administrative security, and other information systems security (INFOSEC) measures or safeguards should also be incorporated.

B. CONCERNING INTERCONNECTING ISs AND NETWORKS

Several conditions should be considered before an interconnection of ISs and networks can be achieved to allow secure ISs or networks to communicate without reducing their inherent security. Methodology other than the examples included below are possible.

l. Memorandum of Understanding/Agreement (MOU/MOA). If more than one DAA is involved in a network, an MOU/MOA should be prepared and signed by all parties as a means of establishing the appropriate security parameters and understanding. An overall cognizant security authority may be agreed upon. The cognizant security authority would coordinate handling practices and the classification levels that may be exchanged between the ISs or networks connected. The MOU/MOA would become a part of the accreditation documentation of each DAA's system.

2. Agreed Accreditation Ranges or Security Parameters. Agreements may be expressed either in terms of (1) accreditation range or (2) accredited security parameters. Individual ISs and networks may be accredited to handle classified information at a single security classification level or within a range of classification levels (i.e., accreditation range). Individual ISs or networks may also be accredited to operate in terms of an accredited security parameter or a specific set of security parameters—a set of security classification levels, compartments, and sub-compartments.

3. Types of Data Exchange. The data exchange rule states that no system may send data to another system that is not accredited to receive that data. This rule may be expressed in two ways in terms of the accreditation range or in terms of the accredited security parameters as follows:

   a. The accrediting authorities would agree upon the categories of information that may be exchanged between their interconnected ISs or systems. These categories may not exceed the accreditation range or accredited security parameters common to the connected ISs or systems.

   b. The sensitivity level of data that may be exchanged between ISs will have the same accredited security parameters, or fall within the overlap range of the subset of accredited security parameters, for the subject ISs. Thus for interconnected PL-1 or PL-2 ISs, the sensitivity level of the data will be equal to the common Accredited Security Parameters (ASP) for the interconnection. For interconnected PL-3 ISs, the sensitivity level of the data packets will fall within the overlap range of the subset of accredited security parameters.

   c. On one-way links (i.e., links that provide no acknowledgment), data may be transmitted from one IS to another without common accredited security parameters, provided the data transfer service is guaranteed to be unidirectional and the accredited security parameters or subset thereof of the receiving IS dominates that of the sending IS (i.e., the receiving IS has accredited security parameters or subset with a greater or equivalent hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET and is accredited for the non-hierarchical categories (compartments). For example, a PL-3 system with a subset of accredited security parameters of TS+TS/AB may send data labeled TS/SI data to a PL-2 IS with an ASP of TS/AB/XY.

   d. To enforce these above rules, either the ISs or specialized security components should implement data-flow controls based on the sensitivity labels of the devices and data involved.

4. Upgrading. If there is a network change in the classification level and/or compartments, or if user access levels change as a result of an interconnection, the AIS may require accreditation

in a higher mode of operation. Additionally, security features may require upgrading relative to the services to be provided by connected ISs, brokers (e.g.,CI's, guards or filters), or the communications services. For example, if a PL-1 mode IS is to be connected to a PL-3 mode IS, the levels of user access in the dedicated IS will change. Consequently, the PL-1 AIS may require upgrading to PL-2 mode to enforce discretionary access controls (DAC) being enforced in the PL-3 IS. Additionally, data-flow control typically needs upgrading. For example, connecting two ISs having a common ASP or SUBSET OF ACCREDITED SECURITY PARAMETERS, but different modes of operation, may require additional data-flow control mechanisms to prevent improper data exchanges between them. Special-purpose components, such as Controlled Interfaces, guards and filters, may be incorporated to improve the security of an otherwise unacceptable system.

5. Communications Protocols. Communications protocols should provide the security features necessary for accurately transmitting information from the source IS to the destination IS, regardless of the number of intermediate points that handle the information. These protocols may also cover such requirements as:

   a. Security Labels—reliably associating a security label with communicated data.

   b. Device Labels—supporting device labels and the enforcement of the data-flow controls.

   c. Integrity—detecting altered information to provide warning of equipment failure or unauthorized modification of transmitted data. For example, the data link protocol could provide an integrity check mechanism such as a cyclic redundancy check (CRC) value to verify the integrity of data and labels transferred between systems.

   d. Identification and Authorizations—supporting the passing and protection of user identifiers and authorizations across the network.

   e. Trusted Path—supporting a trusted path across the network.

6. Compatibility of Security Mechanisms. Whenever two ISs are connected, security mechanisms, especially access control mechanisms, should be examined for compatibility and uniformity. To enable processes to access resources in two systems, a gateway (Controlled Interface) may be necessary to translate resource access requests expressed in terms of one protocol into requests expressed in terms of the other.

7. Connecting to a Separately Accredited Network (SAN) e.g. the SIPRNET. Before an IS is connected to a SAN, it should be verified to operate in a manner consistent with the SAN's security policy and mode of operation. Before attaching a new IS, the SAN security policy and interface requirements should be examined to determine whether the new connection would create any exception(s) to the security policy of the interconnected network.

8. Anti-Cascading. A user should be prevented from taking advantage of interconnections to circumvent defenses protecting against the leakage of information from one compartment to another in a system. If the composite range of security levels of the interconnected systems is greater than the range of any one of the connected systems, the risk of leakage may increase while the defense remains constant. In such a case, additional defense mechanisms should be applied.

9. Internetworking. When several networks are connected (e.g., interconnecting multiple LANs via a SAN), the internetwork security architecture should identify the physical architecture of the internetwork, the protocols involved, and the services and devices needed to ensure secure interconnectivity. For example, the architecture may require secure gateways (Controlled Interfaces) with restrictive routing, security features in the internet protocols, and an internet end-to-end encryption scheme. The architecture should be acceptable to all the systems in the internet.

C. CONSIDERING TRUSTED NETWORK REQUIREMENTS

This section presents some basic security considerations applicable to both unified networks and interconnected networks. The categories of requirements are derived from the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) DoD 5200.28-STD and the Security Addendum to the ISO Reference Model.

1. Discretionary Access Control. All networks should control access to addressable network resources (such as files and services) based upon the expressed wishes of its users or owners of the data. The network should validate each access attempt by a user or group of users and reject unauthorized access attempts. The TCSEC calls this discretionary access control (DAC). The ISO Security Architecture calls this identity-based security. Discretionary controls apply within defined security levels (i.e., an individual with information of a particular security level may determine whether to give it to another individual cleared to that level). An IS, when interconnected to other systems or networks, may choose to enforce a form of DAC to prevent certain information from flowing to an IS that has no need-to-know. However, this is generally not necessary since a system should always enforce DAC locally over the resources within its security perimeter. If ISs using different DAC mechanisms are interconnected, interactions between these mechanisms should not jeopardize security. If a process is to access resources in both ISs, a gateway (Controlled Interface) may translate resource access requests expressed in terms of one mechanism into the terms used by the other.

2. Mandatory Access Control. PL-3 and PL-4 mode networks should also control access to network resources on the basis of formally defined security levels assigned to information and the clearance levels assigned to individuals and processes. TCSEC calls this mandatory access control (MAC); ISO calls it Rule-based Security. Such controls are mandatory in that they cannot be selectively invoked or modified by the user. In interconnected ISs and networks, MAC should be enforced to allow ISs to connect if their accredited security

parameters sets overlap. MAC can also control user access to resources and services in other AISs. For example, a gateway (Controlled Interface) can control host communication by using access control lists that reflect the accredited security parameters of the communicating hosts. The access control mechanisms may reside in gateways or other brokering devices (Controlled Interfaces) as long as the broker's security parameters overlaps those of the connected AISs.

3. Labeling/Framing. PL-3 or PL-4 mode networks should maintain sensitivity labels for any files, processes, sessions, data packets, machine memory, or other resources that the network is expected to keep separated on the basis of sensitivity level. In interconnected ISs and networks, data packets exchanged over the interconnection should be labeled to reflect their security level. For single-level connections, all information entering and leaving the system has an explicit or implicit marking at that level. For PL-3 or PL-4 connections, all information entering and leaving the system should have an explicit security label within the range of allowable classifications and compartments assigned to the system. Labeling is necessary to identify to a receiving IS those security parameters among which the transmitting IS can reliably distinguish. For example, a PL-1 IS implicitly conveys to all recipients the understanding that it cannot reliably separate on the basis of any security parameters. If the ISs satisfy criteria for PL-3 mode, they may produce explicit labels, or the communications linkage may frame the packet with the security parameters of the sending IS. Alternatively, an accredited broker (Controlled Interface) can produce labels, a single-level communications link can be the source of an implicit label (the labeling may be performed implicitly as a consequence of the classification level at which communicating processes are running), and a link that relies on the exchange of cryptographic variables can use different cryptographic keys as a means to identify the label for a particular transmission of data.

4. Data Separation & Data Flow Control. In PL-2 mode networks, data separation is based on need-to-know parameters. PL-3 and PL-4 mode systems should reliably separate intelligence on the basis of the appropriate accredited security parameters of the network. Although separate networks and sub-networks may be used to provide such separation, the most common way is to label information and processes, and enforce mandatory access controls on the basis of these labels. When gateways, routers, and bridges are used to interconnect ISs and networks, these devices should maintain data separation and control data flows, enforcing the data exchange rules, marking data that flows from an IS with a lower sensitivity range to a more sensitive one, and restricting data transfers according to the overall security policy and the security policies of the entities involved.

5. Identification & Authentication. Networks should identify and authenticate users as well as devices to ensure that all users and devices accessing the network have the proper access approvals and need-to-know with respect to the network's mode of operation. Location and other such parameters that may be security relevant may also require authentication. When interconnecting ISs and networks, each IS should identify and authenticate individual users and workstations directly connected to its own system. When it is necessary to communicate

clearance and classification information between systems, the authenticated identification should be protected via trusted communications.

6. Trusted Communications. The transfer of Identification & Authentication information between ISs should be protected by trusted communications. This requires trusted channels that can maintain the integrity of the information sent over that channel. The requirement for trusted communications first arises in PL-2 for Privileged Users and for all Users in PL-3 mode systems. Therefore, the interconnection of ISs may involve a difference in trusted communications requirements. When this happens, only the trusted communications requirements of the lower-level IS need be met. This is because the lower-level IS will be operating over a narrower accreditation range than the higher-level IS. In such a case, the higher-level system need not rely on as strong a form of identification, authentication, and authorization (regarding the users of the lower-level IS) as it does for its own users, since it will restrict the range of classifications it will allow the lower-level system to handle.

7. Audit. PL-1, PL-2, PL-3, and PL-4 mode networks should provide sufficient information about both routine and exceptional events that subsequent investigation can use to determine whether security violations have occurred and the extent to which information or other resources have been compromised. In interconnected ISs and networks, events to be audited should be such so as to ensure end-to-end accountability for information transferred between ISs.

   a. Examples of events that should be audited include:

      (1) The establishment of sessions between ISs or networks (what hosts are talking to each other),

      (2) Security-relevant data flows (source and destination of connectionless data exchanges), and

      (3) Data spills and misrouted messages.

   b. Audit data may be collected either on an IS-by-IS basis or on a network-wide basis. The audit trail from a given system may need a classification as high as the highest level of information in that system. If possible, the audit data related to events for all systems in a network ought to be collected at a central point, such as in an audit server (e.g., there may be a server on a backbone LAN, as well as separate audit servers). Remote locations may also be audited by an audit server at the remote location, and audit data may be collected in guards, gateways, and other interconnection devices. Such devices would audit events they are expected to check, control, or implement. For example, a security guard (Controlled Interface) that controls spillage of information and controls session establishment would audit those events. A Controlled Interface that controlled traffic flow between two PL-3 domains would audit security-relevant data flows to provide information sufficient to allow reconstruction of possible information leakages and/or misrouted information. Care should be taken so audit data from different systems can be compared (e.g., time stamps should be comparable and identifiers should be unambiguous).

8. Confidentiality. Networks should protect security data including authenticators from unauthorized disclosure while such data is being transmitted through unsecured space and while in storage. In interconnected ISs and networks, communications links should be either physically protected or link encrypted. Encryption provides an important security mechanism over a physical link between two ISs. Encryption enables secure communications to pass over a path as if the path were physically protected. End-to-end encryption can also provide implicit rule-based access control (by assigning each pair of encryption keys a specific security level), explicit access control (if the packets sent by the encryption device include a security label), and need-to-know access control. Encryption can also provide identification and authentication service to ensure that a connection precludes a masquerading system.

9. Integrity. The network should provide integrity controls to detect whether security information and mechanisms have been corrupted while in storage, during processing, or in transit. In interconnected ISs or networks, all data, including security information, exchanged between ISs should be protected from corruption.

10. Assurance. Assurance is the guarantee of correctness and effectiveness based on an analysis of the way the network was developed and the way it will be used. Assurance controls provide a means of assessing whether security controls are in place, functioning, tamper-proof, and cannot be circumvented. Assurance should be considered when determining the trust associated with the network. Nine categories of assurance applicable to networks are discussed in the TCSEC—system architecture, system integrity, covert channel analysis, trusted facility management, trusted recovery, security testing, design specification and verification, configuration management, and trusted distribution.

11. Security and Network Management. To be secure, a network must be maintained properly. The interconnection of ISs or networks demands that there be a means for monitoring and controlling the various components. A user in one IS accessing services on another IS, across a backbone network, is a Customer of at least three service Providers. One central facility may be in a position to identify the source of any problems. Additionally, the network may need mechanisms that are specific to security, such as access control, audit data recording and analysis, identification and authentication, guards/filters, and trusted facility management. These mechanisms will manage the attributes, features, and associated software used for security. This includes management of authenticators (such as passwords), cryptographic materials, integrity mechanisms (such as checksums, cryptoseals, and error detection and correction), and tables and lists used for access control. For example, in a highly distributed environment, a directory service containing information about individuals, devices, and services may be essential to support the addressing, management, and control required of distributed processing functions such as a message service. Such a directory would contain authentication keys and security attributes that play a key role in the network security services.