

# **DEFENSE INFORMATION SYSTEM NETWORK**

## **LONG-HAUL BLOCK**

### **SECURITY POLICY**



**May 1999**

DISN Program Office - D21  
5111 Leesburg Pike, Suite 9177  
Falls Church, VA 22180

Summary of changes for May 1999 version.

The title of the document is changed from “Defense Information System Network (DISN) Goal Global Defense Information Systems Network Long-Haul Security Policy” to “Defense Information System Network (DISN) Long-Haul Block Security Policy.” The Executive Summary is reduced to a basic description of the contents.

Summary of changes for January 1998 version.

Corrections reflect consideration of comments on the July 1997 version. Changed Sensitive But Unclassified (SBU) terminology to Unclassified, Sensitive Information to conform to guidance in DoD 5200.1-R and DoDD 5200.28. The Executive Summary was modified to provide a clearer statement of the risk management strategy. Additional wording was added in the remaining sections to clarify that this policy is for the Long-Haul Block, the technical interface points to that block and the Transport Application and the associated information systems supporting the Transport Application.

Summary of changes for July 1997 version.

Throughout the document the abbreviations for several DISN Program documents have been corrected. References to published documents have been updated where appropriate. The reference to the DII as a component of the Defense Information System (DIS) has been corrected. Terminology has been changed from >segment= to >block= to conform with the Capstone Requirements Document terminology. Language has been added to reflect the relationship of the Long-Haul Block to other DISN blocks. Organizational name changes have been added, where appropriate. The security requirements in the Executive Summary has been shortened to provide the security features and their definitions. The security features section in the main body has been expanded with some corrections of terms. The discussion of DISN Long-Haul network management data has been separated from that of user data. Language has been added that of compilations of network management and control information must be reviewed for possible classification.

**DISN ACCREDITATION AUTHORITY APPROVAL**

**Defense Information Systems Agency**

---

Date:                      Signature:

**Office of the Joint Staff**

---

Date:                      Signature:

**National Security Agency**

---

Date:                      Signature:

**Defense Intelligence Agency**

---

Date:                      Signature:

EXECUTIVE SUMMARY ..... 1

Section 1. BACKGROUND ..... 2

    1.1 General ..... 2

    1.2 Definition ..... 4

Section 2. DOCUMENT OUTLINE..... 5

Section 3. PURPOSE and SCOPE ..... 5

Section 4. THREAT ..... 6

    4.1 Policy Statements ..... 6

    4.2 Threat assessment information applicable to DISN..... 6

Section 5. GUIDANCE ..... 7

Section 6. POLICY ..... 8

    6.1 General ..... 8

    6.2 Local Subscriber Environment (LSE)..... 9

    6.3 DISN Long Haul Boundary..... 9

        6.3.1 End-to-end information transfer network ..... 10

        6.3.2 Connections to DISN..... 10

        6.3.3 Communications through the DISN boundary ..... 10

        6.3.4 Inside the DISN Boundary..... 10

            6.3.4.1 Computer and Network Security Features ..... 11

            6.3.4.2 Integrity ..... 11

            6.3.4.3 Identification and Authentication ..... 12

            6.3.4.4 Availability ..... 12

            6.3.4.5 Non-Repudiation (Network Management Data)..... 13

            6.3.4.6 Computer Systems..... 13

        6.3.5 Personnel Security ..... 13

        6.3.6 Administrative (Procedural) and Operations Security ..... 13

        6.3.7 Physical Security ..... 14

        6.3.8 Emanations Security ..... 15

        6.3.9 Information Protection ..... 15

        6.3.10 Management..... 16

Section 7. REFERENCES ..... 16

    7.1 NATIONAL POLICY and PUBLIC LAW ..... 16

    7.2 DEPARTMENT OF DEFENSE and JOINT STAFF ..... 17

    7.3 FEDERAL AGENCIES and COMMITTEES ..... 18

    7.4 PROGRAM DOCUMENTS..... 19

APPENDIX A ..... 20

ACRONYMS ..... 20

TERMS ..... 23



## EXECUTIVE SUMMARY

This is the interim version of the *Defense Information System Network (DISN) Long-Haul Block Security Policy*. It replaces the draft version released January 12, 1998. A final version is currently under development and will be released in Fall 1999.

The DISN is composed of the Sustaining Base, the Long-Haul, and the Deployed Blocks. This security policy applies only to the Long-Haul block.

The goal of the DISN is to construct a seamless, global, secure, standards-based, information domain-to-information domain (end-to-end) capability. This capability will provide integrated, flexible, and affordable voice, data, video, and transmission services to the warfighter and support mission. Section 2 of this policy document provides DISN background information, mission function categories, and introduces the security requirements found within DISN guidance documents to which this policy is applied.

Section 3 provides the document's outline and Section 4 contains the document's purpose and scope. Section 5 discusses the DISN threat assessment process and Section 6 details the relevant guidance documents from which the DISN security requirements are generated.

Section 7 provides more detailed security policy direction. It addresses the DISN Long-Haul block boundary and the numerous security issues within that boundary. They include computer and network security, personnel security, administrative (procedural) and operations security, physical and emanations security, information protection, and security management.

Finally, Section 8 provides the national, public law, Department of Defense, DISN program, and federal guidance documents for reference.

Section 1

BACKGROUND

1.1 General.

1.1.1 The DII [Reference 7.4.7] is the seamless web of communications networks, computers, software, databases, applications, data, security services, and other capabilities that meets the information processing and transport needs of DOD users in peace and in all crises, conflict, humanitarian support, and wartime roles. It includes:

1.1.1.1 The physical facilities used to collect, distribute, store, process, and display voice, data, and imagery.

1.1.1.2 The applications and data engineering practices (tools, methods, and processes) to build and maintain the software that allow C2, Intelligence, Surveillance, Reconnaissance, and Mission Support users to access and manipulate, organize, and digest proliferating quantities of information.

1.1.1.3 The standards and protocols that facilitate interconnection and interoperation among networks and systems and that provide security for the information carried.

1.1.1.4 The people and assets which provide the integrating design, management and operation of the DII, develop the applications and services, construct the facilities, and train others in DII capabilities and use.

1.1.2 The Office of the Secretary of Defense (OSD) directed the Defense Information Systems Agency (DISA) to establish the DISN to incorporate the many disparate DOD communications subsystems into a common, interoperable telecommunications system to support all of the DOD to implement the DII network components, above. The primary objective of the DISN is to be responsive to the warfighter=s national security and defense information transfer needs. The system will also facilitate the dissemination of information while ensuring the provision of affordable services.

1.1.3 Based on this objective, the goal of the DISN is to provide a seamless, global, secure, standards-based, information domain-to-information domain (end-to-end) capability that provides integrated, flexible, and affordable voice, data, video, and transmission services to the warfighter and support mission. Intrinsic capabilities include surge capacity, security, robustness (using both military and commercial media for global operations), interoperability

with tactical and allied systems, and assured service to support military operations and national emergencies. DISN, as an integral part of the DII, provides an information transport platform that is responsive to national security and defense needs under all mission conditions in the most efficient and affordable manner, while maintaining its transparency to the users. DISN is the DOD=s primary telecommunications and information transport network, providing integrated information services worldwide. The DISN is composed of the Sustaining Base, the Long-Haul, and the Deployed Blocks. This Security Policy only addresses the DISN Long-Haul Block. The DISN Long-Haul has three segments: transport functions (switching; audio, video, and data transmission), network management, and value-added services.

1.1.4 The DISN Long-Haul communications infrastructure is viewed as being composed of point of presence connections within local subscriber environments (LSEs) [components of the Sustaining Base Block] and a wide area or enterprise network-based information transfer system. The LSEs include all devices and communication systems under user (organization) control (e.g., networks, workstation, video, voice, etc.). The LSE span also includes responsibility for providing any hardware and software associated with interfacing to the transfer system (e.g., for connecting with the point of presence router, connecting to other DISN service delivery points, and providing the proper connections in the local technical control center). The LSE point of presence router is under the control of the DISN transfer system which may also include other point-of-presence (POP) interface devices installed at or in proximity to the LSE, the communication protocols integrated into POP and enterprise level relay systems, and the infrastructure that supports the transfer functions.

1.1.5 The DISN mission is separated into three distinct functional categories, which include:

- ! Transport Application (Bearer Service) Functions - Backbone Transmission, Bandwidth Manager, Access Area, Circuit Switch, Element Manager, Standardized Tactical Entry Point, Video Teleconferencing Hub, Integrated Digital Network Exchange

- ! Network Management Functions - Management Agents, Global Operations and Security Center, Regional Control Centers/Regional Operations and Security Centers

- ! Value-Added Service Functions - Secure Video-Teleconferencing, Directory Services, Secure Voice Teleconferencing, Terminal Access, and Gateways.

1.1.6 All user data submitted to the Transport Application is assumed to be Unclassified, Sensitive Information whether encrypted or unencrypted. Users in the Sustaining Base or the Deployed Blocks (external users) are assumed to have a valid clearance for the level of classification of their information but as a minimum have clearance for unclassified, sensitive information. Appropriate encryption in the Sustaining Base or Deployed Blocks will provide

sufficient protection to treat the bit-stream in the Transport Application as unclassified, sensitive information. All support and operations personnel in the Long Haul Block will have need-to-know for the level of information processed by the respective systems they support but as a minimum they will be cleared for unclassified, sensitive information. All systems in the Long Haul Block that support any of the functions defined in paragraph 2.1.5 will encrypt or otherwise protect data inserted into the Transport Application to permit handling of the bit-stream as unclassified, sensitive information. Therefore, the Transport Application is considered to be operating in the System High Mode at the unclassified, sensitive information, level.

### 1.2 Definition.

1.2.1 This Security Policy applies to all DISN assets within the ~~global~~ DISN Long-Haul (CONUS and OCONUS) boundary (e.g., personnel, hardware, software, procedures, data, etc.). This Security Policy addresses the security requirements of specific DISN guidance including the MNS, the CRD, and CJCSI 6211.02A. Specific security requirements include the ability to:

X Provide personal, physical, and electronic protection against unauthorized access to information;

X Incorporate appropriate safeguards commensurate with the existing or projected threat, and as required by governing policies; and

X Institute operational security and facilities protection to enforce physical protection standards at DISN facilities and to ensure access to information is consistent with mission assignments and clearance levels;

1.2.2 Security requirements were also derived from applicable security documentation including Executive Order 12958, Public Law (e.g., Freedom of Information Act, Privacy Act), Department of Defense Directive (DODD) 5200.28, DISA Instruction 630-230-19, and Director, Central Intelligence (DCID) 1/16. This policy also conforms to the architecture concepts presented in the Technical Architecture Framework for Information Management (TAFIM) DOD Goal Security Architecture (DGSA) and Goal Network Management Architecture (GNMA).

Section 2

DOCUMENT OUTLINE

The background information above provides a general description of the DISN. Section 4 contains the purpose and scope for this document. Section 5 includes a description of the threat environment. Section 6 briefly discusses the sources of security requirements as derived from the appropriate doctrine and directives. Section 7 includes the security policy for the overall DISN Long-Haul Block. Section 8 includes the references. Appendix A contains a list of acronyms and terms.

Section 3

PURPOSE and SCOPE

3.1 This DISN Long-Haul Security Policy provides the security requirements and the security architecture framework for the phased development and operation of the DISN. This security policy applies to the protection of all data within the DISN Long-Haul Block and how that data crosses the DISN boundary.

3.2 This Security Policy applies to all systems and services<sup>1</sup> (voice, data, video, value-added, etc.) included in the DISN Long-Haul Block. The policies set forth in this document apply during the full range of anticipated conflict scenarios and priorities as contained in the Joint Global Command, Control, Communications, and Computer Assessment: (1) peacetime, (2) crisis, (3) mobilization, (4) armed conflict. This policy also applies to interfaces to other non-DOD organizations (e.g., Drug Enforcement Agency), non-U.S. Government organizations (e.g., American Red Cross), and non-U.S. organizations (e.g., Allies) that connect to DISN. Use of the DISN by foreign governments and allied organizations must be approved under the provisions of CJCSI 6211.02A.

3.3 This Security Policy directly applies only to the DISN Long-Haul Block and its boundary. The LSEs and other hardware, software, and resources located outside the DISN boundary are outside the scope of this security policy, except where specifically noted. Security implementation details in support of this Security Policy will be provided in the

---

<sup>1</sup> Since the word service, as employed in this Security Policy, can be used to refer to both communication and security services, this Security Policy will be specific when it references security services. As such, the term DISN services can generally be understood to refer to the communication services offered by DISN.

System Security Authorization Agreements (SSAAs) prepared after award of the DISN contracts. The SSAAs will be maintained by the DISA element responsible for implementation and will support certification and accreditation actions.

#### Section 4

#### THREAT

4.1 Policy statements, in general, are the response to threat. As examples, applicable national policies and DOD Directive 5200.28 [Reference 7.2.13] acknowledge the general threat to automated information systems (AISs) and provide minimum security requirements that must be met, either through automated or manual means. This security policy for the Long Haul Block of the DISN reflects a positive response a variety of threats present during all operational environments envisioned for this block of the DISN. Residual risks will, however, remain and are documented in the System Security Authorization Agreements (SSAA), when issued, of the respective segments that comprise the Long Haul Block of the DISN.

4.2 Threat assessment information applicable to DISN, and particularly to its nature as a commercial entity processing U.S. National Security and Emergency Preparedness (NS/EP) telecommunications includes the following:

X *Natural and Technological Disasters Threat to NS/EP Telecommunications* provides a description of the natural and technological threats to communications assets and the probability of their occurrence. [Reference 7.3.16]

X *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document* that identifies and analyzes the threat that electronic intrusion represents to a public switched network. [Reference 7.3.15]

X *An Assessment of the Risk to the Security of the Current and Near-Term Public Network* identifies and analyzes several categories of threats to the current and near-term PN. [Reference 7.3.18]

X *Asynchronous Transfer Mode (ATM) Vulnerability Analysis* identifies and analyzes potential vulnerabilities in ATM networks. [Reference 7.3.20]

X *DISN-C Vulnerability Assessment Plan* identifies possible vulnerabilities in the future DISN CONUS infrastructure. [Reference 7.3.19]

X *Defending the Defense Information Infrastructure (DII): DISA's Vision & Strategy for Defensive Information Warfare (IW-D)* identifies basic threat scenarios and the appropriate response. [Reference 7.3.14]

4.3 The Awareness Document, for example, discusses electronic intruders such as members of the computer underground, insiders, industrial spies, and foreign intelligence services, as well as their basic skills and techniques. Also discussed are targeted technologies and services such as data networks, international gateways, signaling networks, wireless systems, and other emerging technologies.

4.4 Periodically, in response to significant technological advances and international geopolitical changes, additional threat information will be released by the NCS or by the DIA and the Services and agencies (S/As).

## Section 5

### GUIDANCE

DISN security policy is driven by several layers of interconnecting and complementary guidance. The general requirements derived from this guidance are summarized below.

X Public Law - Provides direction on the use, distribution, and protection of data as well as prosecution for its misuse.

X National Policy - Provides direction on intelligence activities and the classification and dissemination of data; provides direction on the security of telecommunications systems.

X DOD Directives, Instructions, and Standards - Provides specific guidance on physical, personnel, AIS, and other security requirements.

X Joint Staff, DISA, National Communications System (NCS), and NSA guidance - Provides specific guidance on DISN and C3I systems, as well as requirements for all national priority communications systems; provides specific requirements on all areas of security and on security architecture and management.

X DISN Program Guidance - Provides information on migration of the current DISN components to the target DISN and the services and functionality to be available in the target DISN.

Specific guidance is derived from the MNS, the CRD, and CJCSI 6211.02A. DISN security policy is also driven by the threat and IW-D references listed in Section 7.

Section 6

POLICY

6.1 General. The policy discussion below makes reference to the entire DISN as a single entity in order to establish a context for the Long-Haul Block policy. The DISN Long-Haul Block provides a data transport service, carrying data between end systems. Its users in this context are the users of the end systems that connect to it. The DISN Long-Haul Block must also transport and process its own network management and control traffic. Its users in this context are the operators and administrators of the network itself. This security policy discriminates between these two operating environments by reserving the term "user" for the users of end systems connected to DISN (outside the boundary). The term "DISN support personnel" is used for identifying the personnel who operate DISN equipment and those who perform the administrative control of the network (inside the DISN boundary). There will be no capability for a user outside the DISN boundary to perform those functions assigned to DISN support personnel or in any way affect the security posture of the DISN.

6.1.1 DISN must fulfill a number of security goals (objectives) per the references given in Section 8 of this document. These goals may be achieved through a number of mechanisms such as encryption for confidentiality and digital signatures for non-repudiation. Although some mechanisms and their use within the DISN boundary are currently postulated, the selection of mechanisms to be used at and within the DISN boundary for meeting specific security policy requirements will be determined by DISA and the DISN contractors after award of the DISN contracts. Such decisions will be documented in the respective SSAA [Reference 7.2.15] for the DISN Long-Haul Block Segment or system.

6.1.2 Overall responsibility for DISN security is shared between the LSEs and the DISA. LSE responsibilities include meeting the security requirements of this Security Policy regarding their initial connection to DISN and also when bridging DISN with other networks. LSE responsibilities also include providing sufficient data protection such that the data may be safely submitted to the DISN commercial circuits. DISA responsibility includes providing sufficient DISN availability such that LSEs perceive no loss or degradation of service, and to provide a specific set of value-added services.

6.1.3 The DISN implementation will be subject to formal certification and accreditation. The Certifying Authority is the DISA INFOSEC Program Management Office (Code D25). The Designated Approving Authorities for the DISN are the DISA (Code D03), the Joint Staff (J6T), the National Security Agency (NSA/Q06), and the Defense Intelligence Agency (DIA/SYA-1).

6.1.4 The security requirements in this policy are based on the following general rules:

6.1.4.1 User data entering and leaving the Transport Application (crossing the DISN Long-Haul boundary) is assumed to be already protected by the originator and the DISN must deliver the data to the intended recipient(s). DISN, however, will further protect video and telephone conferences and provide data confidentiality, as described above.

6.1.4.2 Users outside the DISN Long-Haul boundary will not be able to view or manipulate Transport Application data (e.g., network management and control data) that is inside the DISN boundary.

6.1.4.3 DISN Long-Haul support personnel will be sufficiently cleared for the computer and physical access areas. DISN Long-Haul support personnel who can directly affect the security posture of the DISN Long-Haul infrastructure will have at least a Secret clearance, or industry equivalent. All support personnel will require successful identification and authentication and their actions are subject to audit.

6.1.4.4 Strong authentication of network management traffic shall occur at each DISN Long-Haul component. The strong authentication exchange shall allow for the verification of the identities of both the sender and the receiver, enable the verification of the integrity of the management traffic, and allow the receiver to verify the timestamp associated with the management traffic. Strong authentication shall be based on cryptographic techniques. Successful strong identification and authentication shall occur before access to any DISN resources will occur.

6.1.5 These above rules, along with the required administrative (procedural), physical, personnel, operations, emanations and TEMPEST, communications, and other computer and network security requirements for the level of information handled in the processing enclaves form the basis for the DISN Security Policy. Along with active network management and other security monitoring techniques, form the basis for the DISN Defensive Information Warfare (IW-D) capability implemented at the Global and Regional Control Centers/Regional Operations and Security Centers (GOSC and RCC/ROSC) and extending to the DISN boundary.

6.2 Local Subscriber Environment (LSE). The LSE, part of the DISN Sustaining Base Block, will comply with the appropriate requirement of the DISN Long-Haul Block Connection Security requirements. As transport systems are brought into the DISN they will individually publish their connection approval process in the SSAA for the specific system.<sup>2</sup>

6.3 The DISN Long-Haul Boundary.

---

<sup>2</sup> Currently both SIPRNET and NIPRNET have published connection approval requirements. See paragraph 7.3.4.

6.3.1 The end-to-end information transfer network (i.e., DISN) noted in the February 1994 Assistant Secretary of Defense (ASD) C3I memorandum is defined in this DISN Security Policy as the Long-Haul Block extending between Local Subscriber Environments (LSEs) and including the following as its service delivery points for user connection:

6.3.1.1 The Standardized Tactical Entry Point (STEP) for tactical and deployed circuits;

6.3.1.2 The Video Teleconferencing (VTC) Hub;

6.3.1.3 The LSE point-of-presence device (e.g., router for connection to the Integrated Digital Network Exchange (IDNX) or Bandwidth Manager (BWM));

6.3.1.4 The Circuit Switch for two/four wire voice connection;

6.3.1.5 The Access Area for connections from base technical control or wiring facility; and,

6.3.1.6 Value-added service delivery points (e.g., Terminal Access Controllers, Gateways).

6.3.2 Connections to DISN will only be made at these service delivery points. No other LSE connections to the DISN, or to any other networks after connecting to DISN, will be made without the explicit permission of DISA or a DISA-appointed representative in cooperation with the LSE DAA.

6.3.3 Communications through the DISN boundary.

6.3.3.1 Communications through the DISN boundary will only include the transfer of user data between the DISN and the LSEs, the transfer of DISN data from within DISN to certain roles for reporting purposes, and the transfer of data over the DISN boundary to and from DISN support personnel when they are acting in the capacity of users (i.e., web browsing, sending e-mail, etc.).

6.3.3.2 All connectivity, communications, and data access through the DISN boundary are subject, at a minimum, to this Security Policy and to the DISN connection requirements. Connection to the NIPRNET requires an Internet Protocol address issued by the DISA Network Information Center (NIC). Connections to the SIPRNET must comply with requirements in DISA message 121713Z DEC 95, subject: DISN SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) INTERIM NETWORK CONNECTION REQUIREMENTS. Connection requirements to the DISN ATM network are similar to the SIPRNET and are currently in draft. Further information may be obtained from DISA/D311, commercial (703) 735-3236 or (703) 735-8290 (DSN 635).

6.3.4 Inside the DISN Boundary. Communications within the DISN will include network management traffic between DISN transmission components; network management traffic between DISN components, the Element Managers, the RCCs/ROSCs, and the GOSC; and user data traffic between DISN transmission components (e.g., POP router, IDNX, Bandwidth Manager (BWM) hub, Circuit Switch, and Access Area). All communications and data

accesses within the DISN boundary are subject to this security policy. All `internal@DISN` local environments (e.g., GOSC and RCCs/ROSCs) are also subject to the DISN security connection requirements and the requirement for detection and reporting, in real time, of all unauthorized penetration, modification, and intrusion attempts (e.g., probes).

### 6.3.4.1 Computer and Network Security Features.

6.3.4.1.1 Confidentiality. Mechanisms will be provided to restrict users (external and internal DISA) to viewing and accessing only data and processes appropriate to their granted permissions.

6.3.4.1.2 Security Range. Customer data within DISN shall be treated as Unclassified, Sensitive Information. Reference 7.3.6 defines sensitive information as:

Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act) [Reference 7.1.7], but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-235).).

6.3.4.1.3 Access Control. DISN design, as it pertains to the DISN boundary, will ensure that means to enforce access restrictions to all system resources (e.g., bandwidth, routes, VTC connections, computer systems, component ports, firewall proxies, virtual private networks, encrypted tunnels, etc.) based minimally on user and DISN support personnel clearance level, formal access approvals, and privileges ("need-to-know") are incorporated. Additionally, this access control will be based on other parameters such as time of day, resources required, priority, etc., as required and as applicable. This data will be provided to the network access control and network management systems and updated, as required, by the DISN Program Security Manager. Access control may be based on rules, roles, identity, or access levels (e.g., clearances), and also includes physical access control. The principle of least privilege will be followed. The access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. As a minimum, the infrastructure component shall support the distinction between supervisory, operation, and maintenance privileges.

### 6.3.4.2 Integrity.

6.3.4.2.1 Data Integrity. DISN design will prevent the unauthorized modification, destruction, and bogus insertion of data stored, transmitted, and processed by the system. Where DISN only provides transport services, integrity checking will be limited to redundancy checking, etc., to recover bit-level errors, when detected. It is the end-user systems'

responsibility to detect and recover data that may have been damaged or altered within DISN beyond bit-level error recovery.

6.3.4.2.2 System Integrity. DISN must ensure that controls are in place to prevent unauthorized hardware and software configuration modification and to detect and log all authorized and un-authorized hardware and software configuration modification.

6.3.4.3 Identification and Authentication.

6.3.4.3.1 DISN design will ensure that means to identify and authenticate DISN support personnel and users are incorporated in any elements that allow direct access (e.g., login to a management workstation or Terminal Access Controller Access Control System [TACACS]) and any elements that grant network usage and/or network control privileges. Successful identification and authentication of support personnel and users shall occur before access to any DISN resources will occur.

6.3.4.3.2 At a minimum, identification and authentication of authorized network managers and other support personnel shall be provided in accordance with National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publication 112, Password Usage Standard.

6.3.4.3.3 Strong authentication of network management traffic shall occur at each DISN component. The strong authentication exchange shall allow for the verification of the identities of both the sender and the receiver, enable the verification of the integrity of the management traffic, and allow the receiver to verify the timestamp associated with the management traffic. Strong authentication shall be based on cryptographic techniques. Successful strong identification and authentication shall occur before access to any DISN resources will occur.

6.3.4.4 Availability.

6.3.4.4.1 DISN will ensure uninterrupted user and DISN support personnel access to authorized functions, data, and bandwidth to provide assured delivery or connectivity at the required speed of service. Mechanisms and procedures to detect or prevent degradation of processing capabilities and failure or delay in data availability or transfer shall be provided including, for example, redundancy, diversity, repetition, recovery, contingency planning, detection and avoidance, etc.

6.3.4.4.2 The DISN shall be protected from denial of service attacks. Denial of service is defined as any action or series of actions that prevents any part of a system from functioning in accordance with its intended purpose. This shall include any action that causes unauthorized unavailability (blockage, delay of service, etc.).

6.3.4.4.3 Protection shall be provided against loss or degradation of network services. In addition to protection against failures caused by hardware and software failures and component and communications outages, the transport functions shall be protected, as necessary and as

applicable, from maliciously caused attacks, such as jamming, spoofing, manipulated overloads, computer viruses, induced system crashes, and unauthorized message injection, as well as other threats identified in the references in Section 5.

**6.3.4.5 Non-Repudiation (Network Management Data).** The non-repudiation security service affiliated with management data is based upon how the configuration data is communicated. If a file transfer application (e.g., FTP) or a messaging application (i.e., Defense Message System [DMS] agent) is used to communicate this data, then proof of origin is mandatory and proof of receipt is optional; all DMS messages must be signed, but a signed receipt is optional. If network management protocols are used (e.g., Simple Network Management Protocol [SNMP]) then proof of origin is required both from the manager and from the agent.

**6.3.4.6 Computer Systems.**

**6.3.4.6.1** All computer components within the DISN boundary shall meet the requirements as specified in DOD 5200.28-STD, for Division C, ADiscretionary Protection,@ Class C2, AControlled Access Protection,@ (i.e., C2).

**6.3.4.6.2** Audit logging procedures and software shall, at minimum, record security relevant events. All unauthorized access attempts shall be logged on a real-time basis. All activities which attempt to corrupt or modify configuration data in an unauthorized way shall be logged. All authorized changes to configuration data shall be logged. The audit log affiliated with capturing configuration control function audit events shall be protected from unauthorized access and tampering. The software which generates and reports audit events shall be protected from unauthorized access and tampering. Audit events shall be stored on-line for 90 days and on-line or off-line for an additional 9 months.

**6.3.4.6.3** Repeated unauthorized access attempts shall generate an alert to DISN support personnel. Implementation descriptions for specific systems will specify the number of attempts at which alarms will be generated.

**6.3.5 Personnel Security.** Personnel security shall be provided in accordance with DODD 5200.1-R and as delineated in the approved SSAA. Personnel security shall include Secret clearances for all government personnel who have access and authorization to effect security changes to any DISN hardware and software components. Personnel requiring access to Government facilities **as a place of duty** shall obtain and maintain Secret clearances, at a minimum.

**6.3.6 Administrative (Procedural) and Operations Security.**

**6.3.6.1** A configuration management system for DISN will be used through the DISN's life cycle to maintain control of changes to the system, ensuring that the system in operation is the correct one and is consistent with this Security Policy. Configuration management will be

enforced to control all physical, hardware, software, firmware, and documentation changes. Security managers will participate in network hardware and software management configuration management activities, advising the DISN Information Systems Security Officer (ISSO) of changes that affect network security. All changes affecting DISN security posture must be accounted for and assessed by the DAAs, or their authorized representatives, before and after the change.

6.3.6.2 DISN users must be trained to properly interact with DISN and its services. DISN support personnel must be trained to properly operate DISN and its services.

6.3.6.3 Maintenance will be performed only by authorized government and contractor maintenance personnel who shall have clearances consistent with their requirement for access to classified material.

6.3.6.4 Trusted distribution methods will exist to ensure that the trusted system is delivered to a site exactly as intended. Trusted distribution includes procedures that ensure all of the configuration items (hardware, software, and updates) received at the site are actually what was sent. Controls and procedures provide for maintaining the integrity of the mapping between the master data describing the current version and onsite copy of the code. Procedures (e.g., site security acceptance testing) also ensure that the software and hardware distributed are exactly as specified by the master copies.

6.3.6.5 Systems and applications programmers, users, and support personnel shall obtain security clearances consistent with their need for access to classified material. Hardware maintenance personnel will have security clearances where access to classified data cannot be prevented, or where otherwise required by the site where service is performed. Maintenance, systems, and applications programmers, users, and other support personnel who will have access to the ~~Sensitive But Unclassified~~ network configuration control data and databases shall have been determined trustworthy as a result of the favorable completion of a national agency check (NAC), or shall be under escort by appropriately cleared personnel.

6.3.6.6 Vendors, suppliers, and other contractors engaged in maintenance activities must have contracts indicating the requirement for cleared personnel. Maintenance agreements must specify that all such personnel be U.S. citizens (or Foreign Nationals where a Government-to-Government agreement allows for equivalent procedures) who are cleared according to the classification level of the material and data to be accessed. Maintenance of communications security (COMSEC) devices (for OCONUS DISN and for special leased lines for CONUS users) will be performed only by appropriately trained and authorized personnel.

6.3.7 Physical Security. For vendor locations, physical security in accordance with paragraphs 5-306, 5-307.a, 5-800, 5-80 1, 5-900 through 5-906, and 8-300.a of DOD 5220.22-M, and as delineated in the approved SSAA shall be provided for all DISN assets. For

Government locations, physical security shall also include the requirements of Defense Communications Agency Circular (DCAC) 310-90-1.

### 6.3.8 Emanations Security.

6.3.8.1 General. Measures to control compromising emanations (TEMPEST) are required under the provisions of DOD-5200.19, Control of Compromising Emanations.

6.3.8.2 Emanators. Any piece of **AIS** equipment may produce emanations.

6.3.8.2.1 The types of equipment that may be expected to generate the worst radiation are input/output devices in which the circuits creating or transferring data operate at high voltages or high currents levels, and VDT/CRT display devices of the type requiring reiterative refreshing of the viewing screen and their associated buffers.

6.3.8.2.2 Certain devices such as telephones, radio, VCRs, televisions, tape/CD player/recorders, pagers and other electronic equipment have the ability to act as amplifiers and transmitters.

6.3.8.3 Control. The probability of compromising emanations can be greatly reduced by using equipment that is TEMPEST tested and on the TEMPEST qualification special committee Preferred Products List (PPL). Your TEMPEST support personnel should have a copy of the PPL. There are basically three methods recommended for the control of compromising emanations. Any measures taken must be approved by the **Certified TEMPEST Technical Authority**.

### 6.3.9 Information Protection.

6.3.9.1 User data will have been adequately protected by the user before submission to the DISN Long-Haul block, as discussed above, and will be handled as Controlled, Unclassified Information (Appx C, Reference 7.2.7) within the DISN Long-Haul block.

6.3.9.2 DISN Long-Haul network control data (e.g., switch or router level) is considered to controlled, unclassified information. The Single System Manager or Operational Manager responsible for the operational use of any collection of information of network control data will be responsible for assessing the potential classification of the compilation of such information and ensuring information protection guidance (e.g., classification guide) is issued or such guidance incorporated into existing guidance as an amendment.

6.3.9.3 Network management information has a longer persistence and contains a broader range of detail than network control data. Frequently, separate information systems are fielded to support the manipulation of this information. Project Mangers developing such systems are responsible for obtaining an assessment from the appropriate Operational Manager of the classification of such collected information and issuing information protection guidance. This information will be appropriately protected before insertion into the DISN Long-Haul block for

transport. The fielded information systems are considered a segment of the DISN Long-Haul Block.

#### 6.3.10 Management.

6.3.10.1 Accounting, configuration, fault, performance, and security management data shall be protected from unauthorized modification, destruction, and disclosure while in transit, use, and in storage. Security management functionality for the protection of the integrity of backbone and access area transmission services and associated resources shall be provided. Access to security related resources and infrastructure components shall be captured and logged. These audit logs shall be retained online for a period of 90 calendar days and on-line or off-line for a total of one year.

6.3.10.2 The security management function shall have the built-in capabilities to ensure a trusted recovery if the function and/or system component the function operates within fails. Trusted recovery shall include assurance that the integrity of the configuration data is that which it was prior to the failure. Accurate backup configuration data is mandatory.

6.3.10.3 Management of DISN components while directly connected to the component (e.g., from console or attached terminal) shall require successful identification and authentication, at a minimum. Management of DISN components from within the DISN shall require successful identification and authentication and full session integrity. Management of DISN components from outside DISN shall require successful strong identification and authentication, full session integrity, and full session confidentiality.

## Section 7

### REFERENCES

The following references apply to the DISN Security Policy and are applicable through the life cycle of DISN resources, as appropriate:

#### 7.1 NATIONAL POLICY and PUBLIC LAW.

7.1.1 Office of the President, *Executive Order 12333, United States Intelligence Activities*, 4 December 1981.

7.1.2 Office of the President, *Executive Order 12958, Classified National Security Information*, 17 April 1995 (supersedes Executive Order 12356).

7.1.3 Office of the President, *National Policy for the Security of National Security Telecommunications and Information Systems (U)*, 9 July 1990. CONFIDENTIAL.

7.1.4 *National Security Directive 42*, 5 July 1990.

- 7.1.5 Public Law 100-235, *The Computer Security Act of 1987*, 8 January 1988.
- 7.1.6 The Freedom of Information Act, 5 USC 552.
- 7.1.7 *The Privacy Act*, 5 USC 552a.
- 7.2 DEPARTMENT OF DEFENSE and JOINT STAFF.
  - 7.2.1 Assistant Secretary of Defense for C3I Memorandum, *Information Management Definitions*, February 25, 1994.
  - 7.2.2 Assistant Secretary of Defense for C3I, *Interim DoD Policy on the Control of Compromising Emanations*, 28 January 1994.
  - 7.2.3 Chairman, Joint Chiefs of Staff, *Defense Information System Network and Connected Systems*, CJCSI 6211.02A, May 1996.
  - 7.2.4 Chairman, Joint Chiefs of Staff, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems*, CJCSI 6212.01A, 30 Jun 95.
  - 7.2.5 Chairman, Joint Chiefs of Staff, *Defensive Information Warfare Implementation*, CJCSI 6510.01A, 31 May 1996.
  - 7.2.6 DODD 5200.1, 7 June 1982, *Information Security Program*, with Change 1, 29 June 1982, and Change 2, 15 April 1994.
  - 7.2.7 DODD 5200.1-R, 1 June 1986, *Information Security Program Regulation*, with Change 1, 27 June 1988.
  - 7.2.8 DODD 5200.2-R, *Personnel Security Program*, January, 1987, with Change 2, July 14, 1993.
  - 7.2.9 DODD C-5200.5, 21 April 1990, *Communications Security (COMSEC)* (U). CONFIDENTIAL.
  - 7.2.10 DODD 5400.7, 13 May 1988, *DoD Freedom of Information Act Program*, CFR 285.
  - 7.2.11 DODD S-5200.19, *Control of Compromising Emanations (U)*. SECRET.
  - 7.2.12 DODD 5220.22M, January 1995, *National Industrial Security Program Operating Manual (NISPOM)*.
  - 7.2.13 DODD 5200.28, March 1988, *Security Requirements for Automated Information Systems (AIS)*.
  - 7.2.14 DOD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, 26 December 1985.

7.2.15 DODI 5200.40, *Department of Defense (DoD) Security Certification and Accreditation Process*, 30 December 1997

7.3 FEDERAL AGENCIES and COMMITTEES.

7.3.1 Director, Central Intelligence, *DCID 1/16, Security Policy for Uniform Protection of Intelligence in Automated Information Systems and Networks (U)*, 19 July 1988. SECRET.

7.3.2 Director, Central Intelligence, *DCID 1/16 Supplement, Security Manual for the Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)*, 19 July 1988. SECRET.

7.3.3 National Communication Security Committee 11, *National Policy for Protection of Telecommunications Systems Handling Unclassified National Security Related Information*, 3 May 1982.

7.3.4 National Security Telecommunications and Information Systems Security Committee, NSTISS Publication 200, *National Policy on Controlled Access Protection*, 15 July 1987.

7.3.5 National Security Telecommunications and Information Systems Security Committee, NSTISSI Publication. 3013, 8 February 1990, *Operational Security Doctrine For The Secure Telephone Unit III (STU-III) Type 1 Terminal & Annex A-H*.

7.3.6 National Security Telecommunications and Information Systems Security Committee, NSTISS Publication 4009, *National Information Systems Security Glossary*, January 1996.

7.3.7 National Security Agency, NSAM 90-2, *COMSEC Material Control Manual*, October 1989.

7.3.8 National Security Agency, NACSI 4008, *Safeguarding and Control of Communications Security Material*, 12 October 1979. CONFIDENTIAL.

7.3.9 National Security Agency, NACSI 4005, *National COMSEC Instruction*, March 1983.

7.3.10 National Security Agency, NACSIM 5203, *Guidelines for Facility Design and RED/BLACK Installation*, March 1988,

7.3.11 DCAC 310-90-1, Nov 1983, *Physical Security Measures for Defense Communications Facilities*.

7.3.12 Defense Information Systems Agency, *DISA Instruction 630-230-19, Security Requirements for Automated Information Systems (AIS)*, 28 August 1991.

7.3.13 Defense Information Systems Agency, *TAFIM Volume 6: DOD Goal Security Architecture (DGSA)*, draft.

- 7.3.14 Defense Information Systems Agency, *Defending the Defense Information Infrastructure (DII): DISA's Vision & Strategy for Defensive Information Warfare (IW-D)*, September, 1995.
- 7.3.15 National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document*, December 5, 1994, Second Edition.
- 7.3.16 National Communications System, *Natural and Technological Disaster Threats to National Security and Emergency Preparedness (NS/EP) Telecommunications*, August 30, 1993.
- 7.3.17 National Communications System, *Summary Threat to National Security and Emergency Preparedness Telecommunications*, October, 1994. CONFIDENTIAL.
- 7.3.18 Government and National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchanges (NSIEs), *An Assessment of the Risk to the Security of the Current and Near-Term Public Network*, DRAFT, September 10, 1995.
- 7.3.19 Mitre, *DISN-C Vulnerability Assessment Plan*, DRAFT, 28 September 1995.
- 7.3.20 Mitre, Center for Integrated Intelligence Systems, Working Note WN 94W0000126, *Asynchronous Transfer Mode (ATM) Vulnerability Analysis*, September, 1994.
- 7.4 PROGRAM DOCUMENTS.
- 7.4.1 The Joint Staff, Joint Requirements Oversight Council, *Defense Information System Network (DISN) Mission Needs Statement (MNS)*, JROCM 047-95, 30 March 1995.
- 7.4.2 The Joint Staff, *Capstone Requirements Document (CRD) for the Defense Information Systems Network (DISN)*, DRAFT, 29 September 1995.
- 7.4.3 Defense Information Systems Agency, *Defense Information System Network (DISN), Architecture*, September 1996.
- 7.4.4 Defense Information Systems Agency, *Defense Message System Security Policy*, 10 December 1993.
- 7.4.5 Defense Information Systems Agency, *Proposed Defense Information System Network-Near Term (DISN-NT) Security Architecture*, May 1992.
- 7.4.6 Defense Information Systems Agency/Defense Information Systems Security Program, *DOD Goal Security Architecture*, Draft, April 1993.
- 7.4.7 Defense Information Systems Agency, *DII Master Plan THE DEFENSE INFORMATION INFRASTRUCTURE Version 5.0*, 21 November 1996

APPENDIX A: ACRONYMS and TERMS

ACRONYMS

AIS	Automated Information System
ASD	Assistant Secretary of Defense
ATM	Asynchronous Transfer Mode
BI	Background Investigation
BWM	Bandwidth Manager
CAP	Connection Approval Process
CJCS	Chairman, Joint Chiefs of Staff
CJCSI	Chairman, Joint Chiefs of Staff Instruction
COMSEC	Communications Security
CONUS	Continental United States
CRD	Capstone Requirements Document
CUI	Controlled, Unclassified Information (Appx C, DOD 5200.1-R)
DAA	Designated Approving Authority
DCAC	Defense Communications Agency Circular
DCI	Director, Central Intelligence
DCID	Director, Central Intelligence Directive
DCS	Defense Communications System
DCTN	Defense Commercial Telecommunications Network
DGSA	DoD Goal Security Architecture
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DIS	Defense Information System
DISA	Defense Information Systems Agency
DISC	Defense Information Systems Council
DISN	Defense Information System Network
DISN-NT	Defense Information System Network - Near Term
DISSP	Defense-Wide Information Systems Security Program
DMS	Defense Message System
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DSAWG	DISN Security Accreditation Working Group
DSIR	DCS Spain, Italy Reconfiguration

E3	End-To-End Encryption
FIPS	Federal Information Processing Standard
GENSER	General Service
GOSC	Global Operations and Security Center GOSIP      Government Open Systems Interconnection Profile
GNMA	Goal Network Management Architecture
HAL	Host Access Line
IDNX	Integrated Digital Network Exchange
INFOSEC	Information Systems Security
IPMO	Information Program Management Office (DISA/D25)
IPR	Internet Protocol Router
ISO	International Standards Organization
ISSO	Information Systems Security Officer
IW-D	Defensive Information Warfare
JCRD	Joint Capstone Requirements Document
JCS	Joint Chiefs of Staff
JTF	Joint Task Force
LAN	Local Area Network
LSE	Local Subscriber Environment
MILNET	Military Network
MOA	Memorandum of Agreement
MOP	Memorandum of Policy
MLS	Multilevel Security
MNS	Mission Needs Statement
MS	Management System
NAC	National Agency Check
NCS	National Communications System
NIST	National Institute of Standards and Technology
NMC	Network Management Center
NSA	National Security Agency
NS/EP	National Security/Emergency Preparedness

OCONUS	Outside CONUS
OSD	Office of the Secretary of Defense
PCS	Personal Communications Services
PMO	Program Management Office
PN	Public Network
POP	Point of Presence
PSN	Packet Switched Network
RCC/ROSC	Regional Control Center/Regional Operations Security Center
RFP	Request for Proposal
S/A	Services and Agencies
SACS	Secure Access Control System
SBU	Sensitive But Unclassified (Identified State Department information, use CUI for DoD information)
SCARs	Security Connection Approval Requirements
SCI	Sensitive Compartmented Information
SDP	Service Delivery Point
SIOP-ESI	Single Integrated Operations Plan - Extremely Sensitive Information
SMUX	Smart Multiplexer
SNMP	Simple Network Management Protocol
SSAA	System Security Authorization Agreement
STEP	Standardized Tactical Entry Point
STU	Secure Telephone Unit
TAC	Terminal Access Controller
TACACS	Terminal Access Controller Access Control System
TAFIM	Technical Architecture Framework for Information Management
TFS	Traffic Flow Security
TRM	Technical Reference Model
TS	Top Secret
VTC	Video Teleconferencing
X.25	Protocol for Packet-Switched Networks

**TERMS**

**Access Control** - Process of limiting access to the resources of an AIS to only authorized users, programs, processes, or other systems.

**Authentication** - Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information

**Availability** - The goal of ensuring that information and information processing resources both remain readily accessible to their authorized users.

**Confidentiality** - Assurances that information is not disclosed to unauthorized entities or processes.

**Information Domain** - a set of users, their information objects, and a security policy.

**Integrity** - The goal of ensuring that data continues to be a proper representation of information, and that information processing resources continue to perform correct processing operations.

**Local Subscriber Environment (LSE)** - include all devices and communication systems under user (organization) control. LSEs may contain a single end system such as a workstation, a single relay system such as a router, or a complex interconnection of end systems and relay systems through local communication systems.

**Non-Repudiation** - Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

**Peer Entity Authentication** - The corroboration that a peer entity in an association is the one claimed.

**Physical Security** - The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

**Previously-Protected Data** - Data that has been protected (e.g., encrypted) by the end user, or by a device within the LSE, before the data is submitted to the DISN for transport.

**Security Associations** - A virtual secure communications channel that is established to convey and subsequently enforce the necessary security services using the appropriate mechanisms and strength of mechanisms to maintain information domain isolation and integrity over communication systems.

**Security Management** - provides supporting services that contribute to the protection of information and resources in open systems in accordance with the applicable security policy.

**Security Mechanism** - A system or means of implementing a security service within a system. The system security measures by which the security policy objectives are achieved.

**Security Service** - A system or method of providing a security-relevant feature in the system.

**Strong Authentication** - (1) Authentication by means of cryptographically derived credentials. (2) For DISN, and specifically for network management traffic, the establishment of a security association, or a subsequent communication on a previously established association, in which the identities of the sender and receiver can be verified, the integrity of the data can be verified, and the timeliness or timestamp of the data can be verified.

**Terminal Access Controller (TAC)** - A special type of host attached to a PSN that allows direct terminal access to the DISN backbone.

**Traffic flow security (TFS)** - Measures used to conceal the presence of valid messages in an on-line cryptosystem or secure communications system.