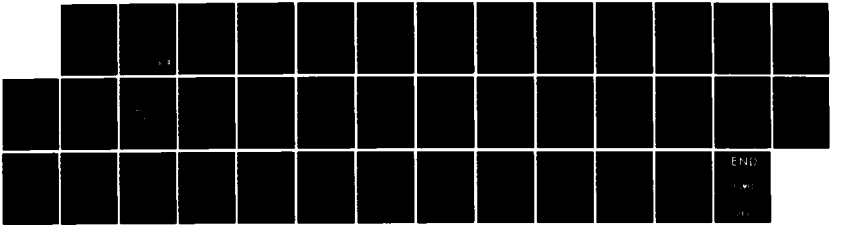
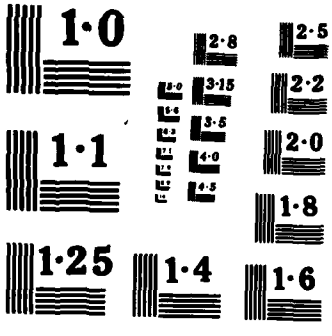
AD-A152 524 DEFENSE DATA NETWORK SUBSCRIBER SECURITY GUIDE(U) MITRE 1/1
CORP MCLEAN VA NOV 83 F19628-82-C-0001

UNCLASSIFIED F/G 15/3 NL




1·0
1·1
1·25
1·4
1·6
2·8
3·15
3·5
4·0
4·5
2·5
2·2
2·0
1·8

(1)

DEFENSE COMMUNICATIONS AGENCY

DEFENSE DATA NETWORK SUBSCRIBER SECURITY GUIDE

NOVEMBER 1983

DDN

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE	READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A152520 / 3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)* Defense Data Network Subscriber Security Guide	5. TYPE OF REPORT & PERIOD COVERED
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s)	8. CONTRACT OR GRANT NUMBER(s) F19628-82-C-0001
9. PERFORMING ORGANIZATION NAME AND ADDRESS The MITRE Corporation 1820 Dolley Madison Blvd. McLean, Virginia 22102	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS	12. REPORT DATE November 1983
	13. NUMBER OF PAGES 30
14. MONITORING AGENCY NAME & ADDRESS *(if different from Controlling Office)* Defense Communications Agency DDN-PMO Code B626 Washington, DC 20305 (Project Monitor: John Walker)	15. SECURITY CLASS *(of this report)* U
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for public release; distribution is unlimited.

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

Accession For	
NTIS GRA&I	X
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

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

Security architecture, Communication networks, Cryptographics, Network security

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

This guide describes the security architecture now being implemented for the Defense Data Network (DDN). The architecture will be used until around 1987 when improved security devices are expected to be available. The guide describes how the architecture will then evolve.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

DEFENSE COMMUNICATIONS AGENCY

DEFENSE DATA NETWORK SUBSCRIBER SECURITY GUIDE

NOVEMBER 1983

Prepared by The MITRE Corporation

DDN

A form for readers' comments is provided at the back of this document. Additional comments and requests for further information should be directed to the Defense Communications Agency, ATTN: Defense Data Network Program Management Office, Code B610, Washington, D.C. 20305.

ABSTRACT

This guide describes the security architecture now being implemented for the Defense Data Network (DDN). The architecture will be used until around 1987 when improved security devices are expected to be available. The guide describes how the architecture will then evolve.

ACKNOWLEDGEMENTS

This guide was prepared by The MITRE Corporation for the Defense Data Network Program Management Office of the Defense Communications Agency (DCA) under Contract Number F19628-82-C-0001. It was prepared by condensing and rewriting a longer report [DCA82b] prepared during the summer of 1982 by an ad hoc working group of personnel from the DCA, the National Security Agency, Bolt Beranek and Newman Inc., System Development Corporation, and MITRE.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

1.0 INTRODUCTION

This Defense Data Network (DDN) subscriber security guide describes the security architecture now being implemented for the DDN. The architecture will be used until around 1987 when improved security devices are expected to be available. The guide describes how the architecture will then evolve. The guide assumes that the reader is acquainted, at least regarding terminology, with the Defense Data Network Program Plan as revised in May 1982 [DDN82], herein called "the Plan". Material is incorporated in this guide by reference to the Plan.

1.1 Background

This guide supersedes Section 3.3 of the Plan, "Security and Privacy Approach." That section sketches a network security architecture that depends primarily on two elements: (1) link encryption on the trunks and (2) end-to-end encryption (E^3) to create logical subnetworks that separate subscriber groups. The Plan assumes that all encryption is military grade (the KG-84) and that the DDN has a single, optimized backbone network of switches and trunks.

After studying the Plan, the Deputy Under Secretary of Defense for Communications, Command, Control, and Intelligence requested a review of some architectural options [Lath82]. One class of options used commercial grade encryption, the Data Encryption Standard (DES) [FIPS46], for unclassified data. Another involved physically partitioning the DDN into classified and unclassified segments, with provision for sharing resources in a crisis. To perform the review, an ad hoc working group of DCA, NSA, and contractor (BBN, MITRE, and SDC) personnel met through the summer of 1982. It defined and analyzed the options with regard to performance, cost, technical risk, schedule, and security risk.

This guide describes the architecture chosen from among the several options documented in [DCA82a, DCA82b, NSA82a, and NSA82b]. Those documents refer to the chosen architecture as "option 2.2, with [Internet Private Line Interface devices] IPLIs on the SECRET users, and without reimplementation of either switch or monitoring center."

This guide describes the security architecture to which the DDN will evolve prior to the introduction of multilevel secure hosts, which will use the next, post-IPLI generation of E^3 devices, called BLACKER devices. The planned stages of the evolution are described in Section 6. The BLACKER devices will permit interconnection of trusted hosts across security levels. To complete the definition of BLACKER requirements for the DDN, a study has already begun [DCA83c].

Implementation of the chosen architecture requires a number of tasks. These have been incorporated in the DDN Management Engineering Plan [DCA83a]. Additional details are contained in the Defense Data Network Subscriber Interface Guide [DCA83b].

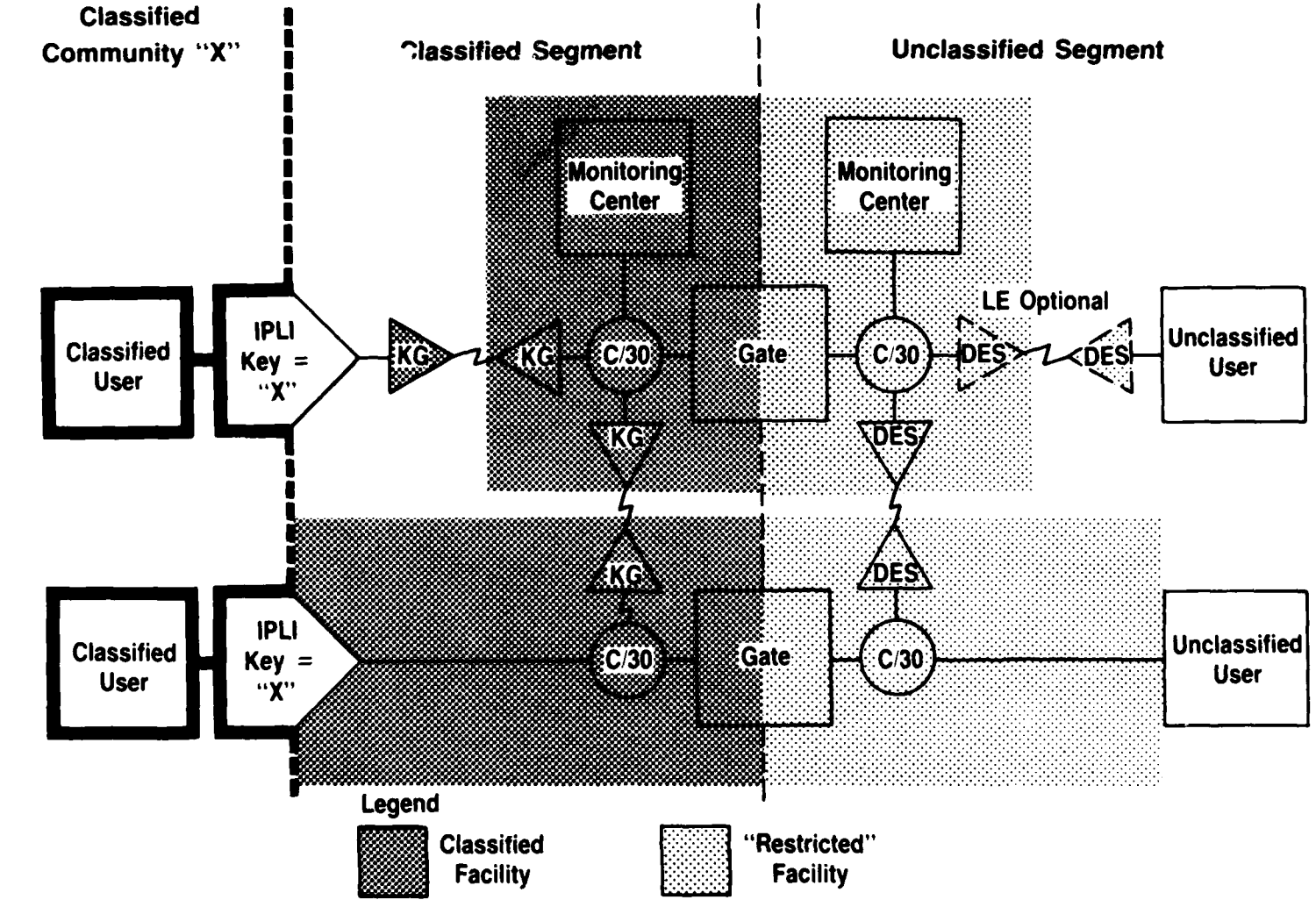
1.2 Security Overview

Figure 1 shows the DDN split into two separate backbone networks called segments, one classified and one not, that are connected by gates. (The term "gate" is deliberately chosen to be different from the term "gateway" that is used in internetworking.)

1 Topology. The segments are optimized independently of each other, one for classified subscribers and the other for unclassified. The segments are linked at several points by gates. Each gate is attached to one switch in each of the segments. Any switch has at most one attached gate.

The segments are assumed to be physically connected by the gates at all times. When allowed by the gate logic, data from the classified segment can flow into the unclassified segment, through the unclassified segment, and back to the classified segment. However, traffic originated in the unclassified segment never can flow through the classified segment.

Figure 1
DDN Security Overview



A gate acts like an IPLI with a modified plaintext side. On its plaintext side it attaches to a switch in the classified segment, and on its cyphertext side to one in the unclassified segment. It provides gate-to-gate E^3 for classified packets that leave the classified segment to flow through the unclassified segment. The two segments are always connected to allow this flow.

2 Switch security. All switches in the classified segment and all OCONUS (outside the continental United States) switches in the unclassified segment reside in facilities protected to the SECRET level. In the rest of the unclassified segment, access to switches is "restricted" [Lath 82] but not necessarily at the SECRET level.

3 Traffic flow security. Trunks and access lines of the classified segment are link encrypted with KG-84s. OCONUS-OCONUS and CONUS-OCONUS trunks of the unclassified segment use KG-84s, but the rest use the DES. Section 2.0 defines what DES means in the DDN context in terms of allowable equipment and procedures.

4 Subscriber connection. Each classified subscriber in the segmented DDN connects to the network only through an IPLI that incorporates a KG-84. But the DDN neither provides nor requires E^3 for unclassified subscribers, and they may connect directly to a switch.

5 Gate Security. Each gate is located in a facility cleared to the SECRET level. The same facility houses the attached classified switch. Traffic passing through a gate from the classified to the unclassified segment is superencrypted by a KG-84 that is part of the gate.

Additional details follow in this guide or are available in the references.

1.3 Section Summaries

The rest of this guide describes the DDN security architecture in greater detail. Section 2 describes the cryptographic security features and points out where subscribers have options regarding encryption. Section 3 describes hardware security, particularly protection against compromising emanations. Section 4 describes the

software features of the DDN that are trusted to operate correctly, including features of the subscribers' hosts. Section 5 describes requirements for physical and personnel security and other operational matters. Section 6 describes how the security architecture will evolve. During the 1982 summer review, the architecture of the integrated DDN was defined in sufficient detail to permit reasonable assurance that it is adequate to meet mid-range needs of the DDN, and to provide the basis for reasonable transitions to a longer range DDN architecture with multi-level secure hosts and BLACKER-style E^3. However, a number of areas continue to be studied.

Originals supplied keywords included → p 1473

2.0 CRYPTOGRAPHIC SECURITY FEATURES

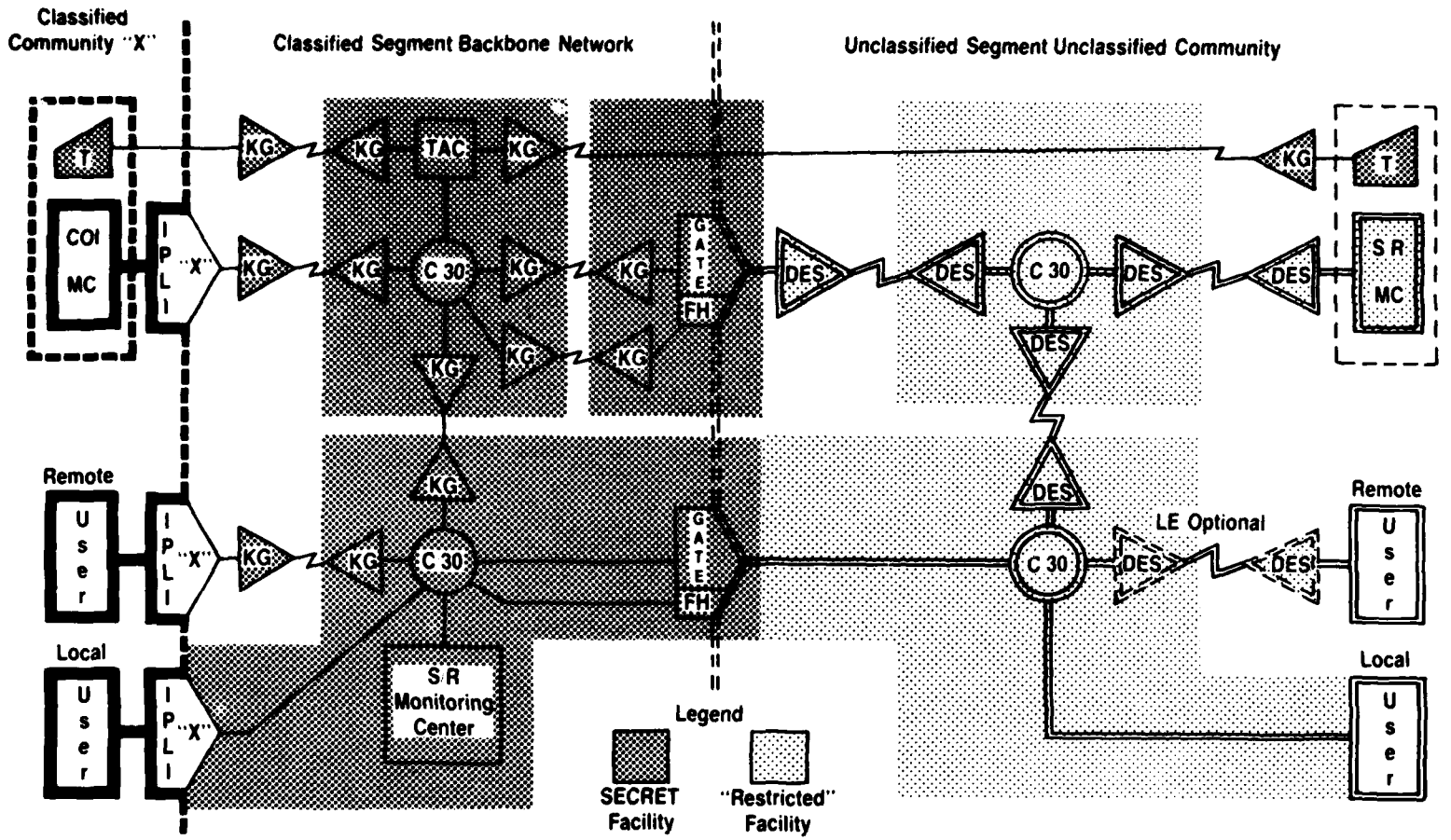
This section describes the cryptographic security provided by the DDN to its subscribers. All classified data and related network control functions are protected by military-grade encryption, the KG-84, for which the required mode of operation in the DDN is described in Appendix A. For unclassified data and related control functions, the the DDN uses commercial-grade encryption, the DES.

- Data Encryption Standard. In the DDN, "DES" means equipment that conforms to [FIPS46], [FIPS81], [FS1027], and any other applicable rules, such as pending [FS1025] and [FS1026]. In particular, it also means equipment certified relative to FIPS46 by NBS, and endorsed relative to FS1027 by NSA. This meaning applies to trunk encryption in the unclassified segment, to unclassified subscriber access line encryption, and to other uses that are subscriber options.

Figure 2 shows the security architecture in more detail. DDN user devices include host computers, network access components (NACs) -- including terminal access controllers (TACs), host front-end processors (HFEPs), and terminal emulation processors (TEPs) -- gateways to neighbor networks, and other devices. This paper refers to all these user devices as hosts or subscribers. All classified hosts connect to the DDN through IPLIs. Remote access lines for classified hosts must be link encrypted.

Portions of the DDN's unclassified segment that are OCONUS, such as the expanded Movements Information Network (MINET) in Europe and DDN assets in the Pacific, use KG-84s on their OCONUS-OCONUS interswitch trunks and on the CONUS-OCONUS interswitch trunks that connect those portions to the CONUS. All such KG-protected trunks connect on both ends to switches protected to the SECRET level. All remaining switches of the unclassified segment that are in the CONUS, that is, all unclassified switches that do not connect directly to an OCONUS switch, reside in at least "restricted" locations. All unclassified trunks connecting two CONUS switches are encrypted with

Figure 2
The Segmented Defense Data Network



the DES. An unclassified remote host access line generally will not be encrypted, but it may be link encrypted with the DES, or with KG-84s if the line connects to a switch in a SECRET facility, if the subscriber wishes to provide that protection.

Each segment has a system monitoring center (SMC) and may have one or more regional monitoring centers (RMCs). In addition, there are five community of interest monitoring centers (COI MCs).

The Plan lists five classified COIs and one unclassified COI. Each classified COI has a COI MC that connects to the DDN through an IPLI just like any other classified host. The unclassified COI does not have a COI MC, because the unclassified hosts do not use E^3 and, therefore, can communicate with the S/R MCs in the unclassified segment.

Figure 3 shows the number of sites serviced by the DDN for each COI and the number of IPLIs required. The estimates assume the largest probable number of subscribers.

Figure 3
Estimated IPLI Quantities

ENCRYPTION COMMUNITY	IPLI SITES	REQUIRED IPLIs
SACDIN	25	60
SCI	70	100
Top Secret	70	100
Secret	200	500
Gates	20	30
Total	475	970

3.0 HARDWARE SECURITY FEATURES

This section discusses security requirements for DDN hardware components.

3.1 Construction

Proposed DDN hardware is not now manufactured in secure facilities. Security clearances are not now required for personnel involved in the construction of any components except KGs and IPLIs. Integrated circuit components of all DDN equipment may have various countries of origin. IPLIs and NACs are entirely assembled in the U.S., but assembly of some printed circuit boards for the C-30 switches and C-70 MCs is currently done in Hong Kong and the U.S., with final assembly in the U.S. Cryptographic equipment is constructed in accordance with NSA practices. No assumptions are made about the location of construction of other DDN components (subscriber hosts and terminals, modems, statistical multiplexers, transmission media, etc.).

3.2 Security-Related Hardware Features

Single-bit error correcting memory is used in the switches, MCs, and NACs. Security-related hardware features of the IPLI are described in [BBN4974A, BBN4975], particularly in Section 7.2 of the latter. No other security-related hardware features are assumed.

3.3 Hardware Configuration Control

The SMCs for the DDN backbone, and the COI MCs for the user-side subnets, maintain (for all system components) descriptions of currently installed items and their configuration. The level of detail varies depending on the item. Vendor and Life Cycle Manager maintenance records will identify system components down to individual "bit, part, and piece" level.

3.4 Emanations Security

DDN equipment is TEMPEST compliant in accordance with NACSIM 5100A at 1 meter. Installation is compliant with NACSEM 5203 (30 June 1982). Testing is according to the current version of DCA circular 370-D195-2. These requirements apply to the following equipment, which is described in the indicated sections of the Plan. A "*" means that the equipment may not be TEMPEST, but is instead protected by the enclosing facility.

EQUIPMENT NAME	PLAN SECTION
Switching Node	2.1
Internet Private Line Interface	2.2
Mini-TAC (Terminal Access Controller)	2.3
Statistical Multiplexor	2.4
Host Interface Devices as follows:	
- Host Front-End Processor (HFEP)	2.5.2
- Terminal Emulation Processor (TEP)	2.5.3
Network Monitoring Center (MC) Equipment	2.6
* Test and Development Facilities	2.7
Cryptographic Equipment	2.8
Automatic Line Restoral Option	2.11
Patch and Test Facilities	2.12
Uninterruptible Power Supplies	2.13
Power and Environment Monitor	2.14
Mobile Reconstitution Van	2.15
- Equipment yes.	
- Van no.	

4.0 SOFTWARE SECURITY FEATURES

This section describes DDN features that are trusted to operate correctly. Different features require different levels of trust because of the differing levels of sensitivity of their operation. The security evaluation criteria needed to achieve levels of trust appropriate to DDN equipment are defined in Figure 4.

Figure 4
Definition of Security Evaluation Levels

LEVEL 0. COMMON COMMERCIAL PRACTICE.
No special requirements for development or maintenance.

LEVEL 1. STRICT CONFIGURATION CONTROL.
- -- No special requirements for initial system development.
- -- After that, strict hardware/software configuration control.
  All maintenance personnel have security clearances.
- -- System documentation sufficient for minimum security review.
  Experienced programmer can understand with effort.
  Includes software module and interface descriptions.
- -- Two person-months of penetration testing.

LEVEL 2. STRUCTURED SOFTWARE DEVELOPMENT. All of level 1, plus:
- -- All software developed (or redeveloped, if necessary) using structured programming methods.
- -- Documentation includes a descriptive, English top level specification (DTLS) of security relevant parts of system.
  Experienced programmer can understand with minor effort.
  Includes detailed descriptions and diagrams for each module.
- -- Penetration testing effort increased to four person-months.

LEVEL 3. MODELED SECURITY. All of level 2, plus:
- -- Documentation includes description of formal model used as basis of security design.
  Model informally shown to be consistent and to satisfy its axioms.
  DTLS informally shown to support the model.
  Experienced programmer can understand with ease.
- -- Penetration testing effort increased to six person-months.

Further refinement of the criteria to individually tailor them for each system element will be done.

Figure 5 shows the level of security evaluation criteria that is met by each major DDN system element.

Figure 5
Required Security Evaluation Levels

	CLASSIFIED SEGMENT	UNCLASSIFIED SEGMENT
Switches and Monitoring Centers	1	0
Internet Private Line Interfaces	3	Not Applicable
Network Access Components	2	0
Subscriber Hosts	0 - 3	0 - 3
Inter-segment Gates	3	
Other System Elements	0	0

The levels are shown separately for each segment because they differ for the switches and NACs. For example, a switch has level 1 for the classified segment and 0 for the unclassified. The unclassified segment will receive the same hardware and software as the classified, so it will be at level 1 when shipped or installed. However, the switch is assumed to be trusted only to level 0 on a continuing basis because the environment may not guarantee its integrity.

4.1 Packet Switch

Nearly all switch software is related to some aspect of secure network operation.

1 Integrity check. A Data Link layer checksum is computed and sent with all switch outputs and computed and compared for all switch inputs, except 1822 Local Host inputs [DCA83b]. A switch periodically checksums all of its programs and tables. In addition, before a switch puts into operation software received from a MC, from a neighbor switch, or from a manual load, it checksums the software. These checks are performed by software.

2 Control message authentication and execution. A switch executes control messages sent from a MC, validating them as follows: (1) Header information is checked for a valid MC logical source address. (2) Control message sequence numbers are checked with a windowing algorithm to assure they are increasing.

3 Neighbor reload. The process by which a switch receives a reload of software from a neighbor is described in [BBN89]. A reload is accepted only from a switch in the same segment. A switch validates neighbor reloads in the same way that it validates MC messages.

4 Correct destination. Information is passed only to the destination for which it is intended. Section 3.2.5 of the Plan discusses the possibility of misdelivery due to errors on host access lines or on trunks. Other possible causes of misdelivery are switch software errors, switch hardware errors, intelligent attacks on the trunks, and host-induced addressing errors.

5 Community of interest. Section 3.3.3 of the Plan defines and discusses COIs. In brief, the DDN can separate COIs either by encryption, by controlled routing, or by both. In the first case, a COI is called a "crypto community" and, in the second, a logical subnet or "routing community."

A DDN crypto community includes as many as 1024 unclassified subscribers or 512 classified subscribers. The DDN separates crypto communities by two means. In the switches and on the trunks, it does it with E^3. At the locations of E^3, the IPLIs, it does it with key control and software control.

There can be 16 routing communities, and they can overlap. The DDN separates routing communities by using software at the source and destination switch of each message. A source switch marks packets from a subscriber with the valid routing communities of the subscriber. Before delivery, a destination switch verifies that the destination subscriber is a member of a routing community specified by the source switch. This is done by comparing a routing COI marking in the header of each message sent from a subscriber to a switch, or vice versa, against a table in the switch. The SMC is responsible for the switch table.

6 Precedence. Processing of traffic is based on the precedence level.

7 Line up/down protocol. Communications links are put into and taken out of service in accordance with the current criteria. The basic criteria are described in [BBN89]. Specific parameter settings may vary based on line experience.

8 Event reporting. A switch reports anomalous events, and periodic status information, including traffic statistics, to a monitoring center and only to a monitoring center.

4.2 Internet Private Line Interface

IPLI operation is described in [BBNDCA, BBN4968, BBN4968B, BBN4974A, and BBN4975], particularly the latter two. An IPLI controls the flow of information on its symmetric ciphertext-plaintext bypass, executes and safeguards control messages sent to it, manages its address and configuration tables, manages cryptovariables, and correctly controls its cryptor. An IPLI translates destination addresses from the plaintext to the ciphertext side, without corrupting either addresses or any other IP header data fields. The ciphertext side of an IPLI implements the network access (host-switch) protocol, and the precedence level of a message sent to a switch by the ciphertext side of an IPLI does not exceed the maximum precedence level that is assigned to the IPLI by its COI MC. Anomalous events and periodic status information, including traffic statistics, are reported to the proper monitoring center.

The plaintext side (1) rejects a DCA-bound Internet Protocol (IP) [DDN83b] datagram if the destination address is not listed in the plaintext address table, and (2), for IP datagrams received from the DDN, performs the normal IP gateway functions. The ciphertext side checks (1) the IP source address received from the switch to see that the address is in that IPLI's destination address table and (2)

the validity of the destination index received from the plaintext side.

The plaintext side verifies the checksum in the header of IP datagrams bound either to or from the ciphertext side. The ciphertext side verifies the checksum for traffic from the DDN and inserts the checksum for traffic to the DDN. On both sides, when an IPLI finds an incorrect checksum, it discards the datagram and reports the error to a MC.

4.3 Network Access Component

Except for IPLIs, the NACs are the only DDN components that contain classified data from a subscriber.

1 Access control. Each NAC operates at a single, system high security level. A HFEP or TEP does not control access either to its host or to the DDN: each host is expected to perform the access control function. A mini-TAC has only a single controlled resource, namely network access. The DDN provides both hardwire and dial-up access to mini-TACs. Hard-wired subscribers, which include all classified subscribers to mini-TACs, are identified in the mini-TAC, and are not required to log into the mini-TAC with a password. Users of such terminals are still required to log into destination hosts. All dial-up subscribers are unclassified. Their access to a mini-TAC is controlled by an account number and password.

2 Precedence and preemption. A mini-TAC associates a precedence with each terminal, and checks that the precedence used does not exceed the associated precedence. A mini-TAC services terminals according to their precedence. A mini-TAC has sufficient resources to support active terminals on all terminal ports simultaneously, so it never needs to initiate a preemption. However, it supports preemption of connections initiated from the destination (when the procedures for doing so are defined). Procedures for a HFEP or TEP are the same as for a mini-TAC, except that preemption may be initiated by a host request, or HFEP independent action, as well as by remote network request.

3 Integrity checking. Duplicate message detection, out-of-sequence message detection (and resequencing), and message alteration detection are provided by the Transmission Control Protocol (TCP) implemented in the mini-TAC [DCA83b]. Hosts may obtain three levels of service from the HFEP: TCP in the Transport layer, IP in the Internet layer, or DDN protocol in the Network layer [DCA83b]. Integrity checking for TCP users is the same as for the mini-TAC. Internet and Network layer protocol users are responsible for providing their own integrity checks, if required. A TEP provides the same integrity checking as the mini-TAC.

4 Separation of traffic. A NAC maintains separation between streams of traffic, such as for the separate terminals on a mini-TAC, and does not alter their information. A mini-TAC does not deliver data to the wrong terminal. All the terminals attached to a given mini-TAC, or all the ports attached to a TEP, operate at the same security level.

5 Audit information. A mini-TAC, and other NACs where appropriate, collects a limited amount of audit information (connection times, duration, destination, caller identity for dial-up users, and, where technically feasible, the calling number for dial-up). Audit information is sent only to a secure COI MC.

4.4 Monitoring Center

Nearly all MC software is related to some aspect of secure network operation.

1 Access control. A MC requires a userid/password for access to it, and it gives either monitor or monitor and control capabilities to the user based on the userid. (This is a partially redundant check, since access to terminals capable of logging on to a MC is restricted to authorized personnel.)

2 Messages and software sent. A MC implements (1) down-line loading of software for switches and (2) control message protocols for switches. A MC cooperates in the integrity and authenticity checks described in Section 4.1. Each MC has a standard logical source address. It sequence numbers the messages it sends. It computes and appends a checksum for software modules. A MC implements control message protocols for IPLIs as described in Section 4 of [BBN4975].

3 Audit information. A MC requests, collects, and retains for a limited period, events reported to it from switches (in the case of the SMC and RMC); from IPLIs (SMC and RMC on the DDN side, COI MCs on user side of IPLI); and from hosts and NACs (COI MCs only).

4 MC Initialization. The MCs unambiguously take and maintain control of network resources in accordance with network policy.

4.5 Subscriber Host

This section discusses particular features of subscriber hosts that are trusted to operate correctly.

1 Access control. All hosts, whether attached directly to the user side of an IPLI or indirectly through a user-side network, are responsible for controlling access to (1) their own user-side network and (2) the DDN-side backbone network. All DDN subscriber hosts are required to have a userid/password or equivalent level of control before granting access to or from the DDN.

2 Integrity checking. Hosts that have HFEP or TEP network connections are provided a TCP level of integrity checking. Other hosts are expected to implement the degree of integrity checking that they require internally. Normally this would be via implementation of TCP. Hosts that require levels of integrity checking beyond that provided by TCP will develop their own procedures to establish (or re-establish) integrity to the required level.

3 Precedence and preemption. Hosts with precedence and preemption requirements will implement appropriate facilities to make use of the precedence and preemption services of the network. The nature of these facilities is dependent on the type of network interface. Hosts are responsible for correct implementation.

4.6 Inter-Segment Gate

A gate executes control messages from SMCs in both the classified and unclassified segments, validating these control messages the same way as the switch, as described in Section 4.1. However, a gate

accepts no software changes or table updates from any MC; a gate has fixed software and tables.

A gate's encryption bypass sends the information necessary to address packets sent from the classified to the unclassified segments. A gate's key update protocol permits synchronized update of the keys in all the gates. The protocol is the same as that used in the IPLI. Anomalous events, periodic status information, and traffic statistics are reported to the appropriate monitoring centers.

4.7 Other Network Elements

Network elements such as modems, statistical multiplexers, patch and test facilities, and automated equipment associated with transmission media are expected to correctly perform their functions.

4.8 Software Configuration Control

All software mentioned above except for Subscriber Hosts and Other Network Elements is controlled using the UNIX-based SCCS (Software Configuration Control System). Note that "strict hardware/software configuration management" is required by level 2 as defined in Section 4.0. Software changes are only made subject to government approval. This control begins when the security evaluation begins and continues throughout the network's life. This control includes physical and personnel security as described in Section 5.

5.0 OTHER SECURITY FEATURES

This section discusses physical and personnel security and some aspects of network operation.

5.1 Physical and Personnel Security

The physical and personnel security provided in the DDN is as follows. First, in the classified segment:

1. Equipment that handles classified plaintext is protected to the level appropriate for that traffic. That is, all the equipment in a COI -- subscriber hosts and terminals, NACs, IPLIs, the COI MC, any unencrypted links, and any KGs on links directly connecting these elements -- is protected at least to the level of its COI. In Figure 2, this is the equipment to the left of the heavy, vertical dashed line.

2. Equipment that does not contain classified COI plaintext is protected at least to the SECRET level. This includes switches, other MCs (system, regional, and mobile), and any KGs on links directly connecting these elements to each other or to IPLIs. In Figure 2, this is the equipment between the heavy dashed line and the double dashed line. It also includes the software and hardware configuration control facilities. The facilities housing these elements are physically protected to handle at least SECRET material in accordance with the requirements of the service or agency responsible for the protection of each facility. Personnel at these locations are required to have at least SECRET level clearances.

3. No specific protection requirements exist for modems and transmission media making up the trunks or link encrypted access lines. Unconstrained access to such media must be assumed.

Second, in the unclassified segment:

1. All OCONUS switches, other switches directly attached to OCONUS switches, and associated KG-84 link encryption equipment will receive the same SECRET level protection as the equipment in the classified segment.

2. All other switches and the DES encryption equipment are in locations protected with restricted access. "Restricted

access" means that only authorized personnel are permitted access to the area in which the equipment is located. Authorized personnel are those who require access to the area in which the equipment is located in order to perform their duties, and personnel accompanied by such personnel. A variety of methods may be employed to restrict access.

Examples of a minimum level of acceptable access restriction would be locked access doors with card or keys required for entry, or guarded access doors with entry based on identification such as a special badge or normal personal identification plus presence on an access list to the (unarmed) guard. Personnel with access to this area are considered ADP.II critical personnel as defined by [OPM78], and they meet the requirements for such personnel.

DES link encryption keying material is stored (when not in the DES device, which itself is protected [FS1027]) in secure containers (i.e., containers with a lock) to which no more than ten people have keys or combinations. Personnel with such access are considered ADP-I critical personnel as defined by [OPM78], and meet the requirements for such personnel.

3 No specific protection is required for transmission media.

4 No restrictions are placed on the locations of unclassified access area equipment.

Third, the inter-segment gates and associated link cryptographic equipment are located in areas protected to the SECRET level.

5.2 Network Operation

The DDN operates as described in [DCA82a]. Specific details of the operation of switches, IPLIs, and MCs are described in [BBN89], [BBN4975], and [BBN4823]. Each segment has separate monitoring facilities. In the classified segment, there are S/R MCs, mobile MCs, and, for each separately keyed IPLI community, a COI MC. In the unclassified segment, the S/R MCs also perform the unclassified COI MC functions, and there are no mobile MCs (although those of the classified segment could be used if required). Control of both sides of a gate is the responsibility of the classified segment S/R MC, but

the cyphertext side of a gate responds to Internet Control Message Protocol [DCA83b] messages that appear to have the address of the unclassified segment S/R MC.

5.3 Key Management for Mobile MCs

A mobile MC needs cryptographic keys to establish communications over any trunk to any switch in the MC's zone of operations. Each switch location has keys for each mobile MC with which the switch might establish contact.

A mobile MC can be deployed with IPLI keys for UNCLASSIFIED, SECRET, and TOP SECRET COIs, if it is appropriate to the mobile MC's mission. Otherwise, and particularly for other COIs, a mobile MC must collocate with a community member and obtain the COI IPLI key directly from the member.

6.0 EVOLUTION

This section describes the stages through which the DDN security architecture will evolve. It also lists areas for further study that are related to the evolution.

6.1 Evolution Stages

The planned approach to evolving the DDN is to develop several physically separate networks for the different security groupings in the DDN, and then merge the networks as IPLIs, gates, and BLACKER devices become available. In implementing this approach, substantial flexibility is possible. The security architecture implementation can parallel the four network integration stages.

1 The first stage, based on the initial, prototype IPLI development, permits integration of the DODIIS and TOP SECRET (WIN) networks. Concurrently, on the unclassified segment, DES link encryption, and access control for dial-up TAC and mini-TAC users, will be established as soon as possible.

2 The second stage, based on the "Phase 2" IPLI, which permits SECRET hosts to run on an unclassified network, will also support hosts that normally run unclassified but sometimes run in periods processing security mode at the SECRET level.

3 The third stage, the joining of the TOP SECRET/SI/SIOP network and the SECRET network will be accomplished with the "Phase 3" IPLI, which will support TOP SECRET hosts on a SECRET network. Since separate networks for TOP SECRET and SECRET users will exist, with optimized configurations for their users, the approach taken to combining them will be as follows. First, a combined optimized topology will be developed. Second, the existing topologies will be connected with trunks approximating the optimized joint topology, and the second homing of dual homed subscribers will be moved to switches of the other (TOP SECRET to SECRET and vice-versa) type. This step is roughly equivalent to the establishment of manual gates between the TOP SECRET and SECRET networks, with the switches normally in the closed position. The advantages of this step are improved survivability, performance, and reliability for both the TOP SECRET and SECRET users, combined with the retention of the

capability to separate back to two networks quickly, with at least adequate capability, if security concerns ever dictate that step. IPLIs will be fielded for all classified subscribers in this stage.

4 The fourth stage will connect the classified network to the unclassified network using automatic, IPLI-like gates. This stage will proceed in two steps: (1) design of an optimized topology and (2) placement of the gates on links between the networks to approximate the optimized topology.

5 Additional stages. Several alternatives are available for the final stage, when BLACKER is available. In one alternative, BLACKER devices could be put on all hosts and the automatic gates replaced by manual gates until confidence was gained in the new architecture. This again would permit separation of the networks quickly if it was felt necessary. In this final stage, link encryption in the unclassified segment would be upgraded, as would the level of protection of the switches, to conform with the physical and cryptographic security of the classified segment. A second alternative would be to employ BLACKER devices on only classified hosts, and replace the automatic gates with true multilevel secure gateways. Tamper-proof containers, together with automatic key distribution features of the BLACKER devices, should greatly lessen the administrative concerns associated with the large number of end-to-end encryption devices required with the combined network.

6.2 Areas for Further Study

The level of definition in [DCA82c] is sufficient to be reasonably certain that the summer review mentioned in Section 1 correctly rated the options with respect to security and other operational factors. The review found that the chosen architecture appears to adequately meet the mid-range needs of DDN subscribers. It also provides the basis for reasonable transition alternatives to longer range DDN security architectures that support multi-level secure users, and controlled interaction between such users and single-level users supported by BLACKER E^3. However, the review also identified a number of areas for further study:

1 Related Research and Development. There are several research and development efforts underway that relate to DDN security. They include BLACKER, PARAGRAM, Multinet Gateway, SCC, MARSHA, on-board cryptors, SCOMP, and COS NFE.

2 Suggested security research and development. Several suggested security research and development topics are related to the DDN. They include E^3 bypass characteristics, E^3 overhead, E^3 key distribution, routing and other system "firewalls," use of public data networks, cryptographic authentication, distributed access control, E^3 and other security issues in upper protocol layers, location of validation functions, software development practices, personnel countermeasures, overrun countermeasures, gate management alternatives, mobile MCs, MC trusted computing base, MC control isolation, use of broadcast satellite networks, and network asset mobility.

3 Architecture refinement. There were several architecture variations that the summer study did not have time to consider fully. They include level-of-trust variations, equipment variations, protocol and algorithm variations, and user security level combinations.

4 Policy and procedure issues. Several policy and procedure issues arose regarding the conduct of the summer study. That is, how might such a study be done better next time? They include alternative definition methods for both initial generation, small variations, and modifications during review; threat definition methods, including who defines them, who knows them, and the significance of perceived versus known threats; and design constraints, including design to cost, design to technical risk level, and design to threat-counter level.

APPENDIX A

USE OF KGs IN THE DDN

This appendix is classified CONFIDENTIAL and is bound separately. It is an update of Appendix A, "Cryptographic Equipment," of the original (January 1982) issue of the Plan [DCA82a]. Interested parties should request a copy from the DDN Program Management Office.

GLOSSARY

BBN	Bolt Beranek and Newman, Inc.
COI	Community of Interest
CONUS	Continental United States
CSC	Computer Security Center
DCA	Defense Communications Agency
DDN	Defense Data Network
DES	Data Encryption Standard
DoD	Department of Defense
E^3	End-to-End Encryption
HFEP	Host Front-End Processor
IP	Internet Protocol
IPLI	Internet Private Line Interface
KG	Key Generator
MC	Monitoring Center
MINET	Movements Information Network
MITRE	The MITRE Corporation
NAC	Network Access Component
RMC	Regional MC
SCCS	Software Configuration Control Procedure
SDC	System Development Corporation
SMC	System MC
S/R MC	SMC or RMC
TAC	Terminal Access Controller
TCP	Transmission Control Protocol
TEP	Terminal Emulation Processor
WIN	WWMCCS Intercomputer Network

REFERENCES

BBNDCA Bolt Beranek and Newman Inc. and the Defense Communications Agency, Statement of Work for Internet Private Line Interface (U), Draft, revised 25 March 1982, CONFIDENTIAL.

BBN89 Bolt Beranek and Newman Inc., The Interface Message Processor Program, Technical Information Report No. 89, revised December 1978.

BBN4823 _____, Network Utility [MC] Users Manual.

BBN4968 _____, Requirements for Stage 1 of the Gray Trunk Program, IPLI-82-1, April 1982.

BBN4968B _____, Appendix B -- Security Requirements for Stage 1 of the Grey Trunk Program (U), Draft, IPLI-82-11, 7 June 1982, SECRET/COMSEC/NOFORN.

BBN4974A _____, Gray Trunk Functional Design - Stage 1, Volume I, Revision 1, IPLI-82-4, October 1982, FOR OFFICIAL USE ONLY.

BBN4975 _____, Gray Trunk Functional Design - Stage 1, Volume II (U), August 1982, SECRET/NOFORN.

CSC83 DoD Computer Security Center, Trusted Computer System Evaluation Criteria, Final Draft, 27 January 1983.

DCA82a Defense Communications Agency, Defense Data Network Program Plan, January 1982, revised May 1982.

DCA82b _____, DDN Security Architecture, report of ad hoc working group, 4 November 1982, FOR OFFICIAL USE ONLY.

DCA82c _____, Director's memorandum to DUSD for C3I, "Subject: Defense Data Network -- Security Architecture Options," 19 November 1982.

DCA83a _____, Defense Data Network Management Engineering Plan.

DCA83b _____, Defense Data Network Subscriber Interface Guide.

DCA83c _____, Technical Assessment of the Application of BLACKER to the Integrated AUTODIN System, 12 April 1983.

DCEC82a This collection of papers documents the topology design analysis.

DCEC82b This collection of papers documents the survivability analysis.

FIPS46 National Bureau of Standards, Data Encryption Standard, Federal Information Processing Standards Publication 46, 15 January 1977.

FIPS81 _____, DES Modes of Operation, _____ 81, 2 December 1980.

FS1025 National Communications System, Interoperability and Security Requirements for Use of the Data Encryption Standard in the Network and Transport Layers of Data Communications, proposed Federal Standard 1025, 1 June 1981.

FS1026 _____, Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical and Data Link Layers of Data Communications, proposed Federal Standard 1026, 21 January 1982.

FS1027 General Services Administration, General Security Requirements for Equipment Using the Data Encryption Standard, Federal Standard 1027, 14 April 1982.

Lath82 Donald C. Latham, "Defense Data Network -- Security Architecture Options," Memorandum to Director DCA and Director NSA, 10 May 1982.

NSA82a National Security Agency, Security Review of the Architectural Options for the Defense Data Network (U), October 1982, SECRET.

NSA82b _____, Director's memorandum to DUSD (C3I), "Subject: Defense Data Network -- Security Architecture Options (U)," 1 November 1982, SECRET.

OPM78 [Office of Personnel Management,] United States Civil Service Commission, Federal Personnel Management Letter 732-7, November 14, 1978, Subject: Personnel Security Program for Positions Associated with Federal Computer Systems. Also is Enclosure 3 to DCAI 630-230-19.

READER'S COMMENT FORM
DDN Subscriber Security Guide

It is the intent of the Defense Data Network Program Management Office to support subscribers throughout the entire process of transitioning systems to the DDN. This Guide has been prepared to assist subscribers in one phase of that process.

Comments concerning this Guide may be made in the space provided below. Comments on the following topics are especially solicited:

1. What aspects of the Guide did you find most helpful?
2. What additions, deletions, or clarifications would make this Guide more useful?
3. What site-specific problems do you have that are not adequately addressed in this Guide?

Comments:

Please fill in the requested information.

Position: _____

Name (Optional): _____

Address (Optional): _____

Status of your system's current or planned DDN connectivity: _____

_____

Thank you for your cooperation.

Reader's Comment Form

Fold and tape | Please Do Not Staple | Fold and tape

Place Stamp Here

Defense Communications Agency

ATTN: DDN PMO, Code B610

Washington, DC 20305

Fold and tape | Please Do Not Staple | Fold and tape

END

FILMED

5-85

DTIC