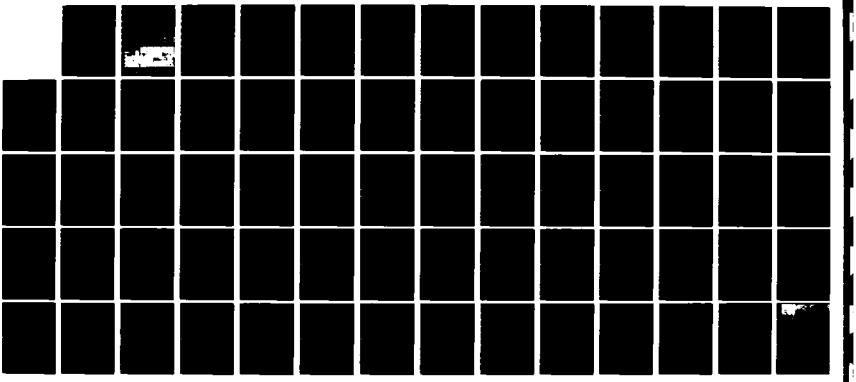
AD-A134 167 RECOMMENDED TEST AND EVALUATION AND INDEPENDENT VERIFICATION AND VALIDATI..(U) COMPUTER SCIENCES CORP FALLS CHURCH VA AUG 83 CSC-DDN-TE-1 DCA100-78-C-0053

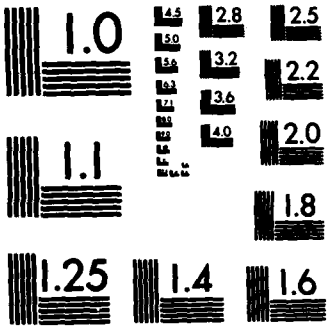
1/1

UNCLASSIFIED

F/G 5/1

NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

(2)

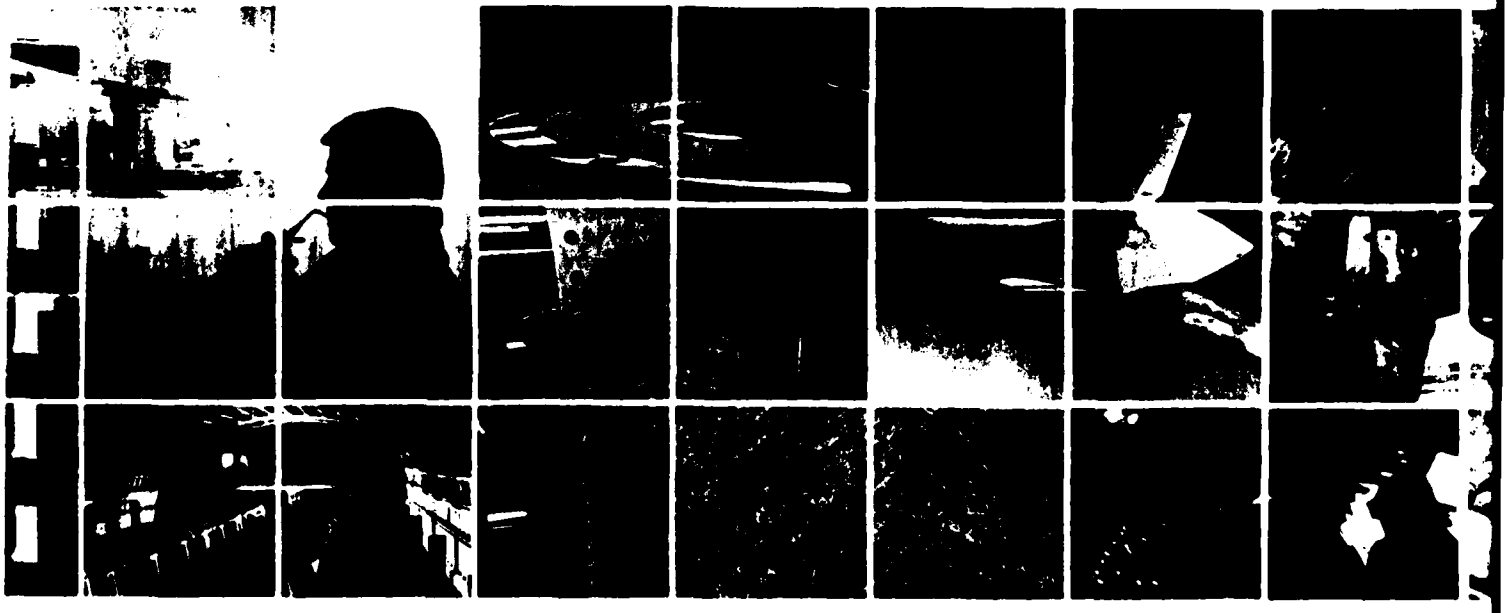
RECOMMENDED TEST AND EVALUATION AND INDEPENDENT VERIFICATION AND VALIDATION ACTIONS FOR THE DEFENSE DATA NETWORK

TECHNICAL REPORT DDN-TE-1

PREPARED FOR
DEFENSE COMMUNICATIONS AGENCY
WASHINGTON, D.C.

UNDER
CONTRACT DCA100-78-C-0053
TASK 6-83

AUGUST 1983



CSC

UNCLASSIFIED

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

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: DDN-TE-1	2. GOVT ACCESSION NO.: AD-A134167
3. RECIPIENT'S CATALOG NUMBER:	
4. TITLE *(and Subtitle)*: Recommended Test and Evaluation and Independent Verification and Validation Actions for the Defense Data Network	5. TYPE OF REPORT & PERIOD COVERED: Final Report June - August 1983
	6. PERFORMING ORG. REPORT NUMBER:
7. AUTHOR(s):	8. CONTRACT OR GRANT NUMBER(s): DCA 100-78-C-0053
9. PERFORMING ORGANIZATION NAME AND ADDRESS: Computer Sciences Corporation, 6565 Arlington Blvd., Falls Church, VA 22046	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: 33126K
11. CONTROLLING OFFICE NAME AND ADDRESS: Defense Communications Engineering Center, 1860 Wiehle Avenue, Code R110, Reston, VA 22090	12. REPORT DATE: August 1983
	13. NUMBER OF PAGES: 65
14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)*:	15. SECURITY CLASS. *(of this report)*: UNCLASSIFIED
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE:

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for public release; distribution unlimited.

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

18. SUPPLEMENTARY NOTES

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

Defense Data Network
Test and Evaluation
Independent Verification and Validation
Packet Data Network

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

This report identifies the major components of the Defense Data Network. Then the necessary test and evaluation actions are described and prioritized in order of their network operation.

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

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

RECOMMENDED TEST AND EVALUATION AND INDEPENDENT VERIFICATION AND VALIDATION ACTIONS FOR THE DEFENSE DATA NETWORK

TECHNICAL REPORT DDN-TE-1

PREPARED FOR

DEFENSE COMMUNICATIONS AGENCY
WASHINGTON, D.C.

UNDER

CONTRACT DCA100-78-C-0053
TASK 6-83

AUGUST 1983

COMPUTER SCIENCES CORPORATION

6565 Arlington Boulevard

Falls Church, Virginia 22046

Major Offices and Facilities Throughout the World

CONTENTS

CONTENTS
(Continued)

LIST OF ILLUSTRATIONS

LIST OF TABLES

1. INTRODUCTION

1.1 Purpose. This report has been prepared in response to Defense Communications Agency (DCA) Task Order 6-83, issued under the terms and conditions of Contract DCA100-78-C-0053 as amended. It constitutes Contract Data Requirements List (CDRL) Line Item 001 of the Task Order. In accordance with the Statement of Work (SOW), its purpose is to identify all Defense Data Network (DDN) testable components (hardware, software), assemblies, subsystems, integrated facilities, and subsystems; to describe the specific nature and objective of the tests required to assure proper network performance, including recommended schedules and locations; and to recommend which software and firmware developments should be monitored by Independent Verification, Validation, and Test (IVV&T).

1.2 Objective. The objective of this report is to provide to the Government, in an easily accessible form, information needed for the development of a Test and Evaluation Master Plan (TEMP) for the DDN. The requirement for a TEMP and, therefore, for the information contained in this report, stems from:

(a) The need to perform test and evaluation on DDN component elements and subsystems to assure proper network performance.

(b) The need for IVV&T of the critical software and firmware elements of the DDN.

(c) The need to develop general descriptions and objectives of performing Test and Evaluation (T&E) and IVV&T actions.

This report provides the information necessary to meet these requirements. Its content is in accordance with the requirements of Subtask 1 of the Task Description of Task Order 6-83.

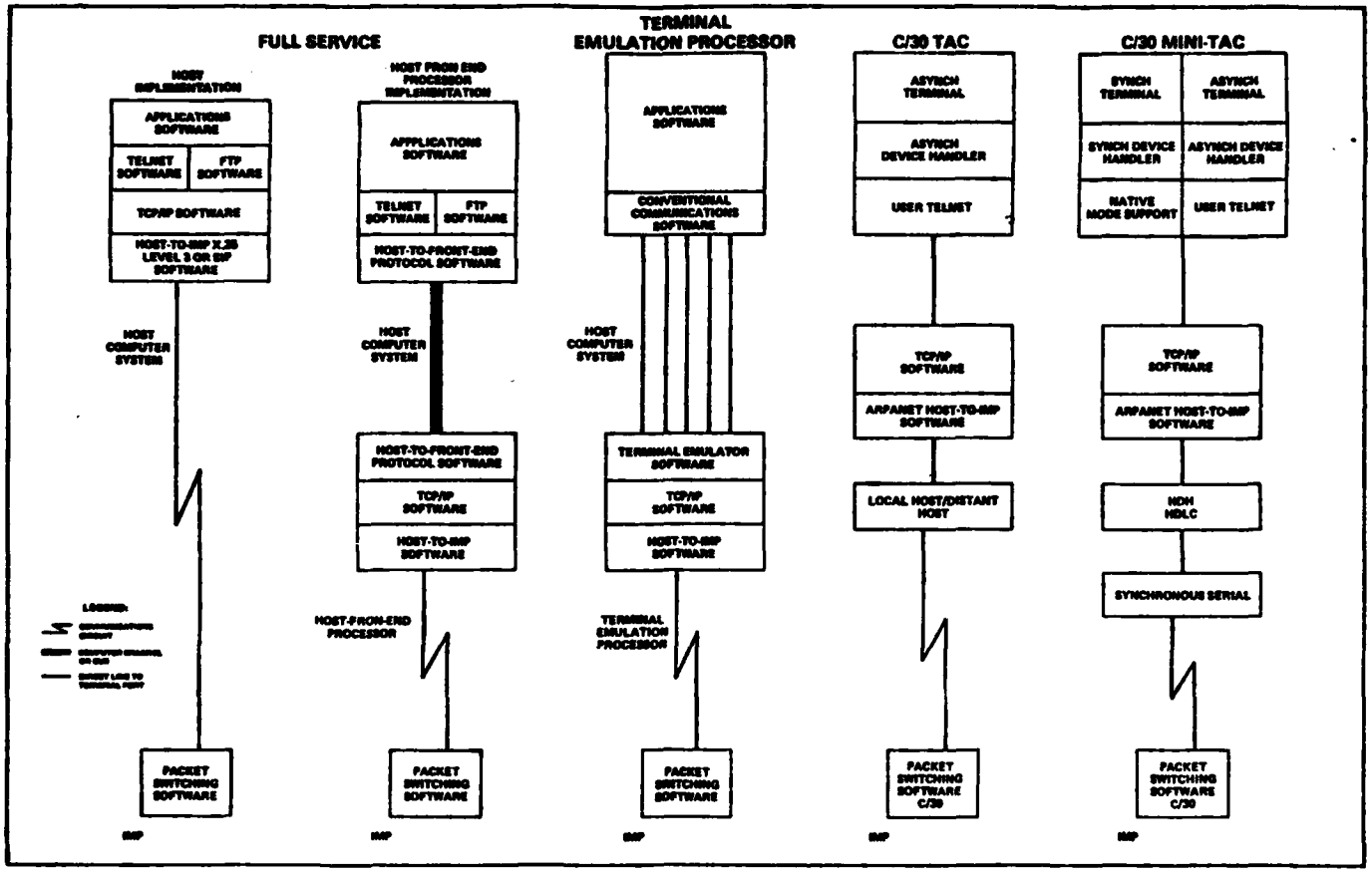
1.3 Background. The DDN, when fully developed, will be an integrated, packet-switching network serving the Department of

Defense (DoD). The DDN is made up of two functional areas: (1) the network backbone, which is based on Advanced Research Projects Agency Network (ARPANET) packet-switching technology and includes the trunk circuits and packet switches, and (2) the subscriber access network, which will enable the subscriber, through the use of circuits and interface equipment, to connect to the backbone.

The DDN backbone will contain approximately 200 packet switches at 100 sites. The hardware for the switches is the C/30 microprogrammed minicomputer, produced by Bolt, Beranek & Newman, Inc. (BBN). It will be compatible with existing ARPANET interface message processor (IMP) packet-switching software. Most backbone circuits will be leased landlines. They will be either digital (56 kbps) or analog (9.6 kbps overseas and 50 kbps in the continental U.S. (CONUS)). Links to overseas sites will be through satellite.

To access the network, subscriber hosts will connect to the backbone packet switches through Host Front End Processors (HFEPs) or Terminal Emulation Processors (TEPs), or directly through a portal on the host computer. These possible connections are illustrated in Figure 1-1. Host circuit transmission speeds will be 2.4 kbps to 56 kbps. Hosts requiring high network availability will be able to connect to more than one packet switch through multiple circuits. Terminal connectivity into the network will be by way of a Terminal Access Controller (TAC) or indirectly by routing through a host which is directly connected to the backbone. TACs, using either leased or dial-up lines, will accept up to 64 terminals. Line speeds will vary from 100 bps to 19.2 kbps. Each TAC will enter the backbone through a packet switch by way of a 4.8 kbps or 56 kbps line.

Four safeguards will protect network security. First, Internet Private Line Interfaces (IPLIs) will be used to provide end-to-end encryption and to separate the traffic by each level of security or by special communities of interest. Second, traffic flow



TP No. 043-9601

Figure 1-1. Subscriber Connectivity to DDN

security will be provided by link encryption used on the backbone trunks and access lines where required. The third measure is locating packet switches and TACs in restricted access areas. The fourth measure will be the TEMPEST certification of all C/30 packet switches and TACs.

DDN operational status control will be maintained through network Monitoring Centers (MCs). The MCs will conduct fault diagnosis and provide software maintenance for DDN. Currently it is planned to have a primary MC and designated alternate MCs in the United States, with regional MCs in Europe and the Pacific. MCs will also be provided for each separately keyed subscriber community. The MC will consist of one or more BBN C/70 minicomputers using the current ARPANET monitoring center NU software.

Development of the DDN will take place in four stages as reflected in the Program Plan. The first stage includes the ARPANET split into the Military Network (MILNET) and the Experimental ARPANET, and integration of the Movements Information Network (MINET) into MILNET. The second stage involves Network Access Component (NAC) availability for terminal access to DDN. The third stage involves integration of the IPLI for community of interest separation in an integrated network. The fourth stage occurs upon introduction of Blacker technology cryptographic devices. During stages two and three, other networks will be merged to form the fully developed DDN. Also, improvements and enhancements will be made as the system develops to meet the needs of more and more subscribers. Subscribers will, therefore, be added during each stage of development.

1.4 Scope. Although the development of the DDN does not follow the standard acquisition process with a T&E program structure to support that process, a well reasoned test program is required and attainable. The Defense Data Network Program Plan of January 1982 (Revised May 1982) gives the T&E Division of the DDN Program Management Office (PMO) responsibility for three levels of testing

for the DDN. The first is developmental testing, the second is initial operational testing, and the third is full operational testing. The draft Defense Data Network Management Engineering Plan (MEP), dated December 1982, describes three basic testing situations which, among them, include the three levels of testing mentioned in the Program Plan. They are:

(a) Testing, at the component level, of new or modified components (hardware and software) to verify that they perform in accordance with specifications. This includes testing of interfaces between two or more components.

(b) Testing of the equipment at a switching node or subscriber site when that site is added to the network.

(c) Testing which is necessary when a network is integrated into the DDN.

These situations include all necessary developmental and operational testing and provide a framework for identifying required DDN testing. This report, therefore, uses this three-part breakdown in describing appropriate T&E and IVV&T actions for the DDN. It is not within the scope of the report to describe testing procedures or to detail the testing methods to be employed. This information is appropriately included in test plans.

In accordance with the requirements of Department of Defense (DoD) Directive 5000.3, recommendations for Developmental Test and Evaluation (DT&E), Initial Operational Test and Evaluation (IOT&E), Follow-on Test and Evaluation (FOT&E), and Production Acceptance Test and Evaluation (PAT&E) are included.

1.5 Assumptions. In recommending T&E and IVV&T actions for the DDN, we have assumed that:

(a) There is no Defense Systems Acquisition Review Council (DSARC) milestone process applicable to the DDN.

(b) There is no Lead Military Department (LMD) to accomplish DDN Operational Test and Evaluation (OT&E) as defined in DoD Directive 5000.3.

(c) Operating tests described in this and other documents relevant to the DDN substitute for the operational tests according to 5000.3

(d) The structure for the DDN test program presented in the revised Program Plan of May 1982 and updated by the Draft Management Engineering Plan of December 1982 provides the basis for test planning.

(e) Prioritization of test recommendations in groups 1 through 5, as described in Paragraph 2.3, meets the DDN PMO requirement for rank ordering the recommendations.

(f) Test recommendations for the DDN can be made on the assumption that all required resources will be available to accomplish the test program.

(g) Operational control of the DDN network by DCA during the period operating tests are conducted will be sufficiently strong to complete valid testing requirements.

1.6 Methodology. Figure 1-2 depicts the methodology used in performing Subtask 1.

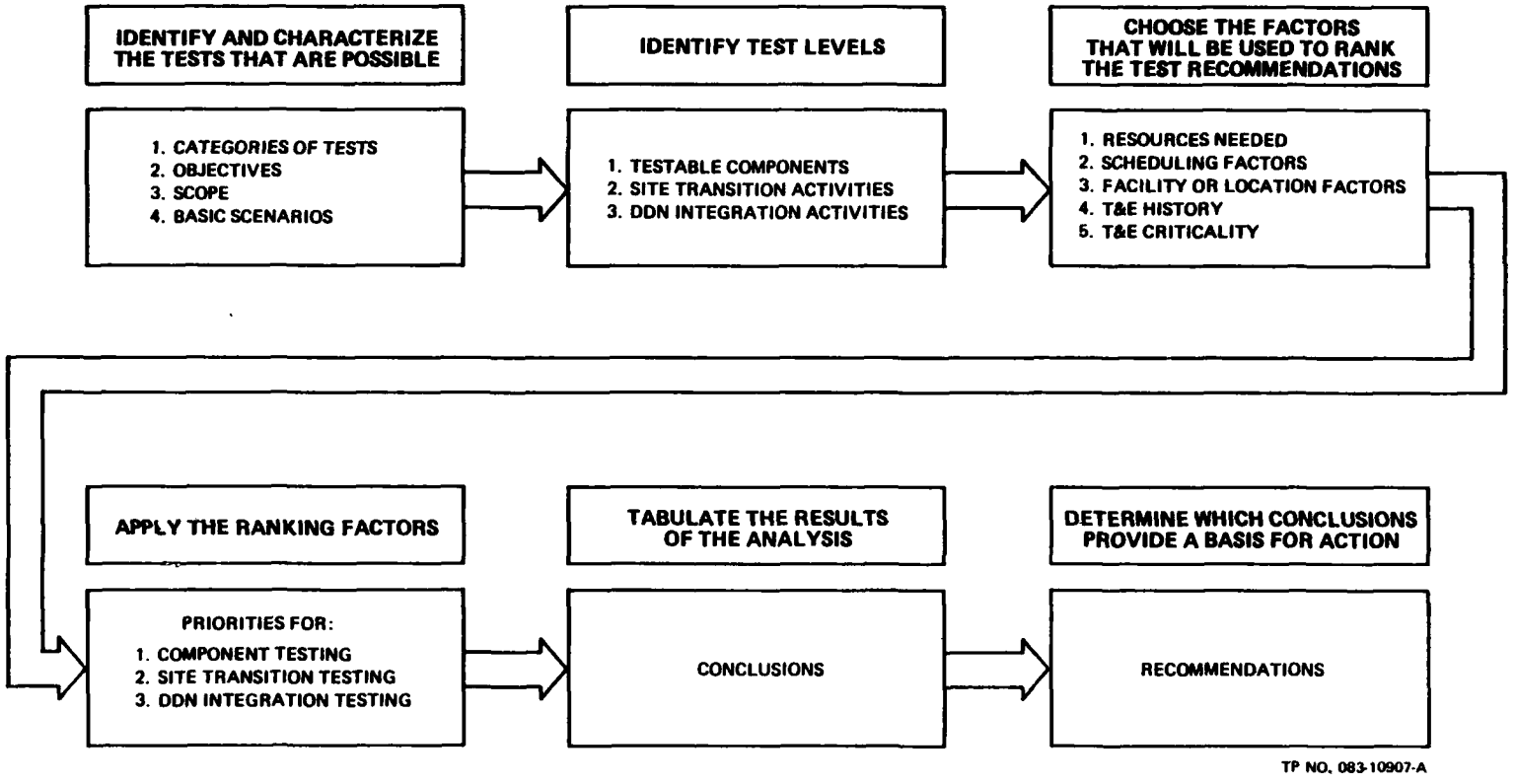


Figure 1-2. Study Methodology

2. TEST AND EVALUATION REQUIREMENTS ANALYSIS

2.1 DDN Test Situations.

2.1.1 Testing at the Component Level. The purpose of component testing is to verify that each unit of hardware or software performs in accordance with its design specifications. It assures that the development of the component has been completed satisfactorily and that hardware and software components will be trouble-free when integrated at a site. It is conducted before installation of hardware and software at a site and before their integration into the network. Component testing also includes testing of lines as appropriate and required.

2.1.1.1 Objectives. The following specific objectives can be achieved through component testing:

(a) Verify that components have been developed in accordance with, and meet all, design specifications.

(b) Verify that hardware and software components have been properly integrated.

(c) Obtain data on component performance in either a laboratory or operational facility.

2.1.1.2 Scope. The scope of testing is different for hardware and software component items. Hardware testing may be conducted in any or all of seven areas:

(a) Design Verification - does the item meet design and performance specifications?

(b) Reliability - will the equipment support the user?

(c) Environmental - does the equipment perform in the required operational environment?

(d) Maintainability Prediction - what is predicted downtime as it relates to required operating time?

(e) Human Engineering - how can the effectiveness of man-machine interfaces be maximized?

(f) Electrical - EMI, ESD, TEMPEST, and HEMP testing

(g) Endurance - does the equipment meet its performance requirements for its intended life?

Software tests may be conducted in any of three areas:

(a) Performance - does the software perform to its specification?

(b) IVV&T - does the software meet design specifications as independently determined?

(c) Quality Assurance - does the already existing or acquired software function properly?

2.1.1.3 Basic Scenarios. Government involvement in component testing normally begins with selected testing of a component under development in the developer's facility. The amount of this involvement will vary according to several factors. If the component being developed is very complex, the Government may direct or conduct testing at each stage of development to assure that each has been completed satisfactorily. Similarly, if developing the component requires the development of new technology, testing at each stage of development may be dictated. Another factor is the cost of a failure of the development effort. When component development costs are low, the cost of testing during development may not be justified, but as development costs increase the benefit from developmental testing likewise increases.

While these factors must be considered for both hardware and software, they are most likely to dictate Government-directed testing during the development of software, since software costs are already high and still increasing out of proportion to the rate of cost increase for hardware. Experience has shown that it is best to monitor and test software during its development rather

software during its development rather than to allow errors to remain undetected until the software is put into operation. If the software development effort is not successful, it is difficult to recoup the resources expended, and remedial efforts may not be possible within the limits of schedules and available resources.

One strategy that can help prevent these problems during the development of new software is Independent Verification, Validation, and Testing, the use of an independent authority to conduct checks and tests during the software development process. IVV&T increases the probability of error detection and correction, thereby enabling successful completion of the development program.

Not all DDN software will be newly developed. In certain cases the DDN PMO will acquire software which has been developed under other auspices. In these instances, a well developed and properly executed quality assurance (QA) program is the appropriate method for assuring that the software meets performance specifications.

When development of a hardware or software component is complete, Government acceptance testing is conducted. This testing may be done in the developer's facility or in a Government test facility. This testing normally constitutes an end item operating check at varied levels of loading, stress, and environmental extremes. The nature of the components governs the nature of the test facility required. Some components may be tested very simply. For other components, a test network or special test driver could be required to fully verify hardware and software component capabilities.

This level of testing ensures that a hardware or software component is ready to be installed at a site and integrated into the network. While additional testing of components will take place in the form of integration and network testing, this level of component testing assures that site or network integration can begin with a high degree of confidence in the component's performance.

2.1.2 Site Transition Testing. Site transition testing consists of those tests needed to ensure that DDN installed equipment has been properly integrated, operates in accordance with design specifications, and provides the subscriber with the required functional capabilities. Site transition testing includes testing at switching node sites to ensure proper operation of the DDN backbone elements and testing at subscriber sites to bring user host computers and terminals on-line. It is an integral part of site transition and cutover, and when completed successfully, assures that the site is interacting correctly with the DDN.

2.1.2.1 Objectives. The objectives of site transition testing are:

(a) To assure that site hardware and software are properly interconnected and operationally compatible with connected DDN facilities and equipment.

(b) To assure that the site meets all protocol requirements for interface formats and codes.

(c) To assure that proper operational techniques have been developed for processing DDN traffic under normal and abnormal conditions.

2.1.2.2 Scope. Subscriber site transition testing is conducted primarily to determine the readiness of a site to accomplish the transition to the DDN and to determine that the transition has been accomplished successfully. Testing therefore consists of:

(a) On-site inspection, acceptance, and integration of DDN supplied components

(b) Diagnostics of hardware and software

(c) Testing of system functional capabilities with DDN equipment installed.

2.1.2.3 Basic Scenarios. Subscriber site transition testing should be conducted as a part of each subscriber site's transition

to the DDN. Subscriber equipment testing is the subscriber's responsibility; the DDN PMO is responsible for DDN supplied equipment and for switching node sites. Normally site transition testing should follow this sequence:

(a) Inventory of all equipment and documentation necessary to accomplish cutover for the site.

(b) Inspection of all equipment to ensure its satisfactory installation and readiness for testing.

(c) Diagnostic testing of equipment to ensure its readiness for operational testing.

(d) Operational testing of site equipment independent of the network.

(e) Operational testing of site equipment utilizing the partitioned network.

(f) Operational testing of site equipment utilizing the full network.

Synergistically, these actions will allow a successful transition to the DDN. Detailed procedures for conducting the necessary tests should be described in the test plan and accompanying documents. The test plan should be written to support the transition and cutover plans for the site.

In order to conduct site transition testing, close coordination with operators and system users is necessary. DDN transition testing should be accomplished with as little network disruption as possible. Nevertheless, some restriction of operational traffic will be unavoidable. This restriction can be minimized through detailed planning and well coordinated transition, cutover, and test efforts.

2.1.3 DDN Network Integration Testing. Network integration occurs as the DDN develops in levels through the integration of MINET, the DoD Intelligence Information System (DODIIS), the Strategic Air Command Digital Information Network (SACDIN), the

WWMCCS Intercomputer Network (WIN), and the SECRET Network with the MILNET. Testing at each stage in the development of DDN is intended to verify the capability of network hardware and software to fulfill the requirements of the network functional baseline. These operating tests conducted on existing networks may be considered in the context of operational tests, according to DoD Directive 5000.3.

2.1.3.1 Objectives. Network integration objectives are:

(a) Exercise and test all areas of system hardware and software to verify that they meet the total requirement of the specification.

(b) Demonstrate that the packet-switching (PS) software and hardware will provide packet integrity and protection with reliable security provisions under all operating conditions while simultaneously meeting requirements for traffic flow, speed of service, routing, throughput, reliability, and availability.

(c) Assure that the switching subsystems, trunking networks, and access area subsystems are integrated for proper network operation..

(d) Demonstrate the capability of the network control facilities to monitor and control the network under both normal and abnormal conditions.

(e) Verify and validate all applicable operational manuals and support documentation.

(f) Validate system performance in providing data transfer services for various transaction scenarios.

(g) Assure that the network meets security requirements.

2.1.3.2 Scope. Network integration testing is designed to verify network performance and acceptability in the following areas:

(a) System performance - discrete testable technical parameters, such as throughput, defined in specifications.

(b) Data handling and control - functional and operational software procedures and protocols that permit traffic and services in accordance with specifications.

(c) System security - subnetwork separation of traffic and system packet integrity and protection.

(d) Network reliability and availability - the probability that the system will support the user and provide the necessary operating time.

2.1.3.3 Basic Scenarios. Network integration testing should be conducted in four phases to provide a gradual transition onto the network of the equipment and procedures being tested. This phase-in will reduce to a minimum the possibility that malfunctions encountered during testing will adversely affect operating portions of the network. It will provide the maximum assurance of proper operation before proceeding to the next step in integration.

In the first phase of testing, network functionality can be simulated in a test facility. The test facility simulates a limited node network, thus allowing hardware and software components to be tested functionally at the unit, subsystem, and system levels; this also allows their testing as parts of a simulated network. If this phase of testing is completed satisfactorily and if it is established that all components are functioning correctly both independently and as components of a test network, the equipment under test can be moved to an operating site for the next phase of testing.

The second phase consists of intrasite testing with a host or hosts to assure proper functioning of host/network interfaces. It also assures that the network components under test provide the proper services to host systems and subscribers.

In the third phase of testing, functionality is tested using a portion of the live network. The purpose of partitioning the network in this phase is to conduct actual network testing while limiting the risk of malfunction or disruption of the network. It allows almost complete, low-risk testing of network functionality with the minimum amount of interference to network operational traffic.

Phase four consists of the remaining tests to be conducted with the full network. If previous phases have been conducted correctly, and if problems have been corrected as they appear, this final phase of testing can be carried out with minimal risk to the network and with minimal interruption of operational traffic. The tests in this phase will serve as a final check for correct network performance.

Like site transition testing, network integration testing must be carefully planned and coordinated. Test plans will contain schedules, responsibilities, test objectives, descriptions of the required test documentation and other information required to coordinate and conduct the necessary tests.

2.1.4 Independent Verification, Validation, and Testing (IVV&T). IVV&T is intended to provide additional objective assurance that a software component has been developed to meet the specification and satisfy the functional requirements. IVV&T is most useful when the development process for a component is particularly long or complex or when there is a high probability of undetected errors during development. IVV&T seeks to reduce the possibility of undetected errors during the development process and to provide independent verification that the development process has been successful. IVV&T should be considered as developmental testing within the purview of DoD Directive 5000.3.

The purpose of IVV&T is to assure quality in software under development. The DDN PMO will, however, acquire certain software

that has been developed by others or assume responsibility for certifying software used by others. IVV&T and acceptance testing procedures are not appropriate in these cases. Instead, strict QA procedures should be used to certify this software. QA procedures should be developed on the basis of approved QA policies. They can fulfill the same purpose for acquired software as T&E can for newly developed software.

2.1.4.1 Objectives. As the name suggests, IVV&T has three objectives. The first is independent verification of system requirements to assure that they are correctly stated and that all requirements will be satisfied in the design.

The second objective is to validate that the software has been designed and developed in such a way that all valid requirements are satisfied.

The third objective of IVV&T is to conduct tests necessary to provide assurance that the software performs to specification.

2.1.4.2 Scope. IVV&T could be appropriately applied to any software system development effort. Its scope is therefore unlimited. Its most common application, however, is in complex software development efforts susceptible to undetected errors which may jeopardize the success of the whole project. In such instances, the cost of IVV&T may be small in relation to the loss incurred if the development effort fails and requires major post-test reworking.

2.2 Identification of DDN Test Items.

2.2.1 Testable Components. The DDN can be functionally subdivided into six groups: the backbone, access approaches, security, monitoring systems, test systems, and support systems. Each of these functional groups can be further broken down into system elements or components as shown in Table 2-1. The backbone components include the C/30 packet switches and the communication trunk lines. The access approaches include the three interface

Table 2-1. DDN Testable Components

FUNCTIONAL AREA	ELEMENT NOMENCLATURE*
DDN Backbone	C/30 Switch Node
	Trunk Lines
DDN/Access Systems	NAC
	- Mini-TAC
	- HFEP
	- TEP
	HID
	Access-Line Modems
	TAC
	Statistical Multiplexers
DDN/Security	IPLI
	Switch Level Gates
	Mailbridges
DDN/Monitor	Network Monitoring Center Equipment
	Power and Environment Monitor
	Automatic Line Restoral Option
DDN/Test Systems	System Test Facility
	Patch and Test Modules
DDN/Support Systems	Mobile Reconstitution Van
	Software Development Facilities
	Network Information Center (NIC)

*Includes software as well as hardware subelements.

methods by which a host can connect to the DDN: the Host Front-End Processors (HFEPs), the Host Interface Devices (HIDs), and the Terminal Emulation Processors (TEPs). Also included in the access approaches are the two means by which terminals may access the DDN: the TACs and the mini-Terminal Access Controllers (mini-TACs). The mini-TACs, HFEPs, and TEPs can be configured from a common-based microprocessor called the Network Access Component (NAC). The statistical multiplexers that will support several terminals connected to a remote mini-TAC are also part of the access approaches, along with the access line modems. The DDN security elements are the IPLI and the switch-level gates which will maintain community of interest separation on DDN, and the mailbridges. The monitoring system components are the DDN MC equipment, the Power and Environment Monitor (PEM), and the Automatic Line Restoral Option (ALRO). The DDN. Test systems including a system test facility, and limited digital patch and test modules at each subscriber site. Finally, the DDN support system consists of the Mobile Reconstitution Vans, software development facilities, and the Network Information Center (NIC).

The purpose of the remainder of this section is to recommend general test approaches for these components. Based on the projected completion date of their development, the testable components are categorized within the stages of the planned evolution of the DDN. Test approaches cover software as well as hardware. Testing of these components may be considered as including developmental testing as well as production acceptance testing within the purview of DoD Directive 5000.3.

2.2.1.1 Stages I and II. Stage I of the DDN began in fiscal year (FY) 1982 and extends through the third quarter of FY 1984. Stage II of the DDN immediately follows the end of Stage I and extends to the end of FY 1985. During this stage, the NAC will be available for host access to the DDN.

With the exception of the production IPLIs, Blacker technology security devices, and the integration of elements in the Mobile Reconstitution Vans, all system components should be completed within Stages I and II.

2.2.1.1.1 Hardware. Hardware testing that applies to the DDN elements falls into seven categories: design verification, reliability, environmental, maintainability, human engineering, electrical, and endurance testing.

Design verification testing determines equipment compliance with all applicable design and performance specifications. It is usually applied to newly developed or modified equipment.

Reliability testing provides the Government reasonable assurance that established minimum acceptable reliability requirements have been met before items are approved for mass production. It applies to items that are newly designed, have undergone major modification, or have failed their allocated reliability requirements under new system conditions (severe environmental stress, for example).

Environmental tests determine component performance under the stress of natural and induced environments peculiar to military operations. In those cases where the DDN equipment is located in a controlled environment within a building, little or no environmental testing will be required. Nominal electronic and thermal stress tests are also appropriate for this type of fixed ground equipment. Since environmental tests focus on basic survivability characteristics of equipment, they should be performed concurrently with the early stages of reliability testing for conditions expected to be encountered.

Maintainability testing attempts to predict the number of hours that a system will be inoperative while it is undergoing maintenance. It highlights those pieces of equipments which,

because of poor maintainability, require improvement, modification, or change of design. In addition, it allows the user to make an early assessment of whether the predicted downtime along with the quality and quantity of personnel, tools, and test equipment are adequate and consistent with system operational requirements. In order to predict maintainability, the tester needs such information as the failure rate of the component, the number of spares carried, the number of test points, the nature of the test equipment to be applied, and the manning schedules of maintenance personnel. Provided that this information does exist, maintainability testing can be applied at any time after the development concept has been established.

Human engineering involves an analysis of the relationship between a piece of equipment and its human interface. Its purpose is to maximize effectiveness, simplicity, efficiency, reliability, and safety of operation, training, and maintenance. It should be done during the early stages of equipment development.

For the purposes of DDN, electrical tests will consist of electromagnetic interference (EMI) tests, electrostatic discharge (ESD) testing, TEMPEST testing, and high-altitude electromagnetic pulse (HEMP) testing. EMI testing, establishes techniques for measuring and determining the EMI characteristics (emission of and susceptibility to) of electronic equipment. Its purpose involves identification and protection of equipment whose performance might be adversely affected by electromagnetic impulses. In addition, EMI testing identifies equipment that emits electromagnetic waves, and methods of shielding it in cases where the effects of those waves might prove to be detrimental. ESD testing involves the identification and protection of equipment whose functions might be adversely affected by static electricity. It is usually applied to equipment which contains such exposed electronic parts as microelectronic and semiconductor devices, thick and thin film resistors, and chips.

TEMPEST testing is directed at ensuring that equipment does not produce compromising emanations. HEMP testing focuses on equipment protection in the form of electromagnetic shielding, line isolation, and surge arrestment. These forms of electrical testing are usually conducted during the latter part of the test cycle.

Endurance testing is one of the last tests to be performed in the development cycle. It can be broken down into three levels. The first level attempts to test an item under normal conditions to ascertain that it meets all of its functional requirements. The second level is overload testing, which stresses the component to its capacity and beyond to determine: 1) whether it can withstand certain stress thresholds and still function; and 2) if it does degrade under stress, how badly it will degrade, and what consequences that degradation will have on the overall host system functions. The third level may repeat some or all of the previous tests, but will do so in an environment that closely approximates the conditions expected in the operating environment. Since endurance testing goes beyond basic survivability analysis and stresses the test item beyond its capacity, it will be applied to those items where testing is considered most critical.

All system element hardware, excluding the production IPLIs, Blacker technology security devices, and the Mobile Reconstitution Vans, can be tested in the first two stages of DDN implementation. In analyzing the criteria for which tests to apply to which equipment, the development status of the equipment appears to be the most critical variable, along with its criticality to overall system performance. If a particular component already exists, such as an access-line modem or a TAC, it should have already proven itself in the field. It therefore should be subject to only minimal reliability and environmental testing to verify and correct any problems detected in operational

use. If an item is still being developed, then it is appropriate to test that component more thoroughly before placing it in the operational system. In this instance, the more rigorous endurance tests should be added to the basic design verification, reliability and environmental tests, along with electrical, maintainability, and human engineering testing. Table 2-2 gives a complete breakdown of each DDN system element, its functional area, the primary action office responsible for it, its major hardware subelements, development completion dates, and hardware test approaches.

Because of their unique functions, the trunk lines and the test equipment associated with the patch and test modules do not adhere to the standard type of component testing. For trunk lines, tests which address the problem of bit error rate in data transmission should be applied. One function of the MC is continual testing of operational circuits with in-use software to determine error rates. For the test equipment associated with the test modules, calibration tests should be performed.

Hardware component testing should be done at the vendor's facility when approved by the Government. If it is determined that a different test location is necessary (endurance, TEMPEST, and HEMP testing would fall into this category), a Government-approved test facility should be used. In any case, the Government should reserve the right to witness any or all testing.

2.2.1.1.2 Software. There are three basic approaches to testing software components. The first is performance testing at the time of acceptance from the developer, the second is utilization of IV&V&T, and the third is the implementation of a well defined QA program.

Performance testing is usually conducted at the time of acceptance by a test agency independent of the procuring agency. Performance testing is intended to exercise all the functions of the software to demonstrate that it is reasonably error-free. This testing ensures that:

Table 2-2. DDN Developmental Testing-System Element/Subelement Level

(Page 1 of 2)

FUNCTIONAL AREA		ELEMENT NOMENCLATURE	RESPONSIBILITY	HARDWARE SUBELEMENTS	DEVELOPMENT COMPLETION	TEST APPROACHES	SOFTWARE SUBELEMENTS	DEVELOPMENT COMPLETION	TEST APPROACHES
DDN BACKBONE		C/30 SWITCH NODE	DDN PMO	MINICOMPUTER (64K RAM)	AVAILABLE	RELIABILITY ENVIRONMENTAL VALIDATION	1. PRECEDENCE/ PREEMPTION 2. LOGICAL ADDRESSING 3. USER AUTHENTICATION 4. X.25 INTERFACE 5. CHARGEBACK ALGORITHM	FY 83 (STAGE I) FY 85 (STAGE II) FY 86 (STAGE II) FY 86 (STAGE II) FY 86 (STAGE II)	QUALITY ASSURANCE
		TRUNK LINES	DDN PMO	1. DEDICATED (2.4, 4.8, 9.6 kbps) 2. DUAL (19.2 kbps) 3. VOICE GRADE (19.2 kbps) 4. WIDEBAND (50 kbps) 5. DDS (56 kbps) 6. DIRECT CABLE CONNECTION (230 kbps)	AVAILABLE AVAILABLE AVAILABLE AVAILABLE AVAILABLE AVAILABLE	BIT ERROR RATE ANALYSIS	NONE		
DDN/ACCESS SYSTEMS	NAC	MINITERMINAL ACCESS CONTROLLER (MINI-TAC)	DDN PMO	1. MOTOROLA MC 68000 MICROPROCESSOR 2. SYNCHRONOUS TERMINAL/SWITCH DEVICE HANDLER 3. ASYNCHRONOUS TERMINAL/ ASYNCHRONOUS HANDLER 4. MODEMS/LOW, MEDIUM SPEED	FY 84 (STAGE I) FY 84 (STAGE I) FY 84 (STAGE I) AVAILABLE	DESIGN VERIFICATION/ RELIABILITY/ ENVIRONMENTAL/ MAINTAINABILITY/ HUMAN ENGINEERING/ ELECTRICAL/ ENDURANCE VALIDATION	1. TERMINAL ACCESS PROTOCOLS 2. HOST-HOST SOFTWARE (TCP/IP) 3. HOST-IMP SOFTWARE (HDH, HDLC) 4. ASYNC TERMINAL SOFTWARE 5. SYNC TERMINAL SOFTWARE	TBD TBD TBD FY 84 (STAGE I) TBD	IVV&T
		HOST FRONT END PROCESSOR (HFEP)	DDN PMO	1. MOTOROLA MC 68000 MICROPROCESSOR 2. HOST/UNIBUS INTERFACE 3. Q-BUS 1822 INTERFACE 4. Q-BUS/HDH INTERFACE 5. UNIBUS/1822 INTERFACE 6. UNIBUS/HDH INTERFACE	FY 84 (STAGE I) FY 84 (STAGE I) FY 84 (STAGE I) FY 84 (STAGE I) FY 84 (STAGE I) FY 84 (STAGE I)	DESIGN VERIFICATION/ RELIABILITY/ ENVIRONMENTAL/ MAINTAINABILITY/ ELECTRICAL/ ENDURANCE VALIDATION	1. TERMINAL ACCESS PROTOCOLS 2. HOST-HOST SOFTWARE (TCP/IP) 3. HOST–IMP SOFTWARE (HDH, HDLC) 4. CMOS CONTROL PROGRAM	TBD TBD TBD FY 85 (STAGE II)	IVV&T
		TERMINAL EMULATION PROCESSOR (TEP)	DDN PMO	1. MOTOROLA MC 68000 MICROPROCESSOR 2. SYNCHRONOUS TERMINAL/SWITCH DEVICE HANDLER 3. ASYNCHRONOUS TERMINAL/HANDLER 4. MODEMS/LOW, MEDIUM SPEED	FY 84 (STAGE I) FY 84 (STAGE I) FY 84 (STAGE I) AVAILABLE	DESIGN VERIFICATION/ RELIABILITY/ ENVIRONMENTAL/ MAINTAINABILITY/ HUMAN ENGINEERING/ ENDURANCE VALIDATION	1. COMMUNICATIONS SOFTWARE 2. TERMINAL EMULATOR SOFTWARE 3. HOST-HOST SOFTWARE 4. HOST-IMP SOFTWARE 5. ASYNC SOFTWARE 6. SYNC SOFTWARE	TBD TBD TBD TBD FY 84 TBD	IVV&T
		HOST INTERFACE DEVICE	DDN PMO	1. HARDWIRED LOGIC COMPUTER 2. MICROCOMPUTER CONTROLLED 3. HOST/UNIBUS INTERFACE 4. UNIBUS/Q-BUS ADAPTER 5. Q-BUS/HDH INTERFACE	FY 85 (STAGE II) FY 85 (STAGE II) FY 85 (STAGE II) FY 85 (STAGE II) FY 85 (STAGE II)	DESIGN VERIFICATION/ RELIABILITY/ ENVIRONMENTAL MAINTAINABILITY/ ELECTRICAL/ ENDURANCE VALIDATION	1. TERMINAL ACCESS PROTOCOLS 2. HOST-HOST SOFTWARE (TCP, IP) 3. HOST-IMP SOFTWARE 4. CMOS CONTROL PROGRAM	TBD TBD TBD FY 85 (STAGE II)	IVV&T
		ACCESS-LINE MODEMS	DDN PMO	1. ASYNCHRONOUS (0-300, 0-1200 BAUD) 2. SYNCHRONOUS (2400, 4800, 9600 BAUD-RACK-MOUNTED)	AVAILABLE	RELIABILITY/ ENVIRONMENTAL VALIDATION	NONE		

TP No. 083-10612-C-1

Table 2-2. DDN Developmental Testing-System Element/Subelement Level (Page 2 of 2)

FUNCTIONAL AREA	ELEMENT NOMENCLATURE	RESPONSIBILITY	HARDWARE SUBELEMENTS	DEVELOPMENT COMPLETION	TEST APPROACHES	SOFTWARE SUBELEMENTS	DEVELOPMENT COMPLETION	TEST APPROACHES
DDN/ACCESS SYSTEMS (CONTINUED)	TERMINAL ACCESS CONTROLLER	DDN PMO	1. MINICOMPUTER 2. ASYNCH TERMINAL/ DEVICE HANDLER	AVAILABLE AVAILABLE	RELIABILITY/ ENVIRONMENTAL VALIDATION	1. TERMINAL ACCESS PROTOCOLS 2. HOST-HOST SOFTWARE (TCP, IP) 3. HOST-IMP SOFTWARE 4. CHARGEBACK ALGORITHM	AVAILABLE AVAILABLE AVAILABLE	QUALITY ASSURANCE
	STATISTICAL MULTIPLEXERS	DDN PMO	1. TIMEPLEX MODEL (M401, M803, M804)	AVAILABLE	RELIABILITY/ ENVIRONMENTAL VALIDATION	NONE		
DDN/SECURITY	INTERNET PRIVATE LINE INTERFACE (IPLI)	DDN PMO	1. KG 84 CRYPTO 2. MC 68000 PACKET PROCESSORS	FY 85 (STAGE II) FY 86 (STAGE III)	DESIGN VERIFICATION/ RELIABILITY/ ENVIRONMENTAL/ MAINTAINABILITY/ ELECTRICAL/ ENDURANCE VALID.	1. IMP-IMP SOFTWARE 2. HOST-IMP SOFTWARE	FY 86 (STAGE II) FY 86 (STAGE II)	IVV&T
	SWITCH LEVEL GATES	DDN PMO	1. SWITCHGATE HARDWARE	FY 83 (STAGE II)	DESIGN VERIFICATION/ RELIABILITY/ ENVIRONMENTAL/ MAINTAINABILITY/ ELECTRICAL/ ENDURANCE VALID.	1. SWITCHGATE SOFTWARE	FY 85 (STAGE II)	PERFORMANCE VALIDATION
	MAIL BRIDGE	DDN PMO	1. MAIL BRIDGE HARDWARE	TBD		1. MAIL BRIDGE SOFTWARE	TBD	PERFORMANCE VALIDATION
DDN/MONITOR	NETWORK MONITORING CENTER EQUIPMENT	DDN PMO	C/70 MINICOMPUTER a. EXECUTION MACHINE b. DISKS c. ONE 800 bpi TAPE d. TERMINALS e. PRINTERS	FY 84 (STAGE I)	RELIABILITY/ ENVIRONMENTAL VALIDATION	1. UNIX OPERATING SYSTEM 2. HOST-IMP PROTOCOL 3. NU SOFTWARE 4. CHARGEBACK ALGORITHM	AVAILABLE FY 86 (STAGE II) 86 JANUARY (STAGE II)	QUALITY ASSURANCE
	POWER AND ENVIRONMENT MONITOR	DDN PMO	1. SENSORS 2. CONTROLS	FY 86 (STAGE II) FY 86 (STAGE II)	RELIABILITY/ ENVIRONMENTAL VALIDATION	1. HOST-IMP PROGRAM 2. DATA COLLECTION AND CONTROL PROGRAM	86 JANUARY (STAGE II) 86 JANUARY (STAGE II)	PERFORMANCE VALIDATION
	AUTOMATIC LINE RESTORAL OPTION	DDN PMO	1. MODEM 2. AUTOMATIC CALLING UNIT 3. DATA AB SWITCH 4. DATA LOOPBACK SWITCH 5. LINE LOOPBACK SWITCH 6. MASTER CONTROLLER UNIT 7. SLAVE CONTROLLER UNIT 8. DIAL-BACKUP ANSWER	OPTIONAL	RELIABILITY/ ENVIRONMENTAL VALIDATION	1. CONTROL PROGRAM	OPTIONAL	PERFORMANCE/ VALIDATION
DDN/TEST SYSTEMS	TEST FACILITY	DDN PMO	1. C/30 SWITCH NODES 2. MONITORING CENTER DEVICES 3. LINE CRYPTOS 4. IPLIs 5. TRUNK LINES 6. DIAL-UP LINES 7. TERMINALS SYNCHRONOUS/ ASYNCHRONOUS 8. LINE MONITORS 9. MODEMS - LOW SPEED MED SPEED	REFER TO INDIVIDUAL ELEMENTS (ACQUISITION DATE - 86 MARCH)		REFER TO INDIVIDUAL ELEMENTS		
	PATCH AND TEST MODULES	DDN PMO	1. VF PATCH AND TEST EQUIPMENT 2. DIGITAL PATCH AND TEST EQUIP 3. DIGITAL SWITCHING MODULE 4. TEST EQUIP a. ANALOG/DIGITAL TEST PANEL b. EIA BREAKOUT TEST PANEL c. DATA LINK ANALYZER	AVAILABLE AVAILABLE AVAILABLE AVAILABLE	ENVIRONMENTAL/ CALIBRATION VALIDATION	DATA LINK ANALYZER SOFTWARE		PERFORMANCE VALIDATION
DDN/SUPPORT SYSTEMS	MOBILE RECONSTITUTION VAN	DDN PMO	1. C/30e 2. C-70 3. MINI-TAC 4. IPLI 5. MODEMS 6. PATCH & TEST EQUIP	REFER TO INDIVIDUAL ELEMENTS		REFER TO INDIVIDUAL ELEMENTS		
	NETWORK INFORMATION CENTER (NIC)	DDN PMO	NIC HARDWARE	AVAILABLE	RELIABILITY/ ENVIRONMENTAL VALIDATION	NIC SOFTWARE	AVAILABLE	QUALITY ASSURANCE

TP No. 083-10812-C-2

(a) The software can satisfy all applicable system and program performance requirements.

(b) The software can properly interface with all interacting systems specified in the program performance requirements.

(c) The software conforms to all applicable requirements for design and documentation.

The usual criteria for ascertaining program conformance to specifications are appropriate functional response, accuracy (low error rate), and timeliness (quick response time).

Testing the software under stress conditions is an inherent part of performance testing. It is usually conducted by operating the program under test at saturation levels for certain periods during the performance testing. The purpose is to demonstrate that program degradation will not be catastrophic if the program is stressed at levels slightly past its design limits.

In certain cases IVV&T of software may be directed, in addition to the performance testing that should be conducted at acceptance. A decision to bear the additional cost of IVV&T will usually be made when the software to be developed is particularly critical to satisfactory network operation or when its development is expected to be unusually difficult or complex. In these cases it may be cost-effective for the PMO to engage an independent contractor to monitor the software development effort. Since the IVV&T is conducted during the period of development, the chances that the software will prove unsatisfactory during acceptance testing are significantly reduced. The method used in IVV&T is to verify requirements and validate that the software fulfills them at each stage of its development. This approach reduces the possibility that errors during development will accumulate and remain undetected until final testing. Since the cost of IVV&T is usually significant, the decision to use it should be made by assessing the impact of a failure to successfully complete a critical software module on time against the cost of IVV&T during its development.

A third approach to software testing is to employ QA policies and procedures to assure initial and continued satisfactory performance. This approach will be most appropriate for the DDN PMO in the case of acquired or assumed software. In the case of software developed elsewhere but acquired by the DDN PMO, QA audits should be conducted to determine the condition of the software and its documentation when acquired. Rigorously applying QA procedures will be the only method available to the PMO to assure that acquired software meets the same standards as software developed under the direction of the PMO.

When the DDN PMO assumes responsibility for certifying software developed and maintained elsewhere, rigorous QA will also be necessary. Requiring appropriate audits, adequate maintenance of documentation, and other QA tools will be the only means available to the PMO for ensuring that such software is maintained properly and continues to function satisfactorily.

Regardless of the testing approach used, all software, excluding that used in the production IPLIs, Blacker technology security devices, and the Mobile Reconstitution Vans, can be tested in the first two stages of DDN development.

Analysis of the criteria used for developing software testing recommendations shows that for software, as well as for hardware, the most important considerations are development status and criticality to the system.

If these criteria are applied to the DDN software, certain conclusions can be made. Because the software for the IPLIs and the network access approaches is critical to the performance of the DDN, and since much of it is still being developed, the more extensive IVV&T procedures should be undertaken. In cases where much of the software already exists, as in the case of the C/30 IMP and TAC, a comprehensive QA test program should be used. Also, as a minimum, extensive QA should be performed on additional

C/30 IMP and TAC and C/70 MC software such as the DDN chargeback algorithm. Finally, in those system elements where the software is still under development but does not directly impact network performance, as in the case of the PEM or system test facility, the performance test approach should be used.

Table 2-2 gives a complete breakdown of system element software with expected completion dates and test approach recommendations.

2.2.1.2 Stage III. Stage III of the planned evolution of the DDN will extend through FY 1986. In this stage, the number of IPLIs will be sufficiently high so that the three subnetworks can be combined into a single network supporting multiple levels of security.

2.2.1.2.1 Hardware. The only system elements involved in this time frame are the production IPLIs and the Reconstitution Vans. The hardware testing approach delineated in Paragraph 2.2.1.1.1 should also apply to these elements. Table 2-2 lists the approaches to be taken for these two items.

2.2.1.2.2 Software. Software testing will follow the rationale described in Paragraph 2.2.1.1.2.

2.2.1.3 Stage IV. Stage IV is the final stage of the DDN evolution. During this stage, any additional subscribers that need to access the network will be brought on-line by the DDN PMO.

2.2.1.3.1 Hardware. The final system element of the DDN, the Blacker security device, should be completed during this stage. More data is required on this device before testing approaches can be determined.

2.2.1.3.2 Software. The software subelements of the Blacker security device scheduled for completion in FY 1987 have yet to be determined.

2.2.2 Site Transition Testing.

(a) Site transition testing includes two basic test situations: (1) testing to insure that the node site equipment is installed and functioning properly, and (2) testing required to enable a subscriber to come on-line as a DDN participant. A testing approach that minimizes interruption of ongoing site operations should be used. Subscribers will enter DDN through a host port, TAC, mini-TAC, HFEP, or TEP and should ensure that their own site equipment is working to an established baseline. The host computer should be interfaced off-line to assure interoperability without degradation to the net. Once this is accomplished, controlled operating tests should be conducted in a NAC wraparound or partitioned net situation. The scope of testing is limited to operational suitability and system functional capability. The MC provides a loop-back capability for checking subscriber software efficacy. Subscriber site testing should also include certifying vendor-software interface.

(b) The testing concept for site transition testing starts with assessment and analysis of existing performance and proceeds with testing of DDN hardware and software required for connectivity. Hardware/software integration testing of site components and backbone components is performed to assure readiness for network integration.

(c) Assumptions and conditions. The assumptions and conditions for hardware, software, test tools, and special test conditions are as follows:

(1) Pass/Fail criteria have been objectively stated.

(2) The sites will be capable of supporting a test environment with their existing hardware inventory.

(3) The software components will support full network operations in consonance with the security environment.

(4) All local host and related software elements are compatible and fully integrated.

(5) System monitoring and data generation/ reduction packages will be made available to all who are involved in testing or problem identification.

(6) Checkout of participants, file space, and systems files will occur before scheduled testing begins. Operating tests will be conducted using the live network; however, sites should be prepared to fall back to an operational system. Sites also should ensure that operational messages are not processed when sites are running under test conditions.

(7) DDN testing will not extend into the subscriber's security system or procedures as he practices them on his host.

(d) Scheduling. Site testing should commence after the site representative and the DDN PMO representative have verified site topology and complete site preparation. Testing times should be coordinated with the DDN Test Director.

(e) Testing. When completed, site transition testing should verify objectives. The program will include testing of both hardware and software, evaluation of subsystem integration and total system operation, and demonstration of Test System subscriber interfaces. To be most effective and reduce the probability of duplicating tests, this program will be coordinated with network integration and cutover and implementation efforts. Government acceptance of the system will be based on

successful testing or demonstration of all end items through this integrated system test approach. Individual site tests should be conducted for host and subnet and DDN subscriber interfaces. Using contractor- developed plans and procedures, site testing will be performed in three phases: a pre-shakedown phase involving installation and checkout of individual configuration items (including software) and subsystems, a shakedown phase (dry run) to confirm interoperability of the site subsystems and to ensure readiness for the final phase, the formal site operational (acceptance) test, which will be performed under Government direction.

(f) Site Test Objectives. The following objectives apply broadly to all formal site acceptance tests to be performed:

(1) Installation and facility performance meets all requirements of the DDN functional baseline.

(2) The site hardware and software are properly interconnected and operationally compatible with DDN facilities and equipment.

(3) The site meets all protocol requirements for interface formats and codes.

(4) Proper operational techniques have been developed for processing traffic under normal and abnormal conditions.

(5) Site testing is conducted to determine operational suitability--that is, can the user get his job done with DDN under operational conditions. In addition, testing of subscriber interface hardware and software will include full operational compatibility and security testing with the host computers and terminals designated as test support systems or components.

It is essential that problems identified during testing be noted and documented, and provision made for analysis and possible resolution and correction. Hardware and software fixes should be submitted to the DDN PMO for a determination of the amount of rework and retesting required before field use.

2.2.2.1 Stages I and II Site Transition Testing.

Hardware	Software
C/30 Switch Node	1. Precedence/Preemption 2. Logical Addressing 3. User Authentication 4. X.25 Interface 5. Chargeback algorithm
Trunk Lines	None
NAC	
Mini-TAC	1. Terminal Access Protocols 2. Host-Host Software (TCP/IP) 3. Host-IMP Software (HDH, HDLC) 4. ASYNC Terminal Software 5. SYNC Terminal Software
HFEP	1. Terminal Access Protocols 2. Host-Host Software (TCP/IP) 3. Host-IMP Software (HDH, HDLC) 4. CMOS Control Program
TEP	1. Communications Software 2. Terminal Emulator Software 3. Host-Host Software (TCP/IP)

Hardware	Software
	4. Host-IMP Software (HDH, HDLC)
	5. ASYNC Terminal Software
	6. SYNC Terminal Software
HID	1. Terminal Access Protocols
	2. Host-Host Software (TCP/IP)
	3. Host-IMP Software
	4. CMOS Control Program
Access-line Modems	None
TAC	1. Terminal Access Protocols
	2. Host-Host Software (TCP/IP)
	3. Host-IMP Software
	4. Chargeback Algorithm
Statistical Multiplexers	None
Switch Level Gates	1. Switchgate Software
Mailbridges	1. Mailbridge Software

2.2.2.2 Stage III Site Transition Testing. This stage assumes all sites are on-line. If a site is not on-line, repeat Stages I and II testing plus Stage III testing.

Hardware	Software
IPLI	. IMP-IMP Software
	2. Host-IMP Software

2.2.2.3 Stage IV Site Transition Testing. This stage assumes all sites are on-line. If a site is not on-line, repeat Stage I and II plus Stage IV testing.

Hardware	Software
Blacker equipment	TBD

2.2.3 DDN Subsystem Integration Testing. This paragraph addresses the sequencing, methodology, and types of DDN integration testing required to establish an initial operating capability (IOC) for DDN. This integration testing must make certain that the combination of all the individual subnetworks retains the original technical performance and subscriber services of each. It must also ensure that required subnetwork separation and security of data are maintained and demonstrated. Testing at this level assumes that successful component and subscriber site transition testing have been accomplished.

Integration testing of the DDN will consist of five progressive phases. These phases are conducted in the following order:

(a) ARPANET split forming MILNET and Experimental ARPANET; and MINET formation and integration into MILNET

(b) C^2(WIN) and DoDIIS integration to form C^2I

(c) C^2I and SACDIN integration to augment C^2I

(d) C^2I and SECRET Network integration

(e) C^2I/SECRET Network and MILNET integration to establish a DDN IOC.

The objective of DDN integration testing is to verify the capability of the network hardware and software to fulfill network requirements as specified in the baseline documents. Four functional categories of integration testing have been identified, together with their corresponding test objectives. These are:

(a) System performance parameter tests - To verify the ability of the system to satisfy user and host requirements at a specified level of network performance.

(b) Network data handling and control tests - To demonstrate that the system's functional and operational structure, along with designed procedures and protocols, will actually transfer messages, transactions, and data from one subscriber to another through the network. In particular, to demonstrate that the system provides required interactive, query-response, narrative, and bulk data transfer services. Also to verify the adequacy of traffic management functions for network control, the system's capability to carry out the initialization functions, and its ability to recover from network disturbances.

(c) System security tests - To verify subnetwork separation and system packet integrity and protection, and to provide a preliminary basis for security certification.

(d) Network availability tests - To demonstrate that the percentage of time any pair of users are able to communicate with each other through the network is at least 99 percent for single-homed subscribers and 99.95 percent for dual-homed subscribers.

All five phases of integration testing will require validation of these four fundamental DDN test objectives, since each phase, upon successful completion, will produce progressive operational versions that must provide uniform DDN network performance.

Each of the four fundamental objectives has a corresponding set of testable functions which will be demonstrated for DDN validation. These testable functions will vary somewhat, however, for each of the five integration phases. For example, security testing for the MILNET integration will not be as extensive as security testing for the C^2 (WIN) and DoDIIS integration. Nevertheless,

a representative set of these functions is provided in Table 2-3. Tailoring will be more appropriately defined in the Test Procedures. Table 2-3 also shows the traceability of these required functions to the Program Plan.

Four types of methodologies can be employed to validate the DDN testable functions in integration testing. These include, in their usual progression:

(a) Network test facility

(b) Intrasite host wraparounds/backbone network wraparounds

(c) Live partitioned network

(d) Live network.

The network test facility will serve two purposes during DDN integration testing. It can simulate a partitioned network or it can be configured to act as a node in a larger network. When configured to serve as a simulated network with no connection to the actual networks that make up the DDN, it can serve as an isolated testbed for component testing. Configured as one or more nodes on the DDN or a subnetwork of the DDN, it can be used to test component, assembly, or subnetwork functionality.

Using the test facility in these ways will constitute the first step in DDN integration testing and allow a maximum amount of testing with minimal risk.

Intrasite host wraparounds are also an effective methodology for testing and validating host and subnetwork hardware and software. Host wraparound simulates, within the host, the testable functions of all DDN network activities, including responses from the network. Using this capability better ensures intrasite integrity and a stable platform for subsequent network test and analysis, and allows validation of the host software and much of the test software before live network entry. A network wraparound can also be employed to ensure proper functioning of the network backbone.

Table 2-3. DDN Testable Functions and Requirements Traceability

OBJECTIVE	DDN TESTABLE FUNCTION	PROGRAM PLAN SECTION
Network Performance Parameters	Backbone Delay	4.1.2/1.2.2
	Undetected Bit Error Rate	3.2.4/1.2.2
	Trunk Transmission Speeds	2.9
	Node Steady State Throughput	2.1.2
	Node Peak Throughput	2.1.2
Network Data Handling and Control	Misdelivery	3.2.5
	Automatic Diagnosis and Recovery	3.2.2
	Reconstitution	3.4.1.4
	Preplanned Rehoming	3.4.1.5
	Reserved Capacity	3.4.1.6
	Capacity/Stress Levels	3.4.3
	Graceful Degradation	3.4.1.8
	Dynamic Adaptive Routing	3.4.1.7
	Protective Mechanisms	3.2.3
	Precedence/Preemption	3.1
Network Security	Link Encryption	3.3.1
	Security Level Separation	3.3.2
	Separation of Communities of Interest	3.3.3
	Individual Access	3.3.4
	Intercommunity Operation	3.3.6
	End-to-End Encryption	1.2.4
Network Availability and Reliability		3.2

Live partitioned networks can be used once the intrasite and network wraparounds have been completed. Any limited combination of new and operational DDN sites can be configured to demonstrate the full range of the testable DDN functions previously outlined.

Finally, all member sites interact to ensure that all DDN functions are tested and perform in accordance with design specifications.

2.2.3.1 Stages I and II.

2.2.3.1.1 Hardware. With the exception of production IPLIs, the Mobile Reconstitution Vans, and Blacker technology, all DDN equipment should be integrated on the separate C^2I (WIN and DoDIIS), SECRET, and MILNET subnetworks in this period. Hardware system performance functions as outlined in Table 2-3 can be tested on the subnetwork level to ensure continued original performance in accordance with the specifications for each. Only C^2I, however, can exercise a representative range of DDN testable functions at this point, and can do this only on a partitioned network basis since limited prototype IPLIs will be available. Moreover, tests must make certain that the required separation of data is maintained across all subnetworks of DDN.

2.2.3.1.2 Software. Most of the DDN software, except that required for the hardware noted in Paragraph 2.2.3.1.1, should be available for integration testing on the C^2I, SECRET, and MILNET subnetworks. The testable software functions are network data handling and control and system security, as detailed in Table 2-3. Again, this testing will deal mainly with the original individual subnetwork performance, since full DDN performance testing can only be accomplished when production IPLIs become available in Stage III.

2.2.3.2 Stage III.

2.2.3.2.1 Hardware. When production IPLIs are available, full DDN hardware integration testing can proceed and will be phased as

previously defined. The testable functions that must be validated for each of the remaining four phases of integration are defined in Table 2-3 in system performance parameters.

2.2.3.2.2 Software. Full DDN software integration testing will proceed in accordance with the testing of functions outlined in Table 2-3 for network data handling and control and system security. At the conclusion of successful integration testing in this stage, the three subnetworks (C^2I, SECRET, and MILNET) will operate as a single network supporting multiple levels of security with adaptive routing. This will establish the initial operating capability (IOC) of DDN.

2.2.3.3 Stage IV.

2.2.3.3.1 Hardware. Blacker security devices made available in this timeframe will require the same DDN integration testing as outlined for the introduction of IPLIs in Paragraph 2.2.3.2.1.

2.2.3.3.2 Software. Testing requirements for integration are the same as those outlined for IPLIs in Paragraph 2.2.3.2.2.

2.3 Description of Test Ranking Factors.

2.3.1 T&E and IVV&T Priority Groups. To establish priorities among DDN hardware and software test recommendations, the following five groups of T&E and IVV&T are established:

(a) Priority 1 - highest priority assigned to required testing. Designates those tests and IVV&T activities determined to be most essential to development and operation of the DDN. Includes all testing necessary to demonstrate compliance with contractual requirements.

(b) Priority 2 - extremely important test directed, for example, at ensuring the integrity of the system in terms of service to the user as well as control of the network.

(c) Priority 3 - test and validation activities that provide added assurance that objectives will be met and/or are conducted for the purpose of substantiating previous test results.

(d) Priority 4 - test and validation actions performed on support equipment not directly involved in network operation.

(e) Priority 5 - ancillary testing directed at long-range improvements and upgrading system performance.

2.3.2 Test Histories of Hardware and Software Items. A major factor to consider in rank ordering test recommendations is the test history of each hardware and software item which comprises the DDN. Testable components of the system range from items which have a long operational history to new development items that are not yet proven operationally.

Maturity of software items range from fully developed off-the-shelf packages which have undergone extensive testing and debugging to items planned for development under Government contract or auspices for special DDN application.

This factor for establishing priorities focuses on the stage of development of the hardware and software items and depends on the availability of appropriate test documentation.

2.3.3 Hardware and Software Criticality and Complexity. Criticality and complexity of hardware and software items bear heavily on the ranking process. Criticality addresses primarily the functions the equipment and software elements are required to perform and involves a judgement of how essential each element is to network operation. Assessment of complexity focuses on hardware design and software programming aspects.

2.3.4 Distribution of Hardware and Software Items Throughout the Subnetworks. The extent to which hardware and software items are used throughout the subnetworks affects priorities for T&E and

IVV&T program recommendations. A high incidence of item commonality favorably affects the test/benefit ratio and supports a modular test approach.

2.3.5 Resources Required to Accomplish the T&E and IVV&T Efforts. The DDN T&E and IVV&T program recommendations may be influenced by the amount and availability of resources required to accomplish the proposed tests. Similarly, tests which require expending considerable resources to develop a new test facility or modification may be given a lower priority than would otherwise be the case if an existing test facility could be used as is for the testing.

2.3.6 Sequencing and Scheduling Considerations. The priority assigned to a particular test or IVV&T recommendation may stem from timing considerations as well as program dependencies and sequencing relationships. Network integration milestones, for example, or major decision points may dictate test priorities at various stages of DDN implementation.

Figure 3-1 shows the schedule for the development of the DDN, together with a plot of the growth of the number of nodes over time and a plot of the major milestones in component development. This way of depicting DDN development activity indicates when major T&E activity must take place. The amount of node site transition testing necessary at any time can be derived from the plot of node growth. Time available for DDN integration testing can be obtained from the plot of network integration activities. Component testing schedules and plans will have to be developed after consideration of the component development schedules shown in the lower third of the figure.

2.4 Application of Test Ranking Factors.

2.4.1 Component Level Testing. In assigning priorities to the testing of system elements of DDN, the two major considerations are the stage of development of the element, and its importance to the performance of system functions. If an element or a major part of that element is still in the process of being developed,

then it should require more testing than an element that has already proven itself in the field. Likewise, components that are essential to the actual utilization of the DDN, such as the network access software and the IPLI software, must be considered more important than such supportive elements as the Power and Environment Monitor (PEM) or the Mobile Reconstitution Vans. The priority ranking attempts to incorporate these distinctions in criticality to network performance with stage of development to obtain relative levels of importance for testing the system elements of DDN.

Table 2-4 lists all DDN system elements (hardware and software) according to their development status, criticality to network performance, recommended test approaches to be applied, and priority ascribed to that testing. The importance levels are relative only to the elements themselves, with 1 being the highest level of importance and 5 being the lowest.

2.4.2 Site Transition Testing. Site transition testing is conducted to ensure that:

(a) The site is ready for cutover to DDN.

(b) The site host subnetwork is not affected by DDN components.

(c) DDN components are not adversely affected by site subnet equipment.

For these reasons, all site transition testing shown in Table 2-5 is considered as priority 1 except for the establishment of the baseline prior to DDN upgrade. Site configuration baseline testing is part of the overall data base required for documenting system performance before DDN access, and is assigned priority 2.

2.4.3 Network Integration Testing. Network integration testing should carry the highest priority. It is imperative that testing at this level fully verify that DDN provides each subnetwork

Table 2-4. Component Level Testing Priorities
(Page 1 of 3)

DDN SYSTEM ELEMENT	DEVELOPMENT STATUS	CRITICALITY TO NETWORK PERFORMANCE	RECOMMENDED TEST APPROACH	PRIORITY
IPLI Software	IMP-IMP Software and Host-IMP Software Under Development	Forms the Basis for Network Security	IVV&T	1
NAC				
Mini-TAC Software	ASYNC/SYNC	Allows Terminals to Access Network	IVV&T	1
HFEP Software	Host Software has Been Completed. CMOS Control Program Under Development	Allows Host Computer to Access Network	IVV&T	1
TEP Software	ASYNC/SYNC Software Under Development	Allows Terminals to Access Host Via the Network	IVV&T	1
HID Software	Host Software has Been Completed. CMOS Control Program Under Development	Allows Host Computer to Access Network	IVV&T	1
Test Facility Software	Refer to Individual Elements	Assures Integrity of DDN Performance	Performance Validation	2
Switch Level Gate Software	Under Development	Allows Interface Between Classified and Unclassified Networks	Performance Validation	2
Mailbridge Software	Under Development	Assists in Transfer of Mail	Performance Validation	2
Network Monitoring Center Equipment Software	Under Development	Monitors Network Performance	Quality Assurance	3
C/30 Software	Precedence/Preemption, Logical Addressing, User Authentication, X.25 Interface Chargeback Algorithm Under Development	Forms the Basis for Network Connectivity	Quality Assurance	3
IPLI Hardware	Microprocessors, KG 84 Crypto Under Development	Forms the Security Basis for Network Connectivity	Design Verification/ Reliability/Environmental/ Maintainability/Electrical/ Endurance Validation	3
NAC				
Mini-TAC Hardware	Microprocessor, Synchronous Terminal/Switch Handler/ Asynchronous Terminal/Switch Handler Under Development	Allows Terminals to Access Network	Design Verification/ Reliability/Environmental/ Maintainability/Human Engineering/ Electrical/Endurance Validation	3

Table 2-4. Component Level Testing Priorities (Page 2 of 3)

DDN SYSTEM ELEMENT	DEVELOPMENT STATUS	CRITICALITY TO NETWORK PERFORMANCE	RECOMMENDED TEST APPROACH	PRIORITY
NAC (cont'd)				
HFEP Hardware	Microprocessor, Host/Unibus Interface, Q Bus Interfaces, Unibus/Interfaces Under Development	Allows Host Computer to Access Network	Design Verification/ Reliability/Environmental/ Maintainability/Human Engineering/ Electrical/Endurance Validation	3
TEP Hardware	Microprocessor, Synchronous Terminal/Switch Handler, Asynchronous Terminal/ Switch Handler	Allows Terminals to Access Host via the Network	Design Verification/ Reliability/Environmental/ Maintainability/Human Engineering/ Electrical/Endurance Validation	3
HID Hardware	Microcomputer, Hardwired Computer, Host/Unibus Interface, Q Bus/HDH Interface, Unibus/Q Bus Adapter	Allows Host Computer to Access Network	Design Verification/ Reliability/Environmental/ Maintainability/Human Engineering/ Electrical/Endurance Validation	3
Test Facility Hardware	Refer to Individual Elements	Assures Integrity of DDN Performance		3
Switch Level Gate Hardware	Under Development	Allows Interface Between Classified and Unclassified Networks	Design Verification/ Reliability/Environmental/ Maintainability/Electrical/ Endurance Validation	3
Mailbridge Hardware	Under Development	Assists in Transfer of Mail	Design Verification/ Reliability/Environmental/ Maintainability/Electrical/ Endurance Validation	3
Network Monitoring Center Equipment Hardware	Development Completed	Monitors Network Performance	Reliability/Environmental Validation	3
C/30 Hardware	Development Completed	Basis for Network Connectivity	Reliability/Environmental Validation	3
Trunk Lines	No Development Necessary	Aids in Network Connectivity	Bit Error Rate Analysis	3
TAC Hardware	Development Completed	Allows Terminals to Access Network - To be Replaced by Mini-TACs	Reliability/Environmental Validation	4
Software	Development Completed	Allows Terminals to Access Network- To be Replaced by Mini-TACs	Quality Assurance	4
Statistical Multiplexers	Development Completed	Support Mini-TAC Functions	Reliability/Environmental Validation	4

Table 2-4. Component Level Testing Priorities
(Page 3 of 3)

DDN SYSTEM ELEMENT	DEVELOPMENT STATUS	CRITICALITY TO NETWORK PERFORMANCE	RECOMMENDED TEST APPROACH	PRIORITY
Power and Environment Monitor (PEM) - Hardware	Sensors, Controls Under Development	Monitors Environments of Sites Having a Switch or Mini-TAC	Reliability/Environmental Validation	4
Software	Host-IMP Program, Data Collection and Control Program Under Development	Monitors Environments of Sites Having a Switch or Mini-TAC	Performance Validation	4
Patch and Test Modules Hardware	Development Completed	Assures Integrity of Performance	Environmental/Calibration Validation	4
Software	Development Completed	Assures Integrity of Performance	Performance Validation	4
Access-Line Modems	No Development Necessary	Support Connectivity	Reliability/Environmental Validation	5
Automatic Line Restoral Option Hardware	No Dates Available	Assures Network Performance Reliability	Reliability/Environmental Validation	5
Software	No Dates Available	Assures Network Performance Reliability	Performance Validation	5
Mobile Reconstitution Vans	Refer to Individual Elements	Provides Backup Capability	Refer to Individual Elements	5
Network Information Component Center (NIC) Hardware	No Dates Available	Contains Statistics on Network Traffic	Reliability/Environmental Validation	5
Software	No Dates Available	Contains Statistics on Network Traffic	Quality Assurance	5

Table 2-5. Site Transition Level Testing Priorities (Page 1 of 2)

DDN COMPONENT	TYPE TEST (NATURE)	OBJECTIVE	WHEN	WHERE	PRIORITY
Site Preparation	Operational Existing Performance Standards	Determine Existing Standards	All Stages	By Type Net/By Site	2
	Limited Operational	Determine the Degree of Enhancement or Upgrades	All Stages	By Type Net/By Site	1
	Contractor Government Site Readiness	HW/SW Integration Interfaces - COI Separation Operational Utility	All Stages	By Type Net/By Site	1
	Limited Operational for Network Cutover	Personnel Equipment Readiness Interfaces Compatibility	All Stages	By Type Net/By Site	1
Site Facility Operation C/30 Switch Node	Operational	SW Interface PREC/PREMP Logical Address User Authentication X.25 Interface	All Stages	By Type Net/By Site	1
MAC					
Mini-TAC	Operational	Term Access Protocols Host-Host SW (TCP/IP) Host-IMP SW (HDH, HDCL) ASYNC SW SYNC SW	All Stages	By Type Net/By Site	1
HFEP	Operational	Terminal Access Protocols Host-Host SW (TCP/IP) Host-IMP SW (HDH, HDCL)	All Stages	By Type Net/By Site	1
TEP	Operational	Communications SW Terminal Emulators SW Host-Host SW (TCP/IP) Host-IMP SW (HDH, HDCL) ASYNC SW SYNC SW	All Stages	By Type Net/By Site	1

Table 2-5. Site Transition Level Testing Priorities
(Page 2 of 2)

DDN COMPONENT	TYPE TEST (NATURE)	OBJECTIVE	WHEN	WHERE	PRIORITY
Host Interface Device	Operational	Term Access Protocols Host-Host SW (TCP/IP) Host-IMP SW (HDH, HDCL)	All Stages	By Type Net/By Site	1
TAC	Operational	Term Access Protocols Host-Host SW (TCP/IP) Host-IMP SW (HDH, HDCL)	All Stages	By Type Net/By Site	1
IPLI	Operational	Security Separation COI Separation	Stage III	By Type Net/By Site	1
Blacker	Operational	Security Separation COI Separation	Stage IV	By Type Net/By Site	1

(C^2I, SECRET, and MILNET) with its original performance quality and services; it is equally important to demonstrate the required separation and security of data.

Network integration testing is the most complex and critical level for DDN hardware and software. Test history will be limited on the network level. The individual network test objectives of system performance, data handling and control, security, reliability, and availability are equally significant on the network level, and are ranked accordingly, as priority 1. Table 2-6 summarizes DDN integration testing and indicates this priority 1 ranking.

Table 2-6. Network Integration Level Testing Priorities

DDN COMPONENT	TYPE TEST (NATURE)	OBJECTIVE	WHEN	WHERE	PRIORITY
DDN Network	OT&E	Verify Network Performance Parameters	By Stage	Intrasite Site-Site	1
	OT&E	Verify Network Data Handling and Control	By Stage	Intrasite Site-Site	1
	OT&E	Verify Network Security Provisions	By Stage	Intrasite Site-Site	1
	OT&E	Verify Availability and Reliability	By Stage	Intrasite Site-Site	1

3. CONCLUSIONS

3.1 Test and Evaluation Ranking.

DDN COMPONENT	LEVEL OF TESTING	TYPE OF TEST	PRIORITY
IPLI Software	Component	IVV&T	1
NAC			
Mini-TAC			
Software	Component	IVV&T	1
HFEP Software	Component	IVV&T	1
TEP Software	Component	IVV&T	1
HID Software	Component	IVV&T	1
Site Preparation	Site Transition	Limited Operational for Network Cutover	1
Site Facility	Site Transition	Operational	1
C/30 Switch Node			
Trunk Lines			
NAC			
Mini-TAC			
HFEP			
TEP			
HID			
Access-Line Modems			
TAC			
Statistical Multiplexers			
Switch Level Gates			
Mailbridges			
IPLI			
Blacker			
DDN Network	Integration	Operational (Performance, Data Handling, Security, Availability/ Reliability)	1

DDN COMPONENT	LEVEL OF TESTING	TYPE OF TEST	PRIORITY
Test Facility Software	Component	Performance Validation	2
Switch Level Gate Software	Component	Performance Validation	2
Mailbridge Software	Component	Performance Validation	2
Site Preparation	Site Transition	Operational Existing Performance Standards	2
C/30 Software	Component	Quality Assurance	3
Network Monitoring Center Software	Component	Quality Assurance	3
IPLI Hardware	Component	Design Verification/ Reliability/ Environmental/ Maintainability/ Human Engeering/ Electrical/Endurance Validation	3
NAC			
Mini-TAC Hardware	Component	Design Verification/ Reliability/ Environmental/ Maintainability/ Human Engineering/ Electrical/Endurance Validation	3
HFEP Hardware	Component	Design Verification/ Reliability/ Environmental/ Maintainability/ Human Engineering/ Electrical/Endurance Validation	3

DDN COMPONENT	LEVEL OF TESTING	TYPE OF TEST	PRIORITY
TEP	Component	Design Verification/ Reliability/ Environmental/ Maintainability/ Human Engineering/ Electrical/Endurance Validation	3
HID Hardware	Component	Design Verification/ Reliability/ Environmental/ Maintainability/ Electrical/Endurance Validation	3
Test Facility Hardware	Component	Refer to Individual Elements	3
Switch Level Gate Hardware	Component	Design Verification/ Reliability/ Environmental/ Maintainability/ Electrical/Endurance Validation	3
Mailbridge Hardware	Component	Same as Switch Level Gate Hardware	3
Network Monitoring Center Equipment Hardware	Component	Reliability/ Environmental Validation	3
C/30 Hardware	Component	Reliability/ Environmental Validation	3

DDN COMPONENT	LEVEL OF TESTING	TYPE OF TEST	PRIORITY
Trunk Lines Hardware	Component	Bit Error Analysis	3
TAC			
Hardware	Component	Reliability/ Environmental Validation	4
Software	Component	Quality Assurance	4
Statistical Multiplexers	Component	Reliability/ Environmental Validation	4
Power and Environment Monitor (PEM) -	Component	Reliability/ Environmental Validation	4
Hardware			
Software	Component	Performance Validation	4
Patch and Test Modules - Hardware	Component	Environmental/ Calibration Validation	4
Software	Component	Performance Validation	
Access Line Modems	Component	Reliability/ Environmental Validation	5
ALRO Hardware	Component	Reliability/ Environmental Validation	5
Software	Component	Performance Validation	
Mobile Reconstitution Vans	Component	Refer To Individual Elements	5
Network Information Center (NIC)	Component	Reliability/ Environmental Validation	5
Hardware			
Software		Quality Assurance	5

3.2 Rationale for Ranking. As stated in Paragraph 2.4.1, the two major considerations in ranking components should be the components' development status and importance to the functioning of the DDN. When one is applying these two variables, component testing can be subdivided into five levels of importance (see Paragraph 2.3.1). The network access approaches and IPLI, because their software is still under development and because they form the basis upon which the whole DDN operates, are the most critical test items. The software associated with the switch level gates, mailbridges, and test facility comprises the bulk of the next level of testing primarily because the extent of software development for these items is not as great as for the IPLI or the NAC. The Network Monitoring Center, because of its vital role in preserving the integrity of the system, has also been assigned priority 2. The hardware testing of the access approaches forms the basis for the next priority level. Its criticality to network performance is the same as its software, but it can be differentiated by the fact that some of the hardware already exists with established performance histories. The test facility and patch and test modules also have been included in this level because of their supportive nature. The last two levels contain elements having functions that are either ancillary to the DDN or having functional histories that have been well established.

Site transition testing, by its very nature of preparing the user for accessing the network, is a vital part of the test cycle. Therefore, all tests for site testing have been assigned as priority 1 except for the testing of baseline host performance standards, which has been assigned as priority 2.

Integration testing, which is the culmination of the entire test cycle, is the most critical of the three phases. Therefore, the network tests involving performance, data handling, security, and availability and reliability have been assigned as priority 1.

3.2.1 Rationale for IVV&T Ranking. Independent Validation, Verification, and Testing (IVV&T) is used when the Project Manager's Office determines that objective, unbiased monitoring and testing are critical to the development of a particular software component. Because IVV&T is an expensive form of testing in the short run, it is important to identify those factors that make IVV&T a cost-effective undertaking in the long run before deciding on its use.

The most important factors in a decision to use IVV&T are the criticality of the software to the performance of the system that it has been designed to support, and the software's complexity. In cases where the software being developed is critical to the performance of the system or extremely complex, IVV&T in the early development stages of the software can prevent:

(a) Cost overruns
(b) Schedule overruns
(c) Modifications
(d) Software non-deliveries.

Avoidance of these can serve as sufficient justification for the cost of IVV&T.

3.3 T&E Location Factors. Generally, hardware and software component testing should be done at the manufacturer's site. IVV&T may be conducted at the manufacturer's site or at a Government-approved test facility. TEMPEST and HEMP testing should be accomplished at a Government-approved facility.

As the software for a piece of equipment evolves, stand-alone development support and laboratory subnetwork testing should be accomplished at the manufacturer's site.

Once the manufacturer has conducted hardware/software integration testing of a configuration item (CI), it should be turned over to a government test facility for laboratory environment testing. Interfaces between CIs should also be tested in the government facility.

The government test facility containing sufficient network backbone equipment, interfaces, and circuits will be able to accept equipment from all vendors, and thus can more closely emulate the operational DDN network. Testing in this manner provides a flexible testing environment quickly adaptable to DDN needs.

Site transition testing is required at each site, since no two sites are exactly the same. Further inspection and evaluation of sites will help determine the amount and type of testing required.

Network integration testing can be seen as two distinct types of testing. Network integration testing in the test facility provides information on system performance and capabilities in a controlled test environment. This testing and resultant information increases the confidence of the testor (DDN) and the potential subscriber to DDN that the DDN upgrades or changes will not degrade an operating network.

From the test facility environment, network integration testing should move to the network itself. This testing should involve partitioned network testing of functionality before cutover. The partitioned testing uses a subset of the tested network (including a CONUS terminal) and the DDN test facility as nodes.

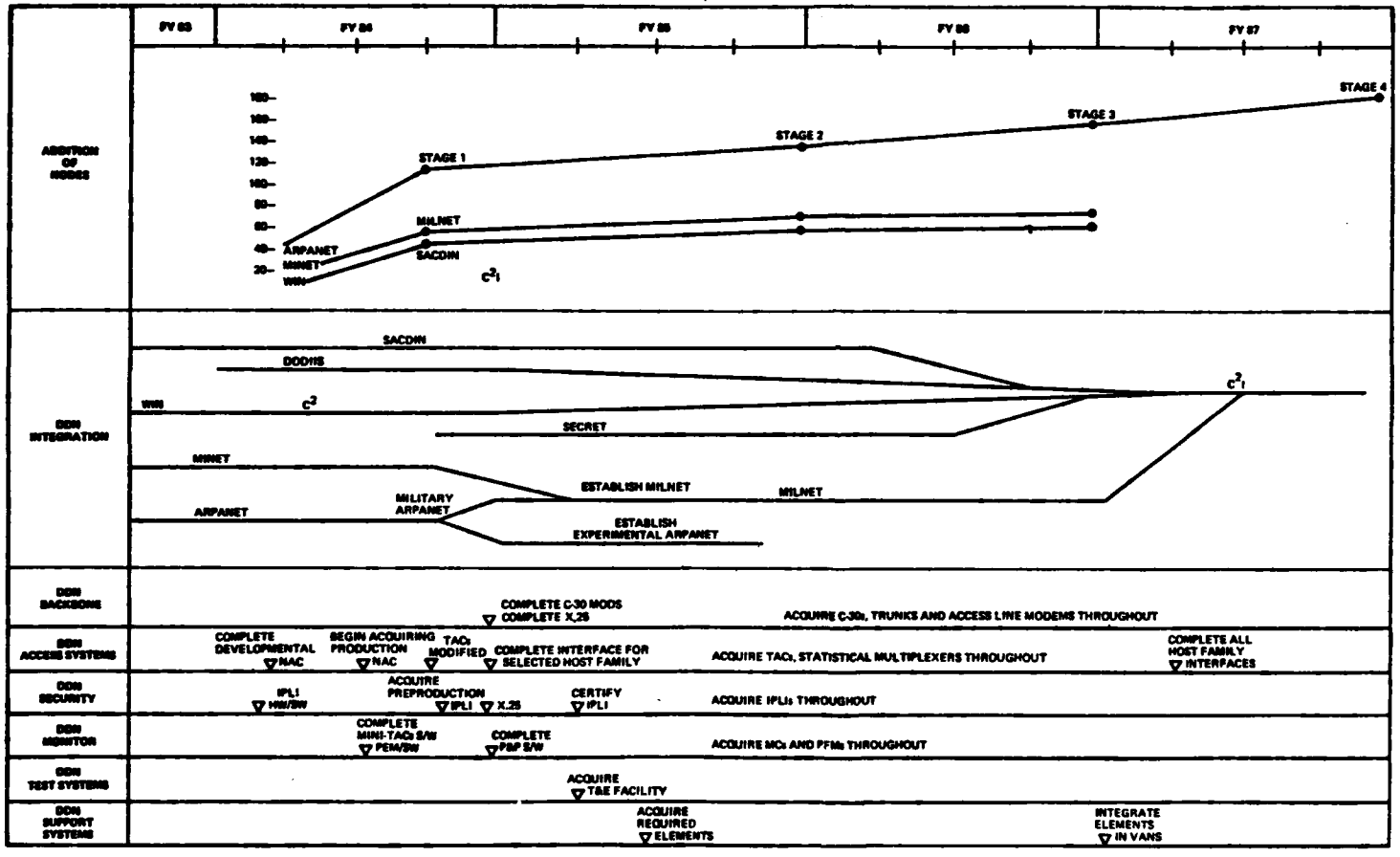
3.4 Sequencing and Scheduling. DDN testing will progress from the component level to site transition, and then through network integration. Test requirements are outlined in the previous corresponding sections.

The sequencing and scheduling of individual tests required at the component level should be as required by the corresponding contract and will be further defined in CDRLs by the developing contractor. Generally, however, as long as the contractor successfully demonstrates all required tests within its allocated resources and delivers the equipment on time to support site transition testing, a specific sequence of component level testing is not required.

Site transition should occur as soon as DDN production equipment is made available to individual sites. The particular sequence will depend on subscriber acquisition planning and funding availability. Another important consideration is the availability of required test time, which will vary from subnetwork to subnetwork and site to site, depending on operational concerns. Specific schedules for site transitions must address these considerations and should be derived on a site-by-site basis. Site transition testing should conclude successfully before network integration of the involved site begins.

The sequencing for DDN integration testing should follow the five progressive phases outlined in Paragraph 2.2.3. Integration testing of all the subnetworks should conclude by the end of Stage III and will establish the initial operating capability (IOC) of DDN.

Examination of the schedule of activities involved in the development of the DDN shows that site transition testing may constitute a problem. While the total number of nodes on the network is not now certain and Figure 3-1 is only an estimate, the number of nodes increases significantly in the year before the establishment of MILNET. ARPANET, MINET, and WIN will provide 50 or more nodes to the DDN and by the time MILNET is fully established, or shortly thereafter, the DDN will have perhaps 120 nodes. Since a realistic estimate of the time required to test each node which goes through this transition is 30 days, careful planning and a heavy commitment of resources will be necessary during this period.



TP No. 083-10808-B

Figure 3-1. DDN Development

4. RECOMMENDATIONS

4.1 Recommendations for Component Level Testing. It is recommended that the component level testing of hardware and software, defined in detail in Paragraph 2.2.1, be conducted with emphasis on the software and, especially, on the IVV&T. If resources of time and funding become constraints to testing, it is recommended that the component level tests (summarized in Table 2-4) with the highest priority be accomplished first, with subsequent lower priority testing accomplished as allowable.

4.2 Recommendations for Site Transition Testing.

4.2.1 A coordinated approach to site transition testing is recommended. This approach should recognize the need to assure the availability of network services at the switching node prior to, or in conjunction with, subscriber connectivity testing.

4.2.2 It is recommended that a transition plan be developed for each site. These plans should be developed 3 to 6 months before site transition testing and coordinated with all participants. The plans should include items such as method of DDN network access and level of security so that the DDN network integration plan may incorporate required tests for overall network integration.

4.2.3 It is recommended that site transition testing be conducted consistent with the DDN evolution schedule.

4.3 Recommendations for Network Integration Testing.

4.3.1 It is recommended that the DDN PMO monitor the upgrading or establishment of nets and sites that will ultimately become subscribers to DDN in order to:

(a) Define network topology

(b) Determine interface requirements to DDN

(c) Facilitate planning and coordination of a comprehensive T&E program for DDN evolution.

4.3.2 It is recommended that the DDN test facility be established and brought on-line so that it may operate as a part of any net and serve as the point of insertion for functional capabilities of the networks to be integrated.

4.3.3 It is recommended that a Network Integration Plan be developed for MINET transition to the MILNET network. This plan should be ready for implementation by the third quarter of FY 84.

4.3.4 It is recommended that a Network Integration Plan be developed for each community-of-interest network transition to DDN. These plans should be ready for implementation by the start of FY 85.

4.3.5 It is recommended that the DDN PMO plan to conduct network integration tests of MINET subscribers to the DDN backbone during the period July 1984 to January 1985.

4.3.6 It is recommended that the DDN PMO plan to conduct network integration tests of WIN/DoDIIS subscribers during the period October 1985 to December 1986.

4.3.7 It is recommended that the DDN PMO plan to conduct integration testing of the SACDIN Network into the C^2I Network during the period January 1986 to July 1986.

4.3.8 It is recommended that the DDN PMO plan to conduct integration testing of the C^2I and SECRET networks during the period April 1986 to October 1986.

4.3.9 It is recommended that the integration tests of the classified and unclassified segments of the DDN be conducted during the period October 1986 to April 1987. This testing follows the insertion of the IPLI into the network.

4.3.10 Lastly, it is recommended that a comprehensive DDN Transition Plan be developed in consonance with the subscribers to identify responsibility for network control during each phase of DDN development.

LIST OF ABBREVIATIONS, ACRONYMS, AND SYMBOLS

ALRO	Automatic Line Restoral Option
ARPANET	Advanced Research Projects Agency Network
BBN	Bolt, Beranek & Newman, Inc.
CDRL	Contract Data Requirements List
CI	Configuration Item
CONUS	Continental U. S.
DCA	Defense Communications Agency
DDN	Defense Data Network
DoD	Department of Defense
DoDIIS	DoD Intelligence Information System
DSARC	Defense Systems Acquisition Review Council
DT&E	Developmental Test and Evaluation
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
FOT&E	Follow-on Test and Evaluation
FY	Fiscal Year
GFE	Government-Furnished Equipment
HDH	High Speed Data Link Control Distant Host
HDLC	High Speed Data Link Control
HEMP	High-Altitude Electromagnetic Pulse
HFEP	Host Front End Processor
HID	Host Interface Device
HIP	Host Interface Protocol
IMP	Interface Message Processor
IOC	Initial Operating Capability
IOT&E	Initial Operational Test and Evaluation
IP	Interface Protocol
IPLI	Internet Private Line Interface
IVV&T	Independent Verification, Validation, and Test
LMD	Lead Military Department
MC	Monitoring Center

LIST OF ABBREVIATIONS, ACRONYMS, AND SYMBOLS (Cont'd)

MEP	Management Engineering Plan
MILNET	Military Network
MINET	Movements Information Network
mini-TAC	Mini-Terminal Access Controller
NAC	Network Access Component
OT&E	Operational Test and Evaluation
PAT&E	Production Acceptance Test and Evaluation
PEM	Power and Environment Monitor
PMO	Program Management Office
PS	Packet-switching
QA	Quality Assurance
SACDIN	Strategic Air Command Digital Information Network
SOW	Statement of Work
T&E	Test and Evaluation
TAC	Terminal Access Controller
TCP	Transmission Control Protocol
TEMP	Test and Evaluation Master Plan
TEMPEST	Certified as having electronic emission controlled
TEP	Terminal Emulation Processor
WIN	WWMCCS Intercomputer Network

END

FILMED

11-83

DTIC