Final Report

Defense Science Board Task Force

on

DEFENSE DATA NETWORK

30 August 1985

Office of the Under Secretary of Defense for Research and Engineering
Washington, D.C. 20301

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

DEFENSE SCIENCE
BOARD

3 October 1985

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

SUBJECT: Final Report of the Defense Science Board Task Force on the Defense Data Network (DDN)

I am forwarding the Final Report of the Defense Science Board Task Force on the Defense Data Network (DDN) along with the forwarding letter of the Task Force Chairman, Dr, Sayre Stevens. Since you chaired the DSB Panel that reviewed the draft report prior to its oral presentation to the Board as a whole, I know you are familiar with its contents.

The recommendations of the Task Force are summarized in Sayre's covering letter as well as being more fully treated in the implementation plan contained in the executive summary of the report. I find the specific recommendations to be worthy of serious consideration and urge the establishment of an oversight group to ensure the effective and realistic treatment of security architectural and procedural problems.

This endeavor by the DSB has continued far beyond the short effort we envisioned when we initially agreed in 1981 to address the question of continuing the development of AUTODIN II. Nevertheless, I feel we have helped launch an important new system, the DDN.

I recommend you read and approve the Executive Summary which includes the Implementation Plan. Enclosed at Tab B is a memo for your signature initiating the actions included in the Implementation Plan.

Charles A. Fowler

Charles A. Fowler, Chairman
Defense Science Board

Enclosure
a/s

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

DEFENSE SCIENCE
BOARD

Mr. Charles A. Fowler
Chairman, Defense Science Board
Office of the Secretary of Defense
Washington, D.C. 20301

Dear Bert:

I am submitting with this letter the Final Report of the Defense Science Board Task Force on the Defense Data Network.

The Task Force was established in May 1983 to review, evaluate, and make recommendations concerning the continuing evolution of the DDN. Since that time, the DDN addressed a number of issues that have arisen as the program has gained momentum, achieved new status, and encountered a number of plaguing problems. This report provides the observations and recommendations generated by that review.

During the past couple of years, the DDN has made significant progress; a network of substantial capability is now in being and a growing number of new users are awaiting the opportunity to join the network as it expands. The DDN Program Office deserves high credit for its accomplishments thus far. Nevertheless, much remains to be done and some significant problems have not yet been solved.

The Task Force has made a number of rather specific recommendations for dealing with some of these problems. They differ from the higher-level, more global recommendations made by the group as it dealt with the AUTODIN II decision. They are appropriate, however, to the type of review it performed of the continuing development of the DDN. These recommendations are summarized in the implementation plan in the Executive Summary of the report. Several deal with the need for establishing explicit policy with regard to new developments significantly affecting the future course of DDN implementation: the proliferation of electronic mail service, the growing use of personal computers as network elements, and the use of enhanced information about network operations to achieve direct user billing services.

Another recommendation, somewhat contentious in circles outside the Task Force, urges that discipline in the control of protocol configuration be maintained despite the apparent appeals of new developments and expectations of strong vendor support. Most important in this regard is its urging that full acceptance of NBS's Transport Protocol (TP) await demonstration of its suitability for Defense purposes and clear evidence of vendor commitment to development and support.

More opportunities for strengthening the survivability of the DDN exist than have been seriously pursued. Possibilities for applying the results of the NETS (Class 4-5) study to this end appear intriguing.

One global problem does however remain. At the end of the Task Force's efforts, the matter of DDN security architecture remained unsettled. Indeed, never during its review, or that of the AUTODIN Task Force, was the matter satisfactorily addressed. It is essential to the success of the DDN that this not continue. In consequence, the Task Force has recommended that a new oversight group be established to ensure that it doesn't. It is an inappropriate job for the DSB, but one of importance. The ASD(C3I) should take implementing action.

Finally, the Task Force wants to express its appreciation for the extraordinary support it was provided by many elements of the DoD, and particularly by the DDN Program Office and DCA. The Chairman must thank his Task Force members whose wisdom and dedication overcame his own failings.

Sincerely,

Sayre Stevens

EXECUTIVE SUMMARY

In May 1983, the Defense Science Board established a new Task Force to review, evaluate, and make recommendations concerning the continuing evolution of the Defense Data Network Program. Since that time, the DDN Task Force addressed a number of issues that have arisen as the Program has gained momentum, achieved new status, and encountered a number of plaguing problems. This report provides the observations and recommendations generated by that review.

The most significant concern of the Task Force surrounds the DDN Security Architecture and the evolution of security in the network. In the next five to ten years security may well be one of the most critical challenges facing DoD. DDN, as a global common-user data communications network, will be subject to this challenge as much as, if not more, than any other system. The Task Force has therefore recommended that major emphasis be placed on the DDN Security Architecture, a detailed security plan and on establishing an independent group to periodically review and assess the progress of the DDN and other relevant security programs in this area.

DEFENSE DATA NETWORK
ACTIONS REQUIRED TO IMPLEMENT
DEFENSE SCIENCE BOARD TASK FORCE RECOMMENDATIONS

A. DDN PMO STATUS AND PERFORMANCE

1. **Recommendation:** DCA (either the DDN Program Office or the Defense Communications Engineering Center) establish simple electronic mail exchange standards similar to those in use on the ARPANET, as well as functionality guidelines for electronic mail services on the net.

   Action: ASD(C^3I) should task DCA to promulgate a DDN policy memorandum (a) to establish the DoD standard Simple Mail Transfer Protocol, MIL-STD-1781, dated 10 May 1984, as the preferred implementation of electronic mail for DDN and (b) to specify minimum functional guidelines for the electronic mail services that should be used on the network. Estimated cost is one staff week within DDN PMO.

B. STATUS OF THE USER COMMUNITY

2. **Recommendation:** Establish policy on the treating of Personal Computers as terminals or independent hosts and investigate the potential of a PC Terminal Access Controller that would embody a reliable protocol for network interactions.

   Action: ASD(C^3I) task DCA to draft a policy document on the use of PCs on the DDN and to investigate the feasibility of and resources required for a PC TAC. Estimated cost is two staff months within DDN PMO.

3. **Recommendation:** JCS and OSD should encourage the components to pass user billing charges directly to the using organization, thus optimizing their use of this resource.

   Action: JCS should insure that policy guidance which establishes user billing on DDN encourages components to pass charges directly to the lowest level of using organization. No additional resources required.

C. PROTOCOLS

4. **Recommendation:** OSD should again direct that Service and Defense Agency data communications users include TCP and IP in their contract specifications. That guidance should further direct the Services and

Defense Agencies to ensure that the direction is disseminated widely to the field.

Action: ASD(C^3I) in a policy memorandum to the Services and Defense Agencies, should restate DoD position on protocol standards to include maximum use in contract specifications and widest dissemination to field activities. Estimated cost is four staff hours within ASD(C^3I).

5. **Recommendation:** Full adoption of the TP standards by DoD must await the demonstration of performance required for military use and the cost advantages associated with real commercial viability.

Action: Complete. ASD(C^3I) established this as the DoD position in a Memorandum to the Director, DCA (Executive Agent for DoD Data Communications Protocol Standards) dated 3 April 1985. No additional resources required.

D. SURVIVABILITY

6. **Recommendation:** The DDN Program Office should make effective use of the results of the NETS (Class 4-5 Study) evolving at DCA, as well as commercial satellite services being developed. In addition, the office should explore strategic placement of packet switches interconnected only by Class 4-5 switches.

Action: ASD(C^3I) task DCA to assess the results of the NETS (Class 4-5 Study) and provide recommendations on the applicability of the Study findings and of the Strategic placement of packet switches interconnected only by Class 4-5 switches. Estimated cost is two staff weeks within DDN PMO.

E. SECURITY ARCHITECTURE

7. **Recommendation:** An oversight group be created to monitor development of the security architecture for DDN, the status and progress of the BLACKER program, and (as necessary) the status and progress of the IPLI program.

Action: ASD(C^3I) establish an ad hoc group under the chairmanship of the Director, Information Systems to periodically review the DDN security architecture and the status of related security programs. Estimated cost is six to twelve staff days semi-annually for one to two day ad hoc security group meetings; membership to be determined.

8. **Recommendation:** The DDN PMO produce a comprehensive overall system security plan for the DDN (to include physical arrangements for the security equipments; operational rules for maintaining security; personnel clearance requirements, etc.).

Action: ASD(C^3I) task DCA to develop an overall system security plan for the operation of the DDN. Estimated cost is three staff months within DDN PMO.

CONTENTS

INTRODUCTION

In September 1981, the Defense Science Board was requested to evaluate the AUTODIN II communications system in relation to alternatives then available and to make recommendations concerning the continuation or termination of AUTODIN II, which had at that time achieved limited operational status. A Task Force, established to undertake that review, expressed a preference in March 1982 for the adoption of an alternative approach to the continued development and installation of the AUTODIN II system. The Task Force supported the results of a DCA review favoring the evolutionary implementation of a common user data network based upon the ARPA packet switching network, ARPANET. Those recommendations and the considerations underlying them are provided in some detail in the Final Report of the Defense Science Board Task Force on AUTODIN II. In April 1982, the Deputy Secretary of Defense directed the termination of AUTODIN II and the implementation of the alternative ARPANET approach, designated the Defense Data Network.

The Task Force met in October 1982 to review the progress of this implementation. Observations on progress to that time are included in the Final Report; while several emerging problems were identified, the outlook was encouraging.

In May 1983, the Defense Science Board established a new Task Force to review, evaluate, and make recommendations concerning the continuing evolution of the Defense Data Network Program. Since that time, the DDN Task Force has met five times and addressed a number of issues that have arisen as the Program has gained momentum, achieved new status, and encountered a number of plaguing problems. This report provides the observations and recommendations generated by that review.

DEVELOPMENTS IN THE DEFENSE DATA NETWORK IMPLEMENTATION

The DDN concept consists of the evolution and expansion of existing and newly established networks based on ARPANET technology and their ultimate consolidation into an integrated network suitable for use at multiple levels of security. The original planning date for integration was 1986. The DDN implementation was to proceed to two parallel projects: first, expansion of the WWMCCS Intercomputer Network (WIN) to include the DoD Intelligence Information System (DODIIS) community to form the Command, Control and Intelligence (C^2I) network which would subsequently include the integration of additional classified nets as requirements dictated. Second, the ARPANET would be partitioned into a Military Network (MILNET) for general DoD unclassified data communications service and a research network for continued network research by DARPA. In addition, the Movements Information Network (MINET) which was being implemented in Europe as a testbed would be merged with the primarily CONUS-based MILNET to form a world-wide unclassified DDN backbone.

These two projects were to continue until end-to-end encryption devices were available, at which time the unclassified and classified networks would be merged. The critical security element in this evolutionary path for the DDN was the end-to-end encryption (E^3) device. Development of that device, the Internet Private Line Interface (IPLI) was begun in November 1981 with completion of the development phase scheduled for February 1984. A production phase was to follow, making production quantities of the IPLIs first available in 1986. A second E^3 device, BLACKER, has been under single vendor development since 1983 and is expected to be available in production quantities beginning in late 1987.

Following the April 2, 1982 decision by the Deputy Secretary of Defense, DCA established a DDN Program Management Office (PMO) to implement the DDN and asked the Air Force to assume a modified Lead Military Department/Life Cycle Manager (LMD/LCM) role in the program. Funding was directed by OSD based on the DDN Program Plan.

The initial efforts of the DDN PMO concentrated on the establishment of user requirements. This was necessary since DCA's review of AUTODIN II and its ARPANET alternative used "representative" requirements. Initial contacts were made with the computer mainframe manufacturers to generate interest in producing commercially available DDN host computer interfaces and requisite protocols. In addition, a contracting structure was developed to acquire the elements needed to implement the DDN as described in the DDN Program Plan.

The DDN PMO then embarked on the program as directed. As the program began there were two projects underway which were continued under the DDN umbrella. These were 1) the WIN Communications Subsystem (WINCS) topology reconfiguration and packet switch hardware upgrade, and 2) the implementation of the MINET testbed system in Europe.

The WIN hardware upgrade was completed in August 1983 and most topology upgrades completed as well. Integration of other systems with the WIN is delayed awaiting completion of the JCS transfer of management functions to DCA and the availability of E^3 production units. The DODIIS integration with the WIN could not be initiated when the first DODIIS sites required service. Consequently, a separate network is being installed to support DODIIS requirements. Node installations are complete and circuit installations are proceeding for the first four sites.

The MINET system was to be implemented in three geographically separate stages. Stage 1 in Central Europe was completed in January of 1984 and installations continue in Stage 2 in the Western Mediterranean with completion scheduled in February 1985. Stage 3 in the Eastern Mediterranean will be delayed until early 1986 for political reasons and transmission availability problems not originally anticipated. As was originally planned, merging the MINET Communications Subsystems with the MILNET was completed on December 18, 1984.

After officially establishing MILNET service on April 4, 1983, the ARPANET partitioning occurred in two stages. First, a logical or software-enforced separation of the two communities was completed on October 4, 1983; it was followed by a second, physical partitioning completed September 6, 1984. In preparation for the logical separation of the network, seven internet gateways were installed to permit interchange of data between the MILNET and the ARPANET, and these gateways will remain to provide for the interchange of data between the MILNET and the ARPANET.

Currently, the DDN networks (excluding the ARPANET) consist of 108 packet switches and 53 Terminal Access Controllers (TACs) connected by 129 trunks. These DDN networks concurrently serve 204 host computers. By the end of CY-86 the DDN is expected to grow to 349 packet switches and 137 TACs connected by 310 trunks and supporting 3550 host computers. From the original DDN Program Plan, DDN requirements have grown nearly exponentially from 448 to 4573 hosts and from 1446 terminals (including a significant number of dial-in terminals) to 15,965.

To insure that the MILNET is used for official purposes while providing the greatest flexibility to terminal users, a method for controlling access to the TACs was developed and implemented. This system, called TAC Access Control (TACACS)

uses a self-authenticating password to validate user access to the TACs in the MILNET. The TACACS system became operational February 15, 1984. It became operational in the MINET as well in January 1985.

IPLI development, which was initiated in November 1981 has proceeded with some problems. The development effort experienced a 10 month slip in mid-1983 caused primarily by problems with hardware suppliers and a clarification of the security constraints of the development effort. A further 3-month slip occurred in September 1984 due primarily to problems encountered in software development and testing. The current target for completion of the development project is March 1985. Each slip in schedule has brought with it a corresponding increase in development cost, with the development now funded at $6.0M. The unit production costs for the IPLI have also risen from the original unit cost of $25K to a range of $45K to $60K. Plans for follow-on production of IPLIs are currently being evaluated in light of BLACKER end-to-end encryption program schedules and cost. Current cost estimates for production quantity BLACKER devices are $6K to $8K per unit.

In reviewing the DDN security architecture produced by the DCA, which called for the heavy use of IPLIs to deal with NSA concerns, OSD determined that architecture should be reviewed and so directed on May 10, 1982. A joint DCA and NSA review was undertaken which revised the DDN security architecture to comprise two separate network segments: a classified segment and an unclassified segment. The two segments were then to be inter connected by gateway devices similar to the IPLIs such that the classified segment could make use of the unclassified segment for improved reliability. On the unclassified segment, CONUS trunks and TAC access circuits were to be protected with Digital Encryption Standard (DES) encryption; DES encryption on access lines was optional based on the user requirement. On the OCONUS unclassified segment, military grade encryption was to be employed on trunks and DES encryption was to be employed on a limited basis on access circuits.

On the classified segment, the revised security architecture required military grade encryption on all circuits and required all host users to use IPLIs for separation of security levels. The architecture also provided for an unclassified segment monitoring center and a classified segment monitoring center to monitor the two backbone networks. User monitoring centers were provided to monitor each classified community on the plain text side of the IPLI. The architecture recognized the BLACKER project as the provider of the final end-to-end security device for DDN, since service to multi-level host computers was a requirement to be satisfied by BLACKER but not the IPLI.

In May 1984, OSD again directed a review of the DDN Security Architecture. The OSD review resulted primarily from the increased unit cost of the IPLI and the problems associated with development of the IPLI-like gateways connecting the classified and unclassified segments.

In october 1984, NSA provided a threat evaluation to OSD and in November 1984, DCA provided an interim response to OSD with final joint NSA/DCA recommendations to be provided in February 1985. The principle actions to be undertaken by DCA during the interim period are planning for the use of high grade military encryption in the unclassified network vice DES devices as previously planned, evaluation of designs for the authentication of Monitoring Center-to-Packet Switch messages, and the initial deployment of the DISNET (the secret-level network) as two separate networks monitored by a single monitoring center.

TASK FORCE OBSERVATIONS ON THE DDN PROGRAM

DDN PMO Status and Performance

The DCA Program Management Office encountered a rather standard set of problems in the early days of its existence. In part, these were amplified by the termination of the AUTODIN II program and the abrupt change to a new approach in providing a common-user data network. Natural user preferences for dedicated links were bolstered by the uncertain course of the common-user program. These problems for the PMO were reflected in the slow provision of Service funding and staffing despite their allocation to the program, in difficulties in coordinating the DDN Management Engineering Plan, and in Service reluctance to accept Lead Military Department responsibility for the DDN, thus forcing the PMO to perform procurement and implementation responsibilities normally performed by the Services.

In time, these problems were overcome, and the PMO has become an effective and respected management group. Through its efforts, DDN has become institutionalized and has achieved the status of a major, robust program. Needless to say, lots of new problems have nevertheless emerged. AT&T divestiture has greatly complicated procedures and extended lead times associated with the acquisition of trunk lines. Costs have risen. Service support is at times still uncertain and staff rotation is a recurring problem for a PMO with a rapidly growing work load. There is little real understanding of interoperability requirements and advantages among the users. There has been an inadequate opportunity to focus on the longer range development of the system.

Distractions are a problem. Typical of these is the determination of responsibility for providing electronic mail service to system users. The rapid spread of informal electronic mail on the DDN is already an established trend. This highly useful communications medium is eagerly sought by individual users, but unless properly implemented could become fragmented and place an excessive traffic load on the network itself. The DDN Program Office has begun to offer limited electronic mail capability through the purchase of C70 hosts to run the INFOMAIL message service. (Ironically, for a considerable time this initial DDN message service was incompatible with those already on the ARPA network.)

Establishing the hosts and administering the service constitutes a substantial burden to the Program Office. Because of this, there has been a reluctance to take on this additional task, but, unfortunately, no other organization is in a position to offer it on a DoD-wide basis. Some individual components may well be able to establish their own electronic mail systems, but

most will not be able to afford their own. In addition, as was already pointed out, individual systems tend to become incompatible in the absence of common standards.

It is recommended that DCA (either the DDN Program Office or the Defense Communications Engineering Center) establish simple electronic mail exchange standards similar to those currently in use on the ARPANET, as well as minimal functionality guidelines for electronic mail services on the net. Individual Service and Agency components could establish their own systems as long as they met these minimal standards. In addition, however, DCA (the DDN Program Office) should offer the service to those unable to establish their own.

One means to achieve this would be for the Program Office to invite commercial time-sharing and interactive mail services to provide systems for use on the DDN by DoD customers, rather than purchase hardware and operate the systems themselves. This could be done either through multiple-requirements type contracts (where DECCO administers the contract and users are billed by DECCO using the Communication Services Industrial Fund) or by DCA, inviting qualified time-sharing services to attach to the network and provide services billed directly to the user. In either case, commercial organizations should be required to meet the minimum communications standards set by DCA. Either approach would provide highly effective service with a minimum of overhead to the DDN Program Office. These alternatives should be investigated as soon as possible.

Status of the User Community

Early work on better defining user requirements was slow in capturing the full range of Service and Defense Agency requirements. That situation has now reversed, however, and, while accurate estimates of user requirements remain elusive, there has been a flood of project requirements for DDN service. The incredible growth in requirements well confirms the large latent potential for the kind of service DDN will provide. How large that demand will ultimately become is uncertain. It appears now that the existing capability to install new equipment and acquire new trunks will limit the Program Office's ability to respond to about half of the rate of growth projected by even the most conservative estimates of future demand. Near-term problems have been alleviated by estimates of future demand. Near-term problems have been alleviated by slippage in user acquisition of host systems. It seems clear, however, that an expansion of the PMO's installation capabilities will become necessary.

The growth in requirements for DDN service is in large measure the result of burgeoning local area networks wanting to join the network and DDN accommodating to use of the vendor

supported X.25 interface protocol. The proliferation of PC users threatens explosive growth in the future. Policy decisions as to whether to treat the latter as terminals or as independent hosts will have to be made. A PC TAC embodying a reliable protocol for network interactions is also required.

These circumstances dictate that a plan of managing for growth be developed which identifies critical uncertainties in user projections and defines and addresses critical policy decisions that will protect the DDN against growth the system cannot handle. It must also provide for alternatives to meet requirements beyond the capacity of the DDN. A study currently underway by Bolt, Beranek, and Newman is a start toward the development of such a plan.

The present user billing system, in which telecommunications services paid for by centralized organizations in each component, is highly counter-productive and leads to serious degradation in services. The experience with AUTOVON (the DoD common long distance service) is a good example. Available to most DoD users, it is paid for by the communications organizations in each of the Services. AUTOVON is viewed as "free" by the individual user, but when budget cuts occur, service is adversely affected for those persons, who unfortunately have no input into the budget cycle.

With the DDN and the possibility of individual user billing, it may be possible to correct this negative feedback process. Although DDN will soon provide accounting for individual user's service, it will be of little value if the components continue with centralized billing, as employed on AUTOVON. If the service is still perceived of as free, with centralized organizations funding usage in bulk, the same problems observed for years in AUTOVON will soon afflict the DDN. The JCS and OSD should encourage the components to pass user billing charges directly to the using organization, thus optimizing their use of this resource. Failure to do so will seriously downgrade the quality of service available on the DDN or any other telecommunications service.

Protocols

In the course of the past two years, the Task Force addressed two protocol problems of some importance to DDN, the emergence of X.25 and NBS's Transport Protocol (TP). The standard DDN lower level protocol interface is the 1822 interface. This protocol approximates the functionality provided by the X.25 interface, which has become a *de facto* industry standard, and which has been specified as a Federal Information Processing Standard. The DoD 1822 interface predates X.25; accordingly, virtually all DoD packet switching networks within the DoD use 1822 as a standard. Most vendors today, however, support the X.25

interface as part of their standard product line. The difficulty is that each vendor has built its "own" X.25, through the selection of a particular set of options and parameters to be supported. These different versions are not fully compatible. Many potential Service users of the DDN are somewhat reluctant to specify an 1822 interface in their ADP contracts, because the vendors would then have to bid a new protocol development, rather than their existing X.25 implementation. DCA has now implemented what appears to be a logical solution--the specification of a single version of X.25 to be supported in the network. This solution does, as most solutions do, pose its own set of problems, one of which is the necessity to provide for interoperability of the X.25 and 1822 interfaces, so that an X.25 user can communicate with an 1822 user. DCA is also working on the front end accommodation to provide the necessary interoperability between the 1822 and X.25 interfaces. Prototype equipment is now scheduled to be available in April 1985.

Another difficulty with adding X.25 as a supported protocol is that most vendors have built their own suite of higher level protocols using X.25 as a base. When a system with such a full set of protocols is added to the network, the pressure will be intense to use that full set instead of the higher level DoD standard Transmission Control Protocol (TCP) and IP protocols. Such a development must not be allowed to happen. Standard internet and transport level protocols are essential for broad DoD host-to-host and network-to-network interoperability. OSD should again direct that Service and Defense Agency data communications users include TCP and IP in their contract specifications. That guidance should further direct the Services and Defense Agencies to ensure that the direction is disseminated widely to the field.

In many regards, the TP issue represents the X.25 issue of the future. TP and DoD's widely used host-to-host protocol, the TCP, are functionally equivalent, though not interoperable. Efforts are underway to gain acceptance for TP as a standard transport protocol promising widespread interoperability in the future. DoD support is obviously sought. TP is, as yet, however, a laboratory demonstration protocol without broadly based vendor commercial support.

In these circumstances, it seems inappropriate for DoD to compromise its efforts to maintain configuration discipline by indicating a willingness to give way to pressures for change so early in the game. It is likely that the time will come when TP has achieved commercial viability and accommodations will have to be made. Consequently, it is important that planning for that transition takes place and that the utility of TP for defense purposes is assured. This planning is in fact underway. A DoD TP specification is being prepared and an interim

protocol-converting gateway is under study to ensure interoperability between TP- and TCP-based systems. Full adoption of the TP standards must await the demonstration of performance required for military use and the cost advantages associated with real commercial viability.

Survivability

Much has been said about the survivability of the Defense Data Network. Certainly having large numbers of packet switches widely distributed and richly interconnected does provide a high degree of survivability. There remain, however, the issues of where the interconnecting links are routed, and how survivable are the connections. Much of the CONUS telephone system long distance service is routed through a small number of long distance switching centers. Even a richly connected DDN could thus be highly vulnerable to a small number of attacks on telephone switching centers.

The DDN Program Office should make effective use of the results of the NETS (Class 4-5 Study) evolving at DCA, as well as the commercial satellite services being developed. In addition, the Office should explore strategic placement of packet switches interconnected only by Class 4-5 switches. A strategically developed subset of the DDN nodes could be interconnected, using no switching center above the Class 4 level, thereby providing a very high degree of survivability to links so connected. Long distance service, via Class 4-5 switches only, would be more expensive than the trunking services now normally available, but such expenditures for a limited subset of the network would provide substantially enhanced survivability for the entire network.

The Status of Security Devices

The future of the DDN as a multi-level secure network depends critically upon the availability of security devices to support the system. In the near term, the classified segments of the network require IPLIs to provide end-to-end encryption across the network so as to maintain the security of communities of interest using different key variables. Because IPLIs are not suitable for remote keying, they cannot realistically be used to support a network used by multi-level secure hosts. Thus, the consolidation of individual nets into a true multi-level system must await BLACKER, with automatic key distribution. The KG-84 crypto device is required as part of the IPLI to provide end-to-end encryption, and to provide high grade link encryption even into the BLACKER era.

In its October 1983 meeting, the Task Force was dismayed to learn that the production rate of KG-84s was grossly inadequate

to meet projected DoD needs in general and DDN needs in particular. Measures taken subsequent to that meeting, including significant fund transfers to NSA to allow for the expansion of production facilities at the two contractors supplying them, led to a far more optimistic outlook by January 1984. It appeared that there had been a recognition of the problem and that given enough time (and funds), there would be enough KG-84s to meet the DDN's needs, if not those of all the Services. Both NSA and DCA deserve credit for moving quickly to deal with this issue which has now been resolved.

As noted above, IPLI development has encountered some significant problems. Delays have occurred, development costs have grown, and, most disturbing of all, unit costs have increased to a point where the proliferation of IPLIs to overwhelm possible security threats no longer appears to be a feasible option. Such an approach has characterized earlier DDN architectures. A new situation is emerging that threatens to "put the squeeze" on the program. On the one hand, IPLIs are needed to provide the end-to-end encryption that will allow different communities of interest with differing security concerns to operate on the same net. Because of IPLI development delays--and uncertainties about BLACKER (as will be seen below)--this requirement urges an early decision to expand IPLI production by establishing a second source. On the other hand, growing IPLI unit costs and the possibilities of the early development of a cheaper BLACKER device urge the limited use of IPLIs and the delay of network consolidation until BLACKER devices are available.

The BLACKER program has had its own difficulties. It got off to an ambitious start with the designation of DIRNSA as the Program Manger, the selection of a single development contractor, with a contract award in July 1983, and a DCA-proposed plan for the simultaneous development of nearly a dozen separate BLACKER devices meeting a full range of functional requirements. By the end of 1983, confidence in meeting the original schedule which called for limited procurement to begin in late 1988 had become shaky. In part, this situation was the result of growing concerns about the difficulties of accreditation which began to resemble those associated with AUTODIN II.

In the summer of 1984, it was concluded that redirection of the program was required. It was slipping on an almost day to day basis. A number of steps were taken to rectify this situation. BLACKER management at NSA was consolidated in a special Project Office, within the C Group (Computer Security) rather than being jointly shared with the S Group (Communications Security), and R Group (Research and Development). Both computer security and communications security accreditation criteria were defined and coordinated. A new delivery schedule

was established calling for production models of host-to-network interface devices to become available in late 1987. On 1 October 1983, a revised purchase description was sent to the contractor. The new implementation plan calls for a simplified approach with a reduction in the number of different devices to be developed. Emphasis was put on meeting IS/A AMPE requirements which are the first to emerge in 1987. The design was changed to employ a single logical processor chip in the host-to-host network interface, a move to simplify accreditation.

Despite the early difficulties, this new approach appears promising, though at the time it was briefed to the Task Force, contractor response to the revised purchase description had not been received by the SPO. If the new delivery schedule can be met, there is an argument for limiting IPLI use and waiting for BLACKER to become available to meet consolidation objectives.

The KG-84 production problem discussed above introduces a cautionary note, however. Though it appears the KG-84 problem has been resolved, it is not occurring until the fourth or fifth year of its production. This raises the concern about availability of BLACKER devices in sufficient quantities for the DDN. We keep automatically assuming that in 1988 BLACKER will be available. But if the experience with the KG-84 is any indication (and it almost certainly is), it may be three to five years longer before enough devices are available to significantly influence the evaluation of the DDN. This has to be a major concern of the DDN Program Office.

NSA also has at least one fall back development underway to reduce the impact of a delay in BLACKER availability. The program discussed with the Task Force involved a lower cost IPLI replacement that would allow network consolidation but not multi-level secure operations. Its schedule is roughly the same as that of BLACKER.

Security Architecture

All of these considerations lead naturally to the question of system architecture. If DDN is to fulfill the goals which motivated the AUTODIN II development and urged the move to DDN, it must ultimately attain the status of a fully consolidated, common-user network serving multi-level secure hosts. Program management difficulties, delays in the availability of security hardware, gateway design problems, and most importantly, unresolved security concerns have all led to repeated extensions of time before planned consolidation can occur.

The DSB DDN Task Force reviewed the DDN security architecture on January 17, 1984 and again on July 10, 1984. A third briefing

was scheduled for the October 5, 1984 meeting, but was not available at that time.

In general, the issue related to the detailed equipment arrangements which must be provided within DDN in order to provide adequate security safeguards to assure that it can be operationally accredited as a multi-level secure system. A related issue is the interaction between the classified and the unclassified segments of DDN, with the latter intended to act as a partial backup to the loss of some parts of the classified segment. As a result of the January meeting, a number of issues were raised that caused the PMO to review the entire issue.

In July it was reported that a number of working groups had been constituted, and that a series of meetings had been scheduled to culminate in the intended October description of a revised system-level security architecture. For example,

- DCA was to address the use of the unclassified segment by the classified segment.
- NSA was to investigate the possibility that secret users might not be required to use IPLI equipment.
- NSA and DCA were to jointly address the scenario that would start DDN with IPLI equipment and gradually phase it over to BLACKER equipment.
- NSA, DCA and the JCS were to investigate NATO interoperability with DDN.

It is in dealing with questions like these that the uncertainties about IPLI and BLACKER schedules tend to become crippling. As noted above, the question of whether or not to speed the rate of IPLI acquisition is particularly plaguing.

There are a number of optional configurations and equipment arrangements that can provide security--with greater or lesser user expense and convenience--for the DDN net. The most elegant arrangement of course is with BLACKER; the most onerous from the user's point of view, with IPLI.

As of this writing, the security architecture is unsettled although the timing of the Task Force meeting may have just been unfortunately early by a few weeks. The details of the architecture clearly interact with the BLACKER schedule, and may have implications for the quantity of IPLIs that the DDN PMO may have to buy. The latter issue is of some import because the anticipated price for an IPLI is presently based on a small buy.

The security architecture, together with its dependence on the BLACKER program and its consequences for the IPLI program,

is obviously of paramount importance. It must be possible to accredit DDN as a multi-level secure system; otherwise, important users will not be able to connect to it and the argument for DDN as a DoD common-user network will be seriously weakened.

The Task Force therefore recommends that:

- An oversight group be created to monitor the development of the security architecture for DDN, the status and progress of the BLACKER program, and (as necessary) the status and progress of the IPLI program.

Security issues have been a continuing source of concern from the very inception of the DSB Task Force, and it is regrettable to report that the situation has been very unstable.

There are additional aspects of security for DDN that the Task Force has not addressed. For example, what are the physical arrangements for the equipment; what are the operational rules for maintaining security; what are the clearance requirements for maintenance personnel (in particular) for node switches OCONUS? There is some risk that an important detail has passed unnoticed.

As soon as the security architecture settles down, the BLACKER schedule is judged clearly feasible and appropriate, it is recommended that:

- The DDN PMO produce a comprehensive overall system security plan for the DDN.

Appendix A

THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

RESEARCH AND
ENGINEERING

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Defense Science Board Task Force on the Defense Data Network

You are requested to organize and convene a Defense Science Board (DSB) Task Force to review, evaluate and make recommendations concerning the continuing evolution of the Defense Data Network (DDN) Program.

The DDN is the Defense-wide common user data communications system which resulted from the decision in April 1982 to terminate the AUTODIN II Program and provide data communications services to the Department through the evolution of existing ARPA network technology systems (e.g., ARPAnet, WWMCCS Intercomputer Network, Movement Information Network). Because of the critical nature of this project in providing the link between all DoD information systems, from highly sensitive C^3I systems to routine administrative and personnel systems, this program requires the extraordinary technical and management review which can only be afforded by a DSB Task Force.

The Task Force should address the full range of questions of network technology as applied to the DDN, cost, security, protocols, and other relevant topics.

The Task Force should begin its work as soon as possible. It should meet at least semiannually with the Senior Service Communicators and appropriate representatives of the JCS and Defense Agencies. A final report should be issued by October 1984 addressing these issues with a specific recommendation on the need for further review. Interim reports should be submitted as issues are resolved to the satisfaction of the membership.

This Task Force is sponsored by Donald C. Latham, Deputy Under Secretary of Defense (C^3I). Dr. Sayre Stevens, Chairman of the AUTODIN II Task Force, has agreed to serve as Chairman of this Task Force. Mr. Stephen T. Walker, Director, Information Systems (ODUSD (C^3I)), will be Executive Secretary. Dr. Ralph Chatham, LCDR, USN, will serve as DSB Staff Representative.

Appendix B

MEMBERSHIP

Defense Science Board Task Force

on

Defense Data Network (DDN)

Chairman

Dr. Sayre Stevens
Systems Planning Corporation

DSB Member

Dr. Harold Rosenbaum
Rosenbaum Associates, Inc.

Associate Members

MGen Van Doubleday, USAF (Ret.)
Honeywell Information Systems

Dr. Seymour Goodman
University of Arizona

Dr. Jerald J. Popek
University of California

Mr. John Stenbit
TRW, Inc.

Dr. Willis Ware
The Rand Corporation

Mr. Stephen T. Walker
Trusted Information Systems, Inc.

Executive Secretary

Col. John Lane, OSAD/C3I

Appendix C

AGENDA

Defense Science Board Task Force
on
Defense Data Network

AGENDA

DEFENSE SCIENCE BOARD TASK FORCE
on
DEFENSE DATA NETWORK

October 20-21, 1983
Room 1A1079, Pentagon

Thursday, October 20

0800-0830	Executive Session	DSB Members Only
0830-0930	DDN Overview	Col. H.B. Heiden
0930-0945	Army Comments	R. Turner
0945-1000	Navy Comments	Capt Byers
1000-1015	BREAK	
1015-1030	Air Force Comments	LtCol Millar
1030-1045	NSA Comment	Mr. D. Austin
1045-1100	OJCS Comments	Major R. Mundy
1100-1130	User Requirements	LtCol J. Wegl V. Russell
1130-1300	LUNCH BREAK	
1300-1700	DDN Update	
	-- MINET Status	Col H. B. Heiden
	-- WIN Subsystem	Mr. J. Milton
	-- MILNET Development	Dr. T. Harris Mr. W. Grindle
	BREAK	
	-- Secret Net Status	Maj S. Wold
	-- IPLI Update	Mr. J Claitor
	-- Test and Evaluation	Mr. R. Philbrook
	-- X.25 Development	Mr. P. Sevcik (BBN)
	-- Interface Development	LtCol J. Wegl
	-- R&D Initiatives	Mr. E. Cain

Friday, October 21

0800-0900	Executive Session	DSB Task Force
0900-0930	Mr. Latham, DSB, Flag & General Officers' Overview	Telecommunications Council
0930-1030	Mr. Latham, DSB, Flag & General Officers' Discussion	Telecommunications Council
1030-1200	Executive Session	DSB Task Force
1200	End of Review	

AGENDA

MEETING OF THE DEFENSE SCIENCE BOARD TASK FORCE

ON

THE DEFENSE DATA NETWORK

June 21-22, 1983
Room MF 614 Pentagon

Tuesday, June 21, 1983

0830-0915	Executive Session
0915-1200	Briefings by DCA
1200-1330	LUNCH
1330-1700	Briefings by DCA

Wednesday, June 22, 1983

0900-1000	Briefing By NSA
1000-1030	Briefing by Army
1030-1100	Briefing by Navy
1100-1130	Briefing by Air Force
1130-1200	Briefing by OJCS
1200-1330	LUNCH
1330-1700	Executive Session

DEFENSE SCIENCE BOARD TASK FORCE

DEFENSE DATA NETWORK

January 17-18, 1984

Room 2E465 Pentagon

AGENDA

Tuesday, January 17, 1984

0845-0900	Executive Session	DSB Members
0900-1010	DDN Overview	Col Heiden, DCA
1010-1030	BREAK	
1030-1130	Threat Briefing	Col Schell, NSA
1130-1300	LUNCH	
1300-1345	Security Architecture Update/Overview	Mr Corrigan, DCA
1345-1405	KG Requirements	Maj Wold, DCA
1405-1425	KG Allocation Status	DCA
1425-1445	BREAK	
1445-1515	IPLI Status	Mr Wood, BBN
1515-1545	BLACKER (BD2/3,AC,MC,KDC) Status	Mr Veiel, NSA
1545-1600	PMO Configuration Management	Mr Gudtschmidt, DCA

Wednesday, January 18, 1984

0845-0900	Executive Session	DSB Members
0900-0930	Gateway/TAC/Auth Unit Status	Mr Corrigan, DCA
0930-1000	DES Devices/TACACs	Mr Kent, BBN
1000-1020	Physical Security	Maj Mundy, OJCS
1020-1040	BREAK	
1040-1100	IASA Developments/Requirements	Mr Wilmot, DCA Mr Barnett, NSA
1100-1130	Security Assessment	Mr Bibb, NSA
1130-1300	LUNCH	
1300-1500	Executive Session	DSB Members

AGENDA

DEFENSE SCIENCE BOARD TASK FORCE
on
DEFENSE DATA NETWORK

July 10-11, 1984
Room 2E385, Pentagon

Tuesday, July 10, 1984

0845-0915	Executive Session	DSB Members
0915-1015	DDN Program Overview	Col Maybaum, DCA
1015-1030	BREAK	
1030-1200	Security Issues	
1030-1100	BLACKER Status	Mr. Bitzer, NSA
1100-1115	DDN View of BLACKER	Mr. Corrigan, DCA
1115-1145	KG84 Status	Mr. Bibb, NSA
1145-1200	KG84 DDN Impact	Maj Wold, DCA
1200-1330	LUNCH	
1330-1415	TCP/TP Report	Mr. Rosenburg, NSF
1415-1515	TCP/TP Issues Discussion	
1515-1530	Electronic Mail Overview	Ms. Fountaine, OSD

Wednesday, July 11, 1984

0845-0900	Executive Session	DSB Members
0900-0945	DDN Security Architecture Review	Mr. Corrigan, DCA
0945-1015	Low Cost DES Device Development	Mr. Sykes, NSA
1015-1030	BREAK	
1030-1230	New Technology Issues	Mr. Herman, BBN
	BBN Future Technology Study Update Interoperable X.25 Status End-to-End Protocol Design Congestion Control	
1230-1330	LUNCH	
1330-1600	Executive Session Draft Report Status	DSB Members