29 JUL 1994

Ref: 93-F-2472

Mr. Tod McMahon
GTE Librarian
Command, Control and Communications Systems
GTE Government Systems Corporation
77 "A" Street
Needham Heights, MA 02194-2892

Dear Mr. McMahon:

This responds to your November 1, 1993, Freedom of Information Act (FOIA) request pertaining to MCM-5-91, dated January 15, 1991. Our November 19 letter, your November 29 letter, and our December 13 interim response, refer.

The Joint Staff has provided the enclosed record as responsive to your request.

The administrative cost of processing this request was $99.45, of which $51.95 is chargeable. The chargeable cost consists of one hour search, and one hour review, at the professional level rate of $25.00 per hour; and 13 pages of office copy reproduction at $0.15 per page. Please indicate our reference number, **93-F-2472**, on a check or money order payable to the U.S. Treasurer in the amount of **$51.95**. To avoid interest charges, payment must be received in this Directorate within 30 calendar days of this letter's date. Our address is:

Office of the Assistant to the Secretary of Defense
(Public Affairs)
Directorate for Freedom of Information and
Security Review, Room 2C757
1400 Defense Pentagon,
Washington, DC 20301-1400

Copy to RR

Sincerely,

SIGNED

D. J. Blakeslee
Acting Director
Freedom of Information
and Security Review

Enclosure
Prepared by Kahn:3F2472L2:7/28/94:DFOI:X71160:gr✓pk__yl__wh__

940729

#627

209576

OFFICE OF THE CHAIRMAN
THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20318-0001

Reply ZIP Code:
20318-0300

MCM-5-91
15 January 1991

MEMORANDUM FOR: Distribution List

Subject: Requirement Statement on Tactical-Strategic Networking Capabilities

1. The enclosed document has been validated* and is to be used as the source document for the high-level requirements and architectural guidelines for tactical-strategic networking.

2. ASD(C3I) has been requested, under separate cover, to task DCA to present the program plan to the Defense Data Network (DDN) Executive Committee and to the Commercial Services Industrial Fund Resources Committee for planning within the existing DDN program structure. Those documents will then be submitted to the Director for Command, Control, and Communications Systems, Joint Staff, for formal Service coordination and approval.

For the Chairman, Joint Chiefs of Staff:

GENE A. DEEGAN
Major General, USMC
Vice Director, Joint Staff

Enclosure

Reference:
* SM-684-88, 23 August 1988, "Policies and Procedures For Management of Command, Control, and Communications Systems"

#629

DISTRIBUTION LIST

	Copies
Chairman, Joint Chiefs of Staff	1
Chief of Staff, US Army	1
Chief of Naval Operations	1
Chief of Staff, US Air Force	1
Commandant of the Marine Corps	1
Commander in Chief, US Atlantic Command	1
Commander in Chief, US Central Command	1
US Commander in Chief, Europe	1
Command in Chief, Forces Command	1
Commander in Chief, US Pacific Command	1
Commander in Chief, US Southern Command	1
Commander in Chief, US Space Command	1
Commander in Chief, US Special Operations Command	1
Commander in Chief, Strategic Air Command	1
Commander in Chief, US Transportation Command	1
Director, Defense Communications Agency	1
Director, Defense Intelligence Agency	1
Director, Defense Logistics Agency	1
Director, Defense Mapping Agency	1
Director, National Security Agency/Chief, Central Security Service	1
Director for Operations, Joint Staff	1
Director for Command, Control, and Communications System, Joint Staff	1
Director for Operational Plans and Interoperability, Joint Staff	1
Secretary, Joint Staff (Documents Division)	20

ENCLOSURE

1. Title. Requirement Submission (RS) on Tactical-Strategic Networking Capabilities, RS 1-90. (Strategic refers to data communications and automated information systems supporting fixed locations, not strategic weapon systems.)

2. Brief Description of the Deficiency

a. The deficiency inhibits operations.

b. Effective and efficient use of joint forces requires greater vertical and horizontal exchange of information than is fielded today. Past development of Service or function-unique networks supporting C2 and information systems has resulted in the fielding of noninteroperable equipment, limiting access to critical decisionmaking information. The unified and specified commands and the Services are often unable to interconnect automated information exchange systems at fixed locations into tactical transmission systems. Interconnection provides access to national assets for targeting, threat analysis, and adversary status, to name just a few capabilities. These links must support all military functional components and provide protection of the information at the required level of security, while denying access to those without the proper

need to know. Multiple level security networking must be extended into various types of tactical transmission media (systems) to support secure exchange of critical information among all echelons. The solution should also adhere to Department of Defense and/or Government Open Systems Interconnection Profile (GOSIP) and interface standards, NATO standardization agreements for data communication protocols, and available international commercial standards to ensure interoperability among subscribers.

3. Background

a. Historically, each of the Armed Services has developed communication systems that best meet their individual tactical requirements. Certain functional areas, such as intelligence, have instituted their own dedicated communications systems to maintain the security and quality of service they require. Fixed networks have been built to capitalize on the increased speed and capacity brought about by recent technology. Tactical networks, on the other hand, have concentrated on specialized hardware and unique protocols, tailored for their individual applications. Neither community has taken on the planning for interconnection and interoperability. The result has been sets of

communications networks with limited interconnections, for security, procedural, and technical reasons.

b. Each of the Services has increased the number of computers used as part of their support to strategic, mobile, and transportable communications platforms. In some cases, state-of-the-art packet switched networks are being planned to facilitate the movement of information among these computers in the tactical arena. These developments offer an excellent opportunity to increase the efficiency of data flow to all echelons by interconnecting tactical and strategic networks to achieve more effective connectivity. Greater survivability, interoperability, security, and cost avoidance are also gained by sharing network facilities and services.

4. Deficiency of Current or Planned Systems. Requirements are increasing at a rapid rate for the timely exchange of information among computers at tactical echelons, with each other and with fixed systems. In particular, tactical units have a requirement to exchange information with adjacent units, unified command elements, senior echelon components to the Military Services, and with national and allied defense agency information systems. This information exchange must occur in a timely and efficient fashion to support joint and combined operations, intelligence,

logistics, and special operations. While large amounts of the information are exchanged within unified commands and Military Service components, critical information often must be exchanged with allied force elements. Further, the information is frequently classified with compartmented caveats; other information is restricted to US-only dissemination or restricted to dissemination within allied organizations. Information is exchanged among computers in a variety of formats, including messages, images, files, and individual data elements. These requirements can be adequately supported only by ensuring that information sent through a given network between two computers, or between two computers attached to different networks, is protected at the proper security level and delivered only to the proper recipient in a timely and efficient manner.

5. Operational Concept

a. Without automated interconnection, many of the benefits computers provide are lost due to the need for cumbersome and awkward manual interfaces. Information from strategic networks cannot be provided instantaneously. As an example, a Tactical Air Control Center (TACC) may not have up-to-the-minute information on the location of enemy air defenses. In fact, they could have relocated since the

latest tactical update while national systems would have that information. Without an automated interface between the tactical and strategic automated information networks, the TACC could vector aircraft into the teeth of the enemy air defenses. This is one example of the threats created by the lack of interoperability between tactical and strategic networks.

b. The core requirements for tactical-strategic networking are complex. In order to take full advantage of the capabilities of tactical automated information systems, it is essential to allow them access to all necessary information in an efficient and timely manner, wherever the source. That capability includes the following characteristics:

(1) Provide computer-to-computer exchange of data within and across network boundaries where necessary and appropriate. Examples of information passed in actual contingencies are intelligence dissemination, logistics and supply information, mission planning, and AUTODIN data traffic.

(2) Protect the security of data exchanged between computers using a networking approach able to handle all levels of classification. Initially, physically separate

networks may be required to interoperate with Defense Secure Networks (DSNET) 1, 2, and 3, with transition to a fully integrated network capable of handling all levels of classification. This capability should be developed in conjunction with the effort to combine DSNETs 1, 2, and 3 into one network for classified data transmission. Security provisions for the network will be developed in accordance with established security policy. Combining classified networks will allow more effective use of transmission media. Rather than separate links for systems of different classifications, one packet switch node with fewer trunks can potentially handle all levels of classification. This will free up much needed transmission capacity. Additionaly, having a single data switch for various levels of traffic will reduce the amount of information an adversary could obtain through traffic analysis.

(3) Minimize management resources required to support connection with those common networks.

(4) Minimize resource personnel and equipment requirements through efficient interface to and application of DCS backbone resources to support common-user tactical internetworking.

(5) Increase effectiveness of operating commands by integrating and networking existing communications systems. The interconnectivity of the network will be mainly at the physical, data, and transport levels. Applications software will be provided on the host systems interconnected by the network. Integrated Tactical-Strategic Data Network (ITDN) protocols must interoperate with those of the Defense Data Network (DDN).

(6) Provide a basis for future evolution through application of GOSIP communications and interface standards.

c. The operational concept for fulfilling these requirements must:

(1) Be based on an internetworking approach, focused on interoperability, which can be implemented in the near term to meet joint tactical information transfer requirements without extensive new development. It will provide the same functionality as DDN, such as multiaddressing and connection to any DDN subscriber host (dial up or direct connect), and comply with DDN security criteria. The basic network must be evolvable to GOSIP

protocols, if not available at initial implementation, to allow for interoperability of all Service tactical packet switching networks.

(2) Provide a feasible and effective interface between the strategic communications network and tactical networks and allow all tactical networks to use each other's data transport capability. This will be accomplished by employing existing DOD and international communications technology standards.

(3) Provide the capability for tactical-strategic networking at multiple security levels.

(4) Include network management capabilities that are effective for integrated tactical-strategic networks with network management focused at the component command level and above. Networks and capabilities should be integrated with circuit switch management functions to provide system-level management.

(5) Deny the adversary access to the network for interception, deception, traffic analysis, and jamming. These concerns must be addressed in capability development.

6. Additional Justification. The US Army is deploying mobile subscriber equipment (MSE) area communications and planning to provide modern packet switched network overlay service to MSE to handle efficiently intercomputer information exchange. A similar approach to overlaying packet switching on tactical communications systems used to connect echelons above Corps is also feasible, but requires joint approval of the Military Services. Headquarters, US Air Force, issued Statement of Need (SON) 07-89, "Tactical Secure Data Communications (TASDAC)." The SON states that the Air Force needs the capability to use available time-sensitive C2, intelligence, and mission support information to lower echelon operating forces. Within the US Navy, MROC 2-88 (Tactical Department of Defense Intelligence Information System) specifically requires connection of afloat computers to national and/or strategic data bases. The Navy has also confirmed the applicability of an integrated tactical-strategic data networking architecture in Navy C3 system planning objectives to ensure interoperability among future tactical data systems.

7. Alternatives Considered. Development of an entirely new capability, in the near term, would be prohibitively expensive. Attainment of interoperability by enforcement of standards is a long-term goal to be met through an evolutionary process. For

the near term, the equipment and procedures developed as part of the ITDN demonstration, conducted in September 1989, should be considered for adaptation and use as a tactical-strategic network. ITDN consists of a multimedia, multisystem, multisecurity level, integrated tactical and strategic packet switched data communications network. The architecture provides a data communications infrastructure model, based on nondevelopmental technology, which transparently supports multiple security information transfer over a common user tactical communication network, across multiple tactical networks, and interconnections with strategic data communication networks. ITDN is a proven approach that provides a baseline capability. ITDN concepts and configurations are essentially ready to be employed. Military Departments and Defense agencies can begin to develop the necessary guidance to implement the ITDN capability in their information systems by the early 1990s. Policy and standards guidance should be developed with capability to migrate to GOSIP communications and interface standards as a fundamental requirement. Employing evolutionary acquisition will be essential. This allows the combatant and supporting commands to employ current capabilities to satisfy existing requirements while planning for upgradings to an open systems interconnecting

environment as that technology evolves. ITDN was employed during proof of concept as follows (this is not all-inclusive):

a. DIA-sponsored integration of packet switches into very small aperture satellite terminals for potential use as quick-reaction mobile communications packages.

b. Rome Air Development Center used HF radio to transmit imagery that was subsequently input into a gateway computer connected to the ITDN internet.

c. Packet switches were incorporated into tactical transmission systems such as mobile subscriber equipment, AN/TTC-39A circuit switch, ground mobile forces satellite terminals and UHF fleet satellite.

8. Priority Category. The capability to establish intercomputer communications is a critical element of C3I systems and should have a priority as high as those systems overall.