DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

AUG 2 4 2000

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Department of Defense (DoD) Chief Information Officer (CIO) Guidance and Policy Memorandum No. 4-8460 - Department of Defense Global Information Grid Networks

In a memorandum, "Global Information Grid," dated September 22, 1999, the DoD CIO issued guidance on the definition and scope of the Global Information Grid (GIG). In essence, the GIG is "a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel."

The DoD CIO's memorandum represented the first formal output of an initiative that began in December 1998 to develop policies on several aspects of information management, including information technology management, for the Department. The initial thrust has been on the development of GIG policies and procedures for governance, resources, information assurance, information dissemination management, interoperability, network management, network operations, enterprise computing, and aligning the technology base to support these activities.

The attached guidance on Global Information Grid networks is one in a series of GIG policies that provides direction and assigns responsibilities for effective, efficient, and economical acquisition, management, and use of network equipment and services. It is effective immediately. If the infrastructure required by GIG network processes is not present, supporting PPBS actions may be necessary.

This Guidance and Policy Memorandum (G&PM) provides high level policy for immediate implementation. It shall also be used to develop future directives and instructions which shall replace DoD Directive 4640.13, " Management of Base and Long-Haul Telecommunications Equipment and Services," December 5, 1991, and DoD Instruction 4640.14, "Base and Long-Haul Telecommunications Equipment and Services," December 6, 1991. In the event of conflict, this G&PM takes precedence over the two aforementioned documents.

Improved and timely GIG policies are the cornerstone to enabling change, eliminating outdated ways of doing business, implementing the spirit and intent of the Clinger-Cohen Act and other reform legislation, and achieving our Information Superiority goals. While the attached policy guidance is effective immediately, I direct the DoD CIO, in coordination with the Director, Administration and Management, to incorporate it into the DoD Directive System within 180 days.

Rudy de Leon

Attachment:
As stated

U08593 /00

DISTRIBUTION:

SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
COMMANDERS OF THE UNIFIED COMBATANT COMMANDS
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS
DIRECTOR, COMMAND CONTROL, COMMUNICATIONS AND
COMPUTER SYSTEMS, JOINT STAFF
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES
DIRECTOR, INTELLIGENCE COMMUNITY MANAGEMENT STAFF
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER

Guidance and Policy
for
Department of Defense Global Information Grid Networks

References: (a) DoD Directive 4640.13, "Management of Base and Long-Haul Telecommunications Equipment and Services," December 5, 1991

(b) DoD Instruction 4640.14, "Base and Long-Haul Telecommunications Equipment and Services," December 6, 1991

(c) DoD Instruction 5200.40, "Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997

(d) DCI Directive 1/6, "The Intelligence Community Chief Information Officer," February 4, 2000

(e) DCI Directive 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," June 5, 1999

(f) DEPSECDEF Memorandum, "FY 2000 Implementation of Commercial Pricing for Telecommunications Services," October 19, 1999

1. PURPOSE. This guidance and policy:

1.1 Ensures effective, efficient, and economical acquisition, life-cycle management, and use of DoD Global Information Grid (GIG) networks and their component network equipment and services.

1.2 Establishes the Defense Information Systems Network (DISN) as DoD's networking capability for the transfer of information in support of military operations, in the context of the Global Information Grid.

1.3 Strengthens security, information assurance, interoperability, and quality and consistency of GIG networks.

2. APPLICABILITY and SCOPE. This guidance and policy applies to:

2.1 The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense (IG, DoD), the Defense Agencies and Offices (see enclosure 2), and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2 Information technology and its operation by DoD Intelligence Agencies, Service intelligence elements and other intelligence activities engaged in direct support of Defense missions. Global Information Grid implementation must comply with policy and responsibilities established herein and, wherever applicable, separate and coordinated Director of Central Intelligence (DCI) Directives and Intelligence Community (IC) Policy.

2.3 All network assets and services (including components embedded in information systems and contractor-acquired capabilities) that are administered, managed, acquired, operated or used by the DoD Components. Under the GIG Reference Model (enclosure 1) these networks fall into five categories: Local Area Networks, Campus Area Networks, Operational Area Networks, Metropolitan Area Networks, and Wide Area Networks.

2.4 If there is a conflict between this document and references (a) or (b), this document takes precedence.

3. DEFINITIONS. Terms used in this issuance are defined in enclosure 2.

4. POLICY. It is DoD policy that:

4.1 All GIG networks possess strict security attributes as specified in the GIG Information Assurance (IA) Guidance and Policy Memorandum (G&PM).

4.2 The GIG shall have the necessary attributes and standards to ensure network interoperability. The Defense Information Systems Network (DISN) shall be the means for DoD Wide and Metropolitan Area (WAN, MAN) networking, unless granted a waiver through the DISN/GIG Waiver Board, and it shall provide the DoD with voice, data, and video services, as well as provide ancillary enterprise services such as directories and messaging. The DISN shall provide Global Information Grid (GIG) network services to DoD installations and deployed forces.

4.3 All decisions on whether to develop a MAN shall be made on an enterprise basis. All MANs shall be developed to preclude the existence of multiple MANs in a given region. MANs will come under the same or complementary funding mechanism as the WAN and will have provisioning and financial mechanisms to ensure services are provided to all DoD users in the region on an equitable basis. MANs will be designed to be interoperable with the WAN and will not extend beyond their service regions.

4.4 GIG networks established for support of the sustaining base and the deployed forces shall be provided and operated by the CINCs, Services and Agencies, except in those instances where other arrangements are determined appropriate by the DoD CIO. The Local Area Networks (LAN), Campus Area Networks (CAN), and Operational Area Networks (OAN) shall be GIG-compliant and therefore fully capable of receiving the GIG network services provided by the DISN WAN and MANs.

4.5 GIG networks and services shall be managed end-to-end. From LAN solutions in the sustaining base, across the WAN/MANs environment, to deployed OANs (also known as Theater Joint Tactical Networks (TJTN)), the GIG networks shall operate as a fully-interoperable network through managed application of standards and configuration management discipline.

4.6 Each GIG network shall have sufficient end-to-end visibility to satisfy management, interoperability, and information assurance requirements.

4.7 GIG networks shall be certified and accredited in accordance with DoD Instruction 5200.40, "Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997 (ref. c). SCI networks shall be certified and accredited in accordance with DCID 6/3 (ref d).

4.8 Quality of service shall be assured by a uniform evaluation process, which shall include collection and reporting of performance metrics on networks, providers, managers, and users.

4.9 Commercially leased and Government-owned assets incorporated into the DISN WAN and associated MANs shall be, unless otherwise directed by DoD, funded through the two-tier pricing system currently used in the Defense Working Capital Fund (DWCF) as provided by reference (f).

4.9.1 Tier one shall cover the cost of assets to provide the military readiness of the GIG WAN and MANs, with costs shared equitably among all DoD components.

4.9.2 Tier two shall cover all remaining network costs, and shall be financed based upon usage, with rates linked to regionally prevailing commercial rates and directly paid by the customer incurring that cost.

4.10 Existing Wide and Metropolitan Area Networks (WANs, MANs) not presently a part of the DISN shall be reviewed for migration to the DISN.

4.11 Any outsourcing activity shall also be subject to this policy.

5. RESPONSIBILITIES.

5.1 The DoD Chief Information Officer shall:

5.1.1 Enforce the provisions of this policy.

5.1.2 Develop, maintain and enforce the Global Information Grid Architecture.

5.1.3 Approve migration strategies for DoD Component WANs and MANs for incorporation into the DISN.

5.1.4 Designate Components or major organizational elements as GIG network providers, managers or executive agents.

5.1.5 Establish and oversee reporting requirements

5.1.6 Oversee the acquisition and procurement of DoD GIG network assets.

5.1.7 Consult, where appropriate, with the IC CIO on matters of GIG policy, acquisition, implementation, and operation.

5.2 Heads of DoD Components shall ensure that all organizational elements:

5.2.1 Extend GIG common services, to include voice, data, and video, to their organizations within the sustaining base and deployed environments.

5.2.2 Identify WANs and MANs as candidates to be incorporated into the DISN.

5.2.3 Plan for and schedule migration or disestablishment of any WAN or MAN as directed by the DoD CIO.

5.2.4 Perform as GIG network providers, managers, or executive agents where designated by the DoD CIO.

5.2.5 Participate in development of the standards necessary to make the five categories of GIG networks GIG-compliant, so as to operate as an interoperable, end-to-end service, including the network management component.

5.2.6 Comply with the standards approved for the GIG.

5.2.7 Assess and evaluate the performance of GIG networks within their purview and provide periodic reports to the DoD CIO and others as directed in support of DoD assessments.

5.2.8 Ensure that providers and managers of GIG networks coordinate planning and implementation to maximize full interoperability and synchronization.

5.3 The Secretary of the Army, in addition to the responsibilities specified above, shall designate an Executive Agent for Theater Joint Tactical Networks (TJTN).

5.4 The Director, Defense Information Systems Agency shall, in addition to responsibilities described above:

5.4.1 Manage DISN Wide Area Networks and Metropolitan Area Networks unless an exception is granted.

5.4.2 Provide commercial satellite transport network assets for the DoD.

5.4.3 Develop and configuration-manage the standards necessary to support fully integrated service connection, including network management, across the five categories of GIG networks.

5.4.4 Lead technical efforts related to the end-to-end integration and capability of GIG networks to include testing support, interoperability certification, and joint spectrum management.

5.4.5 Advise the DoD CIO on quality of service, interoperability and integration matters affecting GIG networks.

5.4.6 Assess wideband network technologies with potential application to GIG networks.

5.4.7 Provide support to the DoD CIO, Joint Staff, Joint Forces Command, and other CINCs to achieve GIG network interoperability.

5.5 The Intelligence Community Chief Information Officer (CIO), on behalf of the DCI pursuant to references (d) and (e), has agreed to perform the following functions:

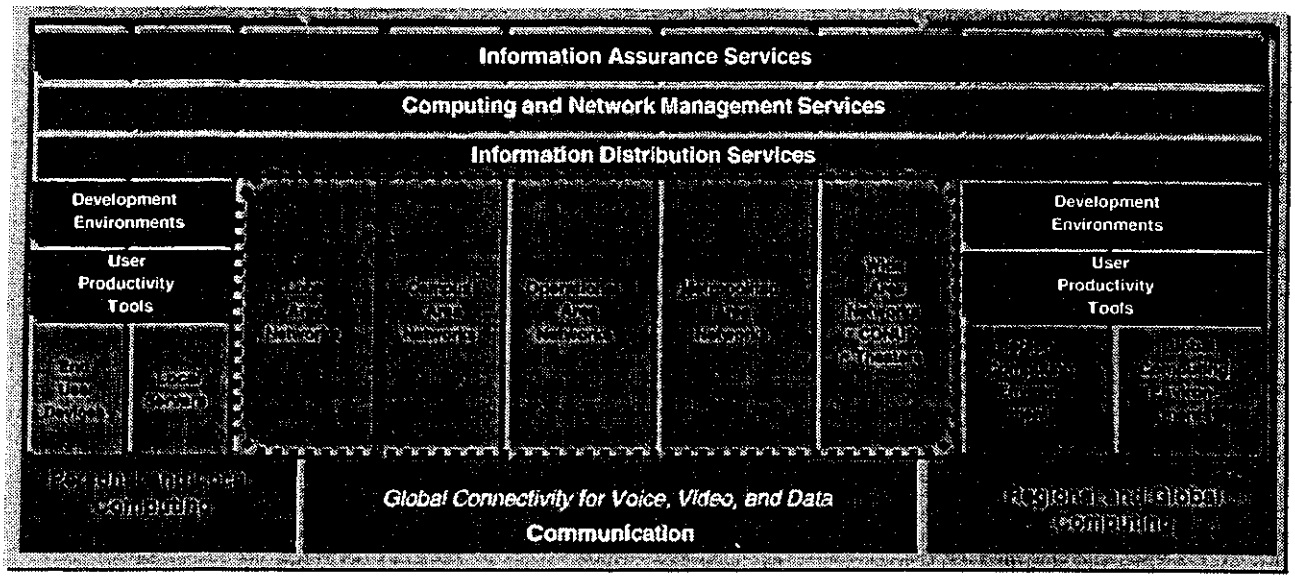
5.5.1 Co-designate, with the DoD CIO, a select set of IC networks, to include all SCI networks, to be defined as the IC portion of the GIG.

5.5.2 Develop, maintain, and enforce the IC portion of the GIG Architecture.

5.5.3 Consult, where appropriate, with the DoD CIO on matters of GIG policy, acquisition, implementation, and operation.

6. EFFECTIVE DATE. This policy is effective immediately upon issuance and until superseded. In the event of conflicts between this policy and other information management or Global Information Grid guidance and policy, this issuance takes precedence.

Enclosure 1: GIG Reference Model: Networks Environment



GIG Networks: DISN-Compliant

Enclosure 2: DEFINITION OF TERMS

E2.1 **Defense Agencies and Offices:** All agencies and offices of the Department of Defense, including Ballistic Missile Defense Organization, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, Defense Information Systems Agency, Defense Intelligence Agency, Defense Legal Services Agency, Defense Logistics Agency, Defense Threat Reduction Agency, Defense Security Cooperation Agency, Defense Security Service, National Imagery and Mapping Agency, National Reconnaissance Office, National Security Agency.

E2.2 **End-to-end**: The inclusion of all requisite components to deliver a defined capability. For the GIG, this implies all components from the user access and display devices and sensors to the various levels of networking and processing, all associated applications, and all related transport and management services. For the DISN services, end-to-end encompasses service user to service user (e.g., PC-to-PC, phone-to-phone).

E2.3 **Defense Information Systems Network (DISN)**: The DISN is an element of the GIG. It is the DoD's worldwide enterprise-level telecommunications infrastructure that provides end-to-end information transfer for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner. The DISN is a construct with defined military requirements that includes all five categories of the GIG reference model.

E2.4 **CAN (Campus Area Network):** Generally considered as the next level in scale of operation to the LAN, a CAN is an interconnected series of LANs within a contiguous area. Within the Defense Department, this is most often aligned with the network environment contained within the boundary of a post, camp, or station.

E2.5 **IC portion of the GIG:** The IC portion of the GIG is the IC worldwide enterprise-level telecommunications infrastructure that provides end-to-end information transfer for supporting IC operations within the Sensitive Compartmented Information (SCI) environment. It is transparent to its users, facilitates the management of information resources, and is responsive to national security, IC, and defense needs under all conditions in the most efficient manner. The IC portion of the GIG is a construct with defined IC requirements that includes all five network categories of the GIG reference model.

E2.6 **LAN (Local Area Network):** A physical medium and associated equipment that supports the interconnection of computers and peripherals usually over a limited physical area such as a building, base, post, or station and under a single management control. The LAN demarcation point is the campus, base, post, or station router/switch.

E2.7 **MAN (Metropolitan Area Network):** A system of links or a ring that interconnects a relatively high concentration of LANs together within a small regional area. It is normally used as the means to efficiently connect numerous LANs to each other as well

as to a WAN(s). The MAN also provides switching and routing between the LANs as well as between the WAN and the LANs. The demarcation points for the MAN are the service delivery nodes at the campus, base, post, or station router/switch and the hub/router/switch of the WAN.

E2.8 **Manage:** In the context of paragraph 5.4.1, means: 1) design and CONOPs approval to ensure interoperability, security, and maintenance of appropriate end-to-end visibility and control; and 2) obtain funding mechanism approval to ensure services are provided to all DoD users on an equitable basis and provisioning and funding procedures are simple and consistent across DoD.

E2.9 **OAN (Operational Area Network):** Those networks created out of assets organic to deployed units, or serving principally to connect deployed units to each other. This is normally the primary mechanism for establishing the Theater Joint Tactical Network (TJTN) from individual Service-deployed CANs and LANs supporting their tactical forces, and interfacing with the DISN MAN/WAN.

E2.10 **Provisioning**: The establishment, operations, and maintenance of voice, data, video transmission, and other services on a network in such a way as to provide end-to-end service to the user.

E2.11 **WAN (Wide Area Network):** A system of links that are used to interconnect geographic regions. The WAN normally provides routing, switching, or gateway points to MANs, LANs, or other WANs.