DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

AUG 24 2000

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Department of Defense (DoD) Chief Information Officer (CIO) Guidance and Policy Memorandum No. 10-8460 - Network Operations

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, networks, network operations, enterprise computing, and aligning the technology base to support these activities.

The attached guidance on Global Information Grid Network Operations is intended to continue the Department's operational focus on the management of the Global Information Grid. It establishes an operational hierarchy that promotes CINC oversight over Component network management capabilities, achieving end-to-end distributed control while providing a common view and joint use of management information. This gradual transformation is intended to shift responsibility for the operation and protection of critical DoD networks into the operational chain of command.

Improved and timely GIG policies are the cornerstone to enabling change, eliminating outdated ways of doing business, implementing the spirit and intent of the Clinger-Cohen Act and other reform legislation, and achieving our Information Superiority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

U08592 /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 THE DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND
COMPUTER SYSTEMS, JOINT STAFF
CHIEF INFORMATION OFFICER OF THE DEFENSE AGENCIES
DIRECTOR, INTELLIGENCE COMMUNITY MANAGEMENT STAFF
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER

Guidance and Policy
for
Department of Defense Global Information Grid Network Operations

References: (a) Global Information Grid (GIG) Overarching Policy

(b) Universal Joint Task List, Chairman, Joint Chiefs of Staff Manual (CJCSM) 3500.04B, October 1999

(c) Status of Resources and Training System (SORTS), Joint Pub 1-03.3, August 1993

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

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

1. PURPOSE : This guidance and policy:

1.1 Establishes a Global Information Grid (GIG) operational hierarchy integrating the CINCs, Services , and Agencies.

1.2 Provides for end-to-end distributed GIG control while providing a common view and joint use of management information.

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

2.1 The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Joint Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies (see Enclosure 1), and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2 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. This encompasses five network categories presented in the GIG Reference Model, contained in reference a, namely, Local Area Networks, Campus Area Networks, Operational Area Networks, Metropolitan Area Networks, and Wide Area Networks.

2.3 This policy recognizes that special measures and exceptions may be required for protection/handling of foreign intelligence or counterintelligence information, Sensitive Compartmented Information (SCI), Single Integrated Operational Plan-Extremely Sensitive

Information (SIOP-ESI), Special Access Program (SAP) information, or other need-to-know information. Accordingly, implementation of this policy must comply, where applicable, with separate and coordinated Director of Central Intelligence (DCI) directives and Intelligence Community (IC) policy.

3. **DEFINITIONS** : Terms used in this issuance are defined in Enclosure 1.

4. **POLICY** : It is DoD policy that:

4.1 DoD will execute Network Operations through a system that distributes management and control functions to Components who are responsible to provide those networks, while integrating CINC operational oversight.

4.2 The DISN Wide Area Network (WAN) and associated Metropolitan Area Networks (MANs) shall operate under a single manager.

4.3 DoD Components exercising management responsibilities for the DISN will be cognizant of DISN support to the NCA, and other global equities, and will preserve DISN integrity and standards.

4.4 Standards-based, interoperable monitoring, control and management capabilities for GIG networks shall be implemented, consistent with the GIG Architecture.

4.5 GIG networks shall be controlled within a tiered management hierarchy consisting of global, regional, and local control centers.

4.6 Network Management, Information Assurance, and Information Dissemination Management activities within organizations who have responsibilities for providing networks and/or extensions shall operate under a single manager, so as to support visibility and security monitoring of all assets identified as part of the DoD GIG.

4.7 GIG network operations information, to include network service visibility, shall be exchanged among DoD and IC Components to facilitate end-to-end management, as well as regional and global situational awareness.

4.8 Combatant CINCs will exercise operational oversight over their apportioned, allocated or assigned network environment through their support relationship with DISA regional offices, as well as through those forces assigned to them in Forces for Unified Commands, or as modified by deployment orders.

4.9 The Intelligence Community Agencies will retain control of network assets and services of the IC portion of the GIG in support of both warfighting and other national interests. As such, they will remain under the control of their respective network manager to the extent necessary to provide protection unique to intelligence information, and to ensure that there is no conflict with other National mission requirements. Operational area extensions to Sensitive Compartmented Information (SCI) networks will come under TACON of the supported CINC through the CINC J2 and J6.

5. <u>RESPONSIBILITIES</u> :

5.1 The <u>DoD Chief Information Officer (CIO)</u> shall:

5.1.1 Designate Components as GIG providers, managers, or executive agents as necessary.

5.1.2 Develop, maintain, and enforce Global Information Grid architecture and standards.

5.1.3 Incorporate performance measures to supplement this policy in Agency support contracts and oversee performance.

5.1.4 Coordinate, where appropriate, with the Intelligence Community CIO on matters of GIG policy, acquisition, implementation, and operation.

5.2 The <u>Chairman of the Joint Chiefs of Staff</u> shall:

5.2.1 Exercise operational oversight of the DISN through the National Military Command Center (NMCC) and DISA's Global Network Operations and Security Center (GNOSC).

5.2.2 Manage the apportionment and allocation of network resources, including the adjudication between CINCs and Services.

5.2.3 Lead the development of common network operations tasks for inclusion into the Universal Joint Task List (UJTL) (reference. b).

5.2.4 Promulgate instructions associated with this policy by coordinating development of Joint Doctrine, Tactics, Techniques, and Procedures (JTTPs) for network operations tasks. Develop criteria and standards for assessing and reporting the readiness status of networks with the intent of incorporating into the Status of Resources and Training System (SORTS) process, as established by Joint Publication 1-03.3, "Status of Resources and Training System (SORTS)", August 1993 reference (c).

5.2.5 Lead the development of a framework for a theater Network Common Operational Picture (Network COP).

5.3 The Commanders in Chief (CINCs) Unified Commands shall:

5.3.1 Oversee and coordinate network operations within their areas of responsibility or theaters through the Defense Information Systems Agency (DISA) Network Operations and Security Center (NOSC) hierarchy, Service Component Command Regional NOSCs as appropriate, and Joint Task Force control centers.

5.3.2 Collaborate with their respective Service Component Commands, DISA, and CINC United States Space Command to create and maintain a theater Network COP.

5.3.3 Develop specific theater unique Tactics, Techniques, and Procedures (TTPs) for network operations, consistent with joint doctrine and TTPs.

5.3.4 When designated as a supporting CINC, provide network visibility to the supported CINC, as required.

5.4 The Commander in Chief (CINC) US Space Command shall:

5.4.1 Direct DoD Computer Network Defense (CND) operations.

5.4.2 Apprise the Chairman, Joint Chiefs of Staff on CND matters impacting the DISN's integrity and support of Defense Department missions.

5.4.3 Exercise TACON over DISA's GNOSC through the Commander, JTF-CND, only with respect to computer network defense activities.

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.

5.6 The Heads of Military Departments and Defense Agencies shall ensure that all organizational elements:

5.6.1 Acquire and maintain standards-based network management systems in accordance with the GIG Architecture.

5.6.2 Establish a global Network Operations and Security Center (NOSC), as appropriate, to serve as a central point of contact in operational matters concerning the DoD Component's portion of the GIG, . The global NOSC will also serve as a central point of contact in operational and emergency provisioning aspects for a supported CINC, when the needs are beyond the capability of the regional NOSCs.

5.6.3 Establish regional NOSCs, as appropriate, to provide a single point of contact for the theater DoD Component for network services, operations status, and anomalies. They may also serve as a central point of contact for operational matters in support of a theater CINC.

5.6.4 Establish Local Control Centers (LCC), as appropriate, to manage and control networks and services either deployed or fixed at the base, post, camp, or station. The LCCs provide the "first line" of problem resolution and are the primary points of contact concerning reliability and availability of managed resources.

5.6.5 Exercise routine, day-to-day management and control of their GIG elements.

5.6.6 Report on their capability to perform Network Operations through the SORTS process, as established by reference (c).

5.6.7 Consolidate Network Management, Information Assurance (to include Computer Emergency Response Team (CERT)), and Information Dissemination Management (IDM) capabilities into an organization consistent with the tiered hierarchy prescribed by this policy.

5.6.8 Provide DISN visibility to DISA regional operations centers, and other DoD Component NOSCs to facilitate end-to-end management, as well as regional and global situational awareness. Special Compartmented Information (SCI) networks controlled by DoD Components shall only be included if the requisite protection is afforded that visibility by the regional center.

5.7 The Director, Defense Information Systems Agency (DISA), in addition to the responsibilities specified in paragraph 5.5 shall:

5.7.1 Integrate the overall DISN, through management of the Wide Area Network and Metropolitan Area Networks, unless an exception is granted, and through standards, all other networks provided by DoD Components utilized to extend DISN services. Advise the Chairman, Joint Chiefs of Staff and CINCUSSPACECOM on matters regarding the allocation of DISN resources and network anomalies.

5.7.2 Maintain visibility to include security provisions of the DISN, through a DoD-Component-integrated Global Network COP.

5.7.3 Coordinate DISN network operations across service delivery points or demarcation lines which are associated with the control of network resources.

5.7.4 Coordinate the provisioning of network services across the transport network, in accordance with CJCS and CINC requirements. As such, DISA will serve as the single point of contact for Component DISN managers when they require service continuity across multiple transport networks.

5.7.5 Lead the development, under the direction of the DoD CIO, of the joint network management component of the GIG Architecture, in collaboration with the CINCs, Services, and Agencies.

5.7.6 Support the Combatant Commands in the creation of a Network COP for their Areas of Responsibility.

6. **EFFECTIVE DATE**: This guidance and policy is effective immediately.

Enclosure 1: Definitions

E1.1 Campus Area Network (CAN): 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.

E1.2 Control of a network resource implies an ability to monitor the resource, but also includes the ability to manipulate the functioning of that resource, or allocate it to a specific use.

E1.3 Defense Agencies: All agencies and offices of the Department of Defense including the 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.

E1.4 Defense Information Systems Network (DISN): The DISN is an element of the GIG. It is the DoD's consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network 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.

E1.5 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).

E1.6 Global Information Grid (GIG): is the 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 GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

E1.7 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.

E1.8 Local Area Network (LAN): 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.

E1.9 Local Control Center (LCC): is a GIG asset that manages CINC, Service, or Agency unique networks, systems, applications, and services either depolyed or fixed at the base, post, camp, station.

E1.10 Manage: In the context of paragraphs 4.2 and 5.7.1 means: 1) design and CONOPS approval to ensure interoperability, security, 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.

E1.11 Metropolitan Area Network (MAN): 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.

E1.12 Monitoring is to watch, observe, and check on a resource for a specific purpose. It may require the ability to communicate directly with the resource and receive status related information.

E1.13 Network Common Operational Picture (Network COP) is a graphical depiction of warfighting information available in an Area of Responsibility (AOR). A Network COP displays network resources showing their operational status and linkage to other resources. When supplemented with additional automated tools and sensors, it is utilized to create and maintain GIG situational awareness.

E1.14 Network Operations are the organizations and procedures required to monitor, manage and control the Global Information Grid. Network operations incorporate network management, information dissemination management, and information assurance.