



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAR 31 2000



MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
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
COMMANDERS OF THE COMBATANT COMMANDS
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

SUBJECT: DoD Chief Information Officer (CIO) Guidance and Policy Memorandum
No. 8-8001- March 31, 2000 - Global Information Grid

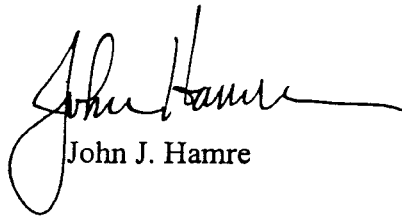
In a memorandum, "Global Information Grid," dated September 22, 1999, the DoD CIO issued guidance on the definition and scope of the Global Information Grid. In essence, the Global Information Grid is "a globally interconnected, end-to-end set of information capabilities, associated processes and personnel 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 Global Information Grid 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.

U04863-00

The attached overarching guidance defines the major policy principles and associated responsibilities for the Global Information Grid. Additional guidance and policy will be issued to further specify aspects of the Global Information Grid as needed to facilitate its implementation across the DoD.

Improved and timely Global Information Grid 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, to ensure that this policy is institutionalized, I direct the DoD CIO, in coordination with the Director, Administration and Management, to incorporate it into the DoD Directive System within 180 days.



John J. Hamre

Attachment:
As stated

Guidance and Policy For The Department of Defense Global Information Grid

- References:**
- (a) Title 10, U.S.C., Section 2223
 - (b) "DoD Information Management (IM) Strategic Plan," Version 2.0, October, 1999.
 - (c) "DoD C4ISR Architecture Framework," Version 2.0, December 18, 1997
 - (d) Subdivision E of the Clinger-Cohen Act of 1996 (CCA), Public Law 104-106, as amended; Section 5142 of the National Defense Authorization Act for Fiscal Year 1996 (40 U.S.C. 1452))
 - (e) Secretary of Defense Memorandum, "Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106)," June 2, 1997
 - (f) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01 A, "Requirements Generation System," August 17, 1999
 - (g) DoD Directive (DoDD) 5000.1, "Defense Acquisition," March 15, 1996 with Change 1, May 21, 1999
 - (h) DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," Change 4, May 11, 1999
 - (i) DoD Joint Technical Architecture (JTA), Version 3.0, November 29, 1999

1. PURPOSE: This guidance and policy:

1.1 Provides for the Global Information Grid (GIG) as a cornerstone in the Department of Defense's (DoD) Revolution in Military Affairs, the Revolution in Business Affairs and in enabling the achievement of Information Superiority.

1.2 Provides overarching DoD guidance, policy and implementation direction for the Global Information Grid in accordance with the authorities referenced herein. Specifically, this policy addresses the relationship of the Global Information Grid to major DoD processes for requirements, resource management and provides policy direction for Global Information Grid configuration management, architecture, and the relationships with the Intelligence Community and Defense intelligence components.

1.3 Assigns management responsibilities for the managing the Global Information Grid on an Enterprise basis in compliance with the Clinger-Cohen Act of 1996 (reference (d)) and Title 10, U.S.C., Section 2223 (reference (a)).

1.4 Provides the guidance, policy framework and key policy principles for networks, computing, information assurance, information management, and network operations -- to

computing, information assurance, information management, and network operations -- to include their interoperability.

2. APPLICABILITY AND SCOPE:

2.1 This guidance and policy applies to:

2.1.1 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 (see enclosure 1), and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.1.2 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 IC Policy.

2.1.3 All DoD acquisitions and procurements of Global Information Grid assets and services, consistent with the provisions of the Clinger-Cohen Act.

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

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

4.1 The Global Information Grid shall support all DoD missions with information technology, for national security systems, joint operations, Joint Task Force, and/or Combined Task Force commands, that offer the most effective and efficient information handling capabilities available, consistent with National Military Strategy, operational requirements and best value enterprise level business practices. (See the Global Information Grid Reference Model, enclosure (2).)

4.2 An enterprise wide inventory of Global Information Grid assets shall be established and maintained.

4.3 The Global Information Grid shall be planned, resourced, acquired, and implemented in accordance with the strategic principles delineated in the DoD Information Management (IM) Strategic Plan (reference (b)).

4.4 Global Information Grid assets shall be interoperable in accordance with approved requirements documents and compliant with the operational, system, and technical views of the Global Information Grid architecture.

4.5 All Global Information Grid assets shall maintain the appropriate levels of confidentiality, integrity, availability, authentication and non-repudiation through the use of information assurance safeguards and operational procedures specified in the Global Information Grid architecture and the Global Information Grid Information Assurance policy.

4.6 All DoD personnel performing Global Information Grid tasks shall be appropriately trained.

4.7 The Global Information Grid shall be based on a common, or enterprise-level, communications and computing architecture to provide a full range of information services at all major security classifications and information handling caveats.

4.8 All applications shall be planned, designed, and implemented to use common Global Information Grid assets. COTS applications shall be in compliance with the Global Information Grid architecture.

4.9 Plans, architectures, designs, hardware and software and supporting organizational resource details shall be available and accessible for the appropriate level of review/management to assure the effective management, engineering, operations, maintenance and sustainment of the Global Information Grid.

4.10 The Global Information Grid shall be implemented, operated and evolved through the acquisition of assets, procurement of services and operational procedures in compliance with the Global Information Grid architecture and approved business case analyses which consider best value. While total cost of ownership will be a factor in this determination, other aspects, such as utility to the warfighter, will be used to determine "best value."

4.11 The Global Information Grid architecture shall represent the Information Technology Architecture required by the Clinger-Cohen Act.

4.12 Global Information Grid operational requirements shall be identified in a manner consistent with the Requirements Generation System defined in reference (f).

4.13 An integrated database of Global Information Grid requirements shall be maintained in such a manner as to allow the aggregation and display of requirements.

4.14 Global Information Grid requirements which include Information Exchange Requirements (IER) and Key Performance Parameters (KPP) for interoperability shall be described in a consistent manner with the overall GIG operations architecture view.

4.15 Major Global Information Grid investment decisions shall be directly linked to the Defense Planning Guidance (DPG) and other recognized statements of DoD missions, goals and outcomes in support of the warfighters, policy makers and support personnel.

4.16 The portfolio of Global Information Grid program investments, corresponding to the computing and communications capabilities defined by the Global Information Grid computing and communications system reference model (see Enclosure 2), shall be reviewed annually to support the synchronization of resources among and within constituent programs via the DoD Planning Programming and Budgeting System (PPBS) and to assure synchronization and integration among programs with interdependencies (e.g., technical, functional, infrastructure, application, configuration management, training, and sustainment).

4.17 The Global Information Grid shall be implemented by the acquisition of assets and procurement of services based on the Global Information Grid architecture and approved business case analyses which consider best value and the benefits of business process reengineering from a DoD enterprise perspective.

4.18 All Global Information Grid acquisitions shall be planned and executed in compliance with DoDD 5000.1 (reference (g)) and DoD 5000.2-R (reference (h)) or other comparable authority officially recognized by the Department of Defense.

4.19 All Global Information Grid acquisitions and procurements, including upgrades or expansions of existing systems and services, shall comply with the Global Information Grid architecture.

4.20 All Global Information Grid acquisition agents shall use enterprise licensing and standard contracts to the maximum extent practical, consistent with the Clinger-Cohen Act. Leases, licenses and service contracts supporting the Global Information Grid shall be reviewed and revalidated annually to ensure requirements still exist.

4.21 Operational assets shall be available and accessible in sufficient detail to ensure architecture standards compliance, information security, operational effectiveness, efficiency and quality of service across the Global Information Grid.

4.22 Performance-based and results-based measures shall be developed for the Global Information Grid. These measures, including those established in Service Level Agreements and operational plans, shall be used to manage the Global Information Grid and provide customer satisfaction feedback.

4.23 Uniform configuration management of Global Information Grid assets will be established in order to ensure interoperability and security across the Global Information Grid.

4 RESPONSIBILITIES:

5.1 The DoD Chief Information Officer shall:

5.1.1 Serve as the Principal Staff Assistant for Information Management.

5.1.2 Develop and issue the DoD Information Management (IM) Strategic Plan and ensure that related strategic plans reflect the Global Information Grid architecture.

5.1.3 Develop, maintain, and enforce compliance with the Global Information Grid architecture, in coordination with the CIO Executive Board and the Architecture Coordination Council as appropriate, and direct the development of associated implementation and transition plans. Provide a Department-wide mission area architecture framework which will be used by DoD Agencies and Components to build Integrated Operational and Systems Architecture views.

5.1.4 Provide recommendations to the JROC for the development of DoD Global Information Grid requirements and direction to the Joint Chiefs of Staff for satisfying non-DoD requirements for Global Information Grid services validated by the Secretary of Defense.

5.1.5 Establish an investment strategy and a process to support the implementation of the Global Information Grid consistent with the operational and functional needs of the DOD and considering Joint and Defense wide priorities.

5.1.6 Establish compliance and enforcement mechanisms to achieve interoperability, information assurance and Global Information Grid program synchronization.

5.1.7 Ensure that Global Information Grid metrics are developed, effectiveness and customer satisfaction are measured and corrective actions are initiated.

5.1.8 Designate enterprise level providers and managers for the Global Information Grid.

5.1.9 Ensure that a managed process is in place to allow Components to certify that Global Information Grid acquisitions and procurements are in compliance with the Global Information Grid architecture.

5.1.10 Ensure that the Global Information Grid is placed under configuration management and that responsibilities for configuration management of Global Information Grid assets are assigned recognizing the importance of Component ownership as well as the need to potentially transcend Component boundaries.

5.1.11 Coordinate DoD liaison activities with other Federal Departments and Agencies, State and Local governments, and Allied Nations on matters regarding the Global Information Grid.

5.1.12 Consult, where appropriate, with comparable Intelligence Community authorities on matters of Global Information Grid policy, implementation and operation.

5.1.13 Develop and maintain a database containing the integrated inventory of Global Information Grid assets.

5.1.14 Develop and maintain an integrated database of aggregated Global Information Grid requirements.

5.1.15 Conduct an annual review of Global Information Grid portfolios as described in paragraph 4.16.

5.2 The OSD Principal Staff Assistants (PSAs), in addition to the responsibilities specified in paragraph 5.7, shall:

5.2.1 Require the use of Global Information Grid common computing and communications assets within their functional areas.

5.2.2 Coordinate with the DoD CIO to ensure that architectures developed to meet the combat support and business needs of the PSA accurately reflect and utilize current and planned common Global Information Grid assets.

5.3 The Under Secretary of Defense for Acquisition, Technology and Logistics, in addition to the responsibilities specified in paragraphs 5.2 and 5.7, shall ensure that acquisition programs and Advanced Concept Technology Demonstrations (ACTD) are planned and executed in compliance with the guidance and policy expressed herein.

5.4 The Under Secretary of Defense, Comptroller, will collaborate with the DoD CIO to, where necessary, identify and coordinate improvements to the identification and portrayal of IT resources in order to improve overall IT visibility.

5.5 The Director, Operational Test and Evaluation (DOT&E) shall ensure that Global Information Grid related operational test and evaluation includes Critical Operational Issues addressing interoperability and information assurance.

5.6 The Chairman of the Joint Chiefs of Staff, in addition to the responsibilities specified in paragraph 5.7, shall:

5.6.1 Ensure that Combatant Commanders identify and require Global Information Grid capabilities in the generation of requirements for support to Joint and Combined operations and that architectures developed to meet the mission area needs of the Combatant Commanders accurately reflect and utilize current and planned common Global Information Grid assets.

5.6.2 Develop Joint doctrine and associated Joint Tactics, Techniques, and Procedures (JTTP) for the Global Information Grid and ensure the compatibility of the Chairman of the Joint Chiefs of Staff Instructions (CJCSI) with Global Information Grid policy and guidance.

5.6.3 Develop the Joint Operational Architecture (JOA) that describes key information elements, information flow, and information exchanges that must occur in support of Combined/Joint Task Force (JTF) operations across all relevant mission areas.

5.7 The Heads of the DoD Components shall:

5.7.1 Populate and maintain their portion of the Global Information Grid asset inventory.

5.7.2 Ensure that Component architectures are developed and maintained in a manner that is consistent with and reflective of the Global Information Grid architecture.

5.7.3 Ensure that all Component subordinate elements coordinate with the Component CIO to ensure that all architectures developed to meet the functional needs of a Component accurately reflect and utilize current and planned common Global Information Grid assets.

5.7.4 Require the use of Global Information Grid common computing and communications assets within their functional areas.

5.7.5 Ensure that Component-managed portions of all Global Information Grid programs are planned, resourced, acquired, and implemented in accordance with the DoD Information Management (IM) Strategic Plan, Global Information Grid architecture and Defense resource priorities.

5.7.6 Ensure that Component acquired, procured or managed Global Information Grid assets are under formal configuration management to the extent necessary to establish and maintain information assurance, quality of service throughout the Global Information Grid over the lifecycle of the asset.

5.7.7 Provide configuration management of assigned Global Information Grid assets and actively support the overall Global Information Grid configuration management process.

5.7.8 Ensure that component-managed portions of the Global Information Grid are secure, assured, and interoperable, in accordance with the operational, system, and technical views of the Global Information Grid architecture.

5.7.9 Ensure that all component personnel performing Global Information Grid tasks are appropriately trained.

5.8 The Director, Defense Information Systems Agency, in addition to the responsibilities specified in paragraph 5.7, shall:

5.8.1 Develop, coordinate and maintain the DoD Joint Technical Architecture in coordination with the CINCs, Services and Agencies and sponsor its approval by the DoD Architecture Coordination Council (ACC).

5.8.2 Coordinate and maintain, in conjunction with the CINCs, Services and Agencies, the Common Operating Environment, for use by Command and Control (C2), Combat Support, Combat Service Support, and Intelligence information systems directly supporting a Joint Task Force (JTF) and Commands.

5.8.3 In conjunction with the CINCs, Services and Agencies, evolve the Common Operating Environment to meet the enterprise-wide requirements as defined by the Global Information Grid architecture.

5.9 The Component Chief Information Officers shall ensure that:

5.9.1 The Component's Information Management Strategic Plan is consistent with the DoD Information Management Strategic Plan.

5.9.2 Component architectures accurately reflect and utilize current and planned common Global Information Grid computing and communications assets.

5.9.3 All Component leased, owned, operated, or managed Global Information Grid systems, services, upgrades or expansions to existing systems or services are acquired or procured in compliance with the Global Information Grid architecture and the relevant Global Information Grid policies.

5.9.4 Component Global Information Grid plans, architectures, designs and assets are available and accessible for effective management and engineering.

5.9.5 Global Information Grid assets assigned to the Component maintain the appropriate levels of confidentiality, integrity, availability, authentication and non-repudiation.

5.9.6 Global Information Grid assets assigned to the Component are operated, maintained, and managed so as to be interoperable in accordance with the operational and system views of the Global Information Grid architecture.

5.9.7 Global Information Grid acquisition programs and procurements, including leases, licenses and service contracts, are reviewed annually in consultation with the DoD CIO to assure requirements currency, continued cross program synchronization and architecture compliance.

5.9.8 Global Information Grid operational effectiveness and customer satisfaction are measured, corrective actions taken and feedback provided to the DoD CIO upon request.

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

Enclosure 1: Definitions

<u>Term</u>	<u>Definition</u>
Acquisition Executive	The individual, within the Department and Components, charged with overall acquisition management responsibilities within his or her respective organizations. The Under Secretary of Defense (Acquisition and Technology (A&T)) is the Defense Acquisition Executive (DAE) responsible for all acquisition matters within the Department of Defense. The Component Acquisition Executives (CAEs) for each of the Components are the Secretaries of the Military Departments or Heads of Agencies with power of redelegation. The CAEs, or designee, are responsible for all acquisition matters within their respective Components. The Department's Chief Information Officer (CIO) is the Department's Acquisition Executive for automated information systems (AISs) and establishes acquisition policies and procedures unique to AISs (DoDD 5000.1, Defense Acquisition).
Architecture	The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time. It is composed of three major perspectives, operational, systems, and technical views. (C4ISR Architecture Framework)
Architecture, Joint Technical	The minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The technical architecture view provides the technical systems-implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The technical architecture view includes a collection of the technical standards, conventions, rules and criteria organized into profile(s) that govern system services, interfaces, and relationships for particular systems architecture views and that relate to particular operational views.
Defense Agencies	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.

End to End	The inclusion of all requisite components to deliver a defined capability. For the GIG, this implies all assets 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 service networks, end-to-end encompasses service user to service user (e.g., PC-to-PC, phone-to-phone). For transport networks, end-to-end encompasses equipment-to-equipment (e.g., Service Delivery Point (SDP)-to-Service Delivery Point (SDP), router-to-router, PBX-to-PBX).
Enterprise	The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities.
Enterprise Network	Designated by the DoD CIO Executive Board as Enterprise Networks because they 1) provide a defined capability, 2) are available to serve multiple DoD components, 3) are consistent with the Global Information Grid architecture, 4) are managed with Enterprise-wide oversight, and 5) provide service to any user with a validated requirement.
Global Information Grid (GIG)	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.
Global Information Grid Architecture (GIGA)	The architecture, composed of interrelated operational, systems and technical views, which defines the characteristics of and relationships among current and planned Global Information Grid assets in support of National Security missions. The Global Information Grid architecture, developed in accordance with the standards defined in the C4ISR Architecture Framework and using the definitions contained within the Global Information Grid Reference Model, incorporates all major organizational relationships, information flows, Enterprise networks, systems configurations and technical standards pertaining to the design, acquisition and operation of the Global Information Grid.

Information Assurance	Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoDD S-3600.1) For purposes of this definition the following meanings apply:
Information Assurance - Authentication	Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. (National Security Telecommunications Information Systems Security Instruction (NSTISSI) 4009)
Information Assurance - Availability	Availability: Timely, reliable access to data and information services for authorized users. (National Security Telecommunications Information Systems Security Instruction (NSTISSI) 4009)
Information Assurance - Confidentiality	Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices. (National Security Telecommunications Information Systems Security Instruction (NSTISSI) 4009)
Information Assurance - Integrity:	Integrity: Protection against unauthorized modification or destruction of information. (National Security Telecommunications Information Systems Security Instruction (NSTISSI) 4009)
Information Assurance - Nonrepudiation	Nonrepudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. (National Security Telecommunications Information Systems Security Instruction (NSTISSI) 4009)
Information Handling Caveat	A phrase (e.g., Special Access Required, Restricted Information, For Official Use Only) that invokes special information management processes and procedures not related to Sensitive Compartmented Information (SCI).
Information Management	The planning, budgeting, manipulating, and controlling of information throughout its life cycle.
Information Superiority	The capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Joint Vision 2010)
Information Technology	Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a Component directly or used by a contractor under a contract with the Component which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and

related resources. Notwithstanding the above, the term does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Intelligence Community Interoperability	The departments, agencies, and activities enumerated in Sec. 3, National Security Act of 1947, as amended, (50 USC 401a). The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. JSC Pub. 1
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.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which- - (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) subject to subsection (b), is critical to the direct fulfillment of military or intelligence missions. Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 10 U.S.C., Section 2315)
Network Operations	Organizations and procedures required to monitor, manage and control the Global Information Grid. Network operations incorporates network management, information dissemination management, and information assurance.
Non-DoD 5000 Series Acquisitions	Acquisitions such as grants, services or Advanced Concept Technology Demonstrations, which are not covered by DoDD 5000.1.

OSD Principal Staff Assistants (PSAs).	The OSD PSAs are the Under Secretaries of Defense (USDs), the Director of Defense Research and Engineering (DDR&E), the Assistant Secretaries of Defense (ASDs), the Director, Operational Test and Evaluation (DOT&E), the General Counsel of the Department of Defense (GC, DoD), the Inspector General of the Department of Defense (IG, DoD), the Assistants to the Secretary of Defense (ATSDs), and the OSD Directors or equivalents, who report directly to the Secretary or the Deputy Secretary of Defense (DoDD 5025).
Service Level Agreement	Any type of management vehicle between a service provider and a customer that specifies performance requirements, measures, reporting, cost, and recourse.
Service Provider	Any type of organization internal or external to DoD who has designated responsibility for the operation of one or more of the GIG computing and communications assets.
Synchronization	Process of aligning program investments, development and implementation schedules to ensure the timely delivery of desired integrated assets.
Wide Area Network (WAN)	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.

The GIG Systems Reference Model

