DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

APR 6 2001

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: DoD Chief Information Officer (CIO) Guidance and Policy Memorandum (G&PM) No. 11-8450, Department of Defense (DoD) Global Information Grid (GIG) Computing

In a memorandum, "Global Information Grid," dated September 22, 1999, the DoD CIO issued guidance on the definition and scope of the 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, and computing.

The attached guidance on GIG Computing is one in a series of GIG policies that provides direction and assigns responsibilities for effective, efficient, and economical acquisition, management, and use of computing services. It is effective immediately.

Improved and timely GIG policies are the cornerstone to enabling change, eliminating outdated ways of doing business, implementing the spirit and intent of the Clinger-Cohen Act and other reform legislation, and achieving our Information Superiority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

Paul Wolfowitz

Attachment
As stated

U15449 /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 (DoD) Global Information Grid (GIG) Computing

References:
(a) DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No.-8001-March 31, 2000-Global Information Grid
(b) Title 10, United States Code
(c) DoD Information Management (IM) Strategic Plan, V2.0, October 1999
(d) DoD C4ISR Architecture Framework, V2.0 December 18, 1997
(e) Division E of the Clinger-Cohen Act of 1996 (CCA), Public Law 104-106, as amended
(f) Chairman Joint Chiefs of Staff Instruction (CJCSI) 3170.01A, Requirements Generation System, August 10, 1999
(g) DCI Directive 1/6, "The Intelligence Community Chief Information Officer," February 4, 2000
(h) DCI Directive 6/3, "Protecting Sensitive Compartmented Information Within Information Systems, " June 5, 1999

1. PURPOSE: This guidance and policy:

1.1. Establishes DoD GIG computing policy and responsibilities under reference (a) to enable the secure storage, processing, exchange and use of information necessary for the execution of the DoD mission.

1.2. Ensures effective, efficient, and economical acquisition, life-cycle management, and use of GIG personal, local, regional and global computing environments. Provides for choices in computing platform (from microcomputer to mid-tier to mainframe to supercomputer) and placement of application and data while managing the diversity of the GIG computing environments.

1.3. Promotes best value Business Case Analyses (BCAs) across GIG computing environments.

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

2.2. All computing assets and services that are administered, managed, acquired, operated or used by the DoD Components (except for those integral to a weapon). Under the GIG Systems Reference Model (Enclosure 2), these computing assets and services fall into four categories: Personal, Local, Regional and Global computing environments. The applications and data, which use these environments, are also included.

2.3. GIG 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.

2.4. This policy applies to computing at all security levels. However it is recognized 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.

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

4. POLICY: It is DoD policy that:

4.1. All GIG computing must be adequately protected and comply with the requirements of the DoD GIG Information Assurance G&PM. GIG computing operations shall ensure continuity of operations consistent with operational needs.

4.2. All GIG computing capabilities (including applications and data) shall comply with the requirements of this computing policy. All GIG computing shall comply with the GIG Architecture.

4.3. Computing operations shall be consolidated to a limited number of computing centers based on mission requirements, operational effectiveness, and cost efficiencies.

4.4. All computing environments (i.e., local, personal, regional and global) shall:

4.4.1. Be planned, designed, and implemented to maximize the use of standard GIG configurations where necessary for interoperability and information assurance.

4.4.2. Implement best practices in human systems integration, human factors engineering and user accessibility in the requirements analysis, design and implementation phase.

4.5. All applications shall be planned, designed, and implemented to maximize the use of common GIG computing environments.

4.6. Global and functional area applications or associated data that are common to more than one operational location shall utilize a designated regional or global computing provider or obtain a waiver. The Defense Information Systems Agency (DISA) is designated as the global/regional computing service provider for mainframe and cross-Component computing. Other regional/global computing service providers for cross-Component computing may be designated at the discretion of the DoD CIO.

4.7. Best value BCAs and performance assessments shall be conducted to determine computing strategy (e.g., the optimal choice of computing platform, placement of applications and associated data on personal, local, regional, and global environments, and computing service provider).

4.8. GIG computing service providers shall be chosen on a competitive best value basis, including consideration of mission requirements and Circular A-76.

4.9. Each DoD installation shall have a single GIG computing point of contact for coordinating personal and local computing and communications activities.

4.10. Service Level Agreements (SLAs) (or equivalent) shall be established between the using organizations and computing service providers.

4.11. Inventories of all hardware and software installed on GIG computing environments shall be created and maintained.

4.12. A process shall be established to collect and make available metrics (including historical trends) of GIG computing environment performance to users, customers, and operations managers.

4.13. DoD Command and Control (C2), Combat Support, Combat Service Support, and Intelligence capabilities supporting the Joint Task Force (JTF) and CINCs shall meet the Defense Information Infrastructure Common Operating Environment (DII COE) minimum level of compliance as specified by the DoD CIO, with a recommendation from DISA, the Joint Staff, and affected organizations. All other capabilities shall use DII COE components to the maximum extent necessary to meet DoD portability and security requirements and enable information interoperability.

4.14. When DoD Components outsource a functional process or acquire management information (e.g., the acquired product is information or the leasing of an application), the selected non-DoD entity will normally be responsible for providing the computing infrastructure necessary for performance. These computing infrastructures must comply with all requirements for this policy related to achieving needed interoperability and for protecting DoD information.

5. RESPONSIBILITIES

5.1. The DoD Chief Information Officer (CIO) shall:

5.1.1. Ensure, with the support of Components, that all DoD computing capabilities (including applications and data) comply with the requirements of this policy.

5.1.2. Develop, maintain and enforce the GIG Architecture. Ensure the GIG architecture responds to DoD's planned acquisition of functional applications, accommodates commercial standards, and facilitates the overall sufficiency and efficiency of GIG computing capabilities.

5.1.3. Ensure appropriate level of consolidation for cross-Component and mainframe computing. Approve Component plans for consolidating Component-specific computing operations. Ensure opportunities for consolidating across two or more Components are identified and implemented as appropriate (in accordance with DoD CIO responsibilities defined in Chapter 131 of Reference (b)).

5.1.4. Select, evaluate, and accredit designated regional and global computing service providers for mainframe and cross-Component processing; monitor their performance; and grant waivers to their use. Arbitrate issues regarding non-performance of SLAs for designated computing service providers.

5.1.5. Establish standard GIG configurations where necessary for interoperability and information assurance. Such configurations must consider mission requirements, operational effectiveness, and cost efficiencies.

5.1.6. Establish processes for:

5.1.6.1. Selecting (and deselecting), evaluating, and accrediting designated regional and global computing service providers, monitoring their performance, and granting waivers.

5.1.6.2. Creating and maintaining inventories of all current and planned GIG computing assets.

5.1.6.3. Collecting and making available metrics on GIG computing performance.

5.1.7. Establish further guidance on:

5.1.7.1. Developing and evaluating best value BCAs with OSD/PA&E.

5.1.7.2. Developing and using SLAs.

5.1.7.3. Roles/responsibilities of computing service providers (including performance measurements).

5.1.8. Identify the minimum DII COE compliance level (per paragraph 4.13).

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

5.1.10. Develop a process to dynamically determine infrastructure requirements based on planned mission area applications.

5.2. The Heads of DoD Components shall:

5.2.1. Ensure that all Component-specific computing capabilities (including applications and data) comply with the requirements of this policy and the GIG Architecture.

5.2.2. Ensure that all acquisition agents provide a best value BCA and performance assessment to determine the optimal choice of computing platforms, placement of applications and associated data on personal, local, regional, and global computing environments, and evaluation of alternative computing service providers.

5.2.3. Review annually the Component IT investment strategies for alignment of priorities and synchronization of Component computing programs with the GIG Architecture.

5.2.4. Ensure elimination of unnecessary duplicate computing environments.

5.2.5. Implement the process to collect and make available metrics (including historical trends) on GIG computing environment performance.

5.3. The Component CIOs shall:

5.3.1. Oversee the acquisition of GIG computing assets and the selection and monitoring of computing service providers for the Component. This includes:

5.3.1.1. Establishing a process for selecting, evaluating and accrediting personal and local computing service providers, including specific performance measurements, use of SLAs, and arbitration of issues regarding non-performance of SLAs.

5.3.1.2. Designating regional/global computing service providers for Component-specific processing; monitor their performance and SLAs; grant waivers to their use in accordance with DoD-developed process (per paragraph 5.1.6) and arbitrate issues regarding non-performance of SLAs for designated computing service providers.

5.3.1.3. Ensuring that available standard GIG configurations are used for personal, local, regional and global computing environments. Ensure DII COE compliance as established by the DoD CIO (per paragraphs 4.13 and 5.1.8).

5.3.2. Plan and oversee consolidation of Component-specific computing operations.

5.3.3. Create and maintain inventories of current and planned personal, local, regional, and global computing assets and applications (IAW paragraph 5.1.6).

5.3.4. Ensure that each Component-hosted installation has a designated GIG computing point of contact for coordination of personal and local computing and communications activities.

5.3.5. Report to DoD CIO, as requested, on status of implementing this G&PM.

5.4. The Director, DISA, in addition to responsibilities described above, shall:

5.4.1. Evolve, integrate, and maintain a robust DII COE capability focused on CINCs/JTFs.

5.4.2. Establish a GIG common operating environment for the broader enterprise focused on the minimal essential capabilities needed to enable secure information interoperability across DoD.

5.4.3. Be the designated mainframe computing service provider and designated computing service provider for cross-Component global/regional computing services.

5.4.4. As a designated computing service provider, ensure that SLAs (or equivalent) are defined with the users and met; provide performance metrics information to the DoD CIO and customers; and ensure all computing services comply with this G&PM.

5.5. The IC CIO, on behalf of the DCI pursuant to references (g) and (h), has agreed to perform the following functions:

5.5.1. Co-designate, with the DoD CIO, a select set of computing capabilities and services, 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.

Enclosure 1: DEFINITION OF TERMS

E 1.1 Business Case Analysis (BCA) is the evaluation of alternative solutions that includes the ability to meet the defined requirements (e.g.. technical, functional. training, implementation, operational, and scheduling), total cost of delivery and sustainment, operational performance considerations. and associated risks. While total cost of ownership will be a factor in this analysis, other aspects, such as utility to the warfighter, will be used to determine "best value."

E 1.2 Component-Specific Computing are application and/or data processing services used only within one Component.

E 1.3 Consolidation includes three types of computing realignments—logical, physical and rationalized consolidations. In logical consolidation, the hardware remains distributed; however, there is a more centralized, standardized configuration and systems management. Physical consolidation also includes the actual physical relocation of computer platforms to fewer locations. In rationalized consolidation, the number of physically consolidated computing platforms are reduced by rehosting and/or use of new platforms.

E 1.4 Cross-Component Computing are common application and/or data processing services provided to users from more than one Component. This includes Joint and Defense-wide applications and their processing.

E 1.5 Defense Agencies and Offices are 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 Contract Management 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, and National Security Agency.

E 1.6 Defense Information Infrastructure Common Operating Environment (DII COE) is a multi-faceted approach for enhancing software and data reuse and interoperability. The concept includes a mission application-independent architecture, a collection of reusable software, a software infrastructure and a set of guidelines and standards. It is implemented with a set of modular software that provides generic functions or services such as operating-system services. These services or functions are accessed by other software (e.g., global or functional area application) through standard Application Programming Interfaces.

E 1.7 End User Devices are user computers including desktop and laptops, thin clients, high-end workstations, personal digital assistants, telephones, and pagers.

E 1.8 Functional Process in the context of this policy refers to the set of functions associated with combat support (in the case of the Navy and Air Force) and/or combat service support (in the case of the Army).

E 1.9 GIG Architecture is composed of interrelated operational, systems, and technical views, defines the characteristics of, and relationships among, current and planned GIG assets in support of national security missions. The GIG Architecture, developed in accordance with the standards defined in the C4ISR Architecture Framework and using the definitions contained within the GIG Systems 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 GIG. (GIG G&PM 8-8001)

E 1.10 Global /Regional Computing Service Provider is any type of organization, internal or external to DoD, who has designated responsibility for the operation of global and /or regional computing services.

E 1.11 Global Computing Center is an operations facility (e.g., Defense Mega Center) supporting global computing environments of required types of platforms providing centralized computing services for the enterprise.

E 1.12 Global Computing Environment is a computing capability that supports centralized application or data processing for the enterprise.

E 1.13 Global Information Grid (GIG) is :

(A) 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.

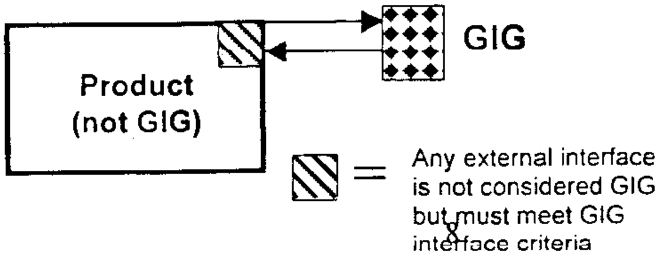
(B) Includes any system, equipment, software, or service that meets one or more of the following criteria:

(1) Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software and services (see para (C) below with respect to embedded information technology).

(2) Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software and services

(3) Processes data or information for use by other equipment, software and services

(C) The embedded information technology within a product is not considered part of the GIG; however, if it provides the functionality described in (B) above, it must meet GIG interface criteria. See sketch below:



E 1.14 **Global Information Grid Computing Point of Contact** is the focal point on a military or civilian installation that is responsible for coordinating the connectivity of the end user devices, local servers and local networks.

E 1.15 **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 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 Systems Reference Model.

E 1.16 **Information Technology** means 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 if the equipment is used directly or is used by a contractor under a contract which (i) requires the use of such equipment, or (ii) requires the use of such equipment in the performance of a service or the furnishing of a product. This includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (Division E of Clinger-Cohen Act of 1996)

E 1.17 **Installation** is a grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base. (Joint Pub 1-02)

E 1.18 **Local Computing Environment** is a combination of local servers, shared peripherals, local networks, user productivity tools, and associated software available at a given work site, which may be fixed, mobile, or deployable.

E 1.19 **Mainframe computing** is any processing done by large-scale, multi-tasking computers that (1) serve large numbers of concurrent on-line users and/or (2) execute batch applications. These machines generally operate on raised computer room floors and require controlled environmental conditions. (OMB Bulletin 96-02).

E 1.20 **National Security Systems** means any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions (but not a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications)).

E 1.21 **Personal and Local Computing Service Providers** is any type of organization, internal or external to DoD, who has designated responsibility for the operation of personal and/or local computing services.

E 1.22 **Personal Computing Environment** is a combination of end user devices, peripherals, user productivity tools, and associated software available at a personal work location, which may be fixed, mobile, or deployable.

E 1.23 **Regional Computing Center** is an operations facility supporting regional computing environments of required types of platforms providing computing services to a regional operating area.

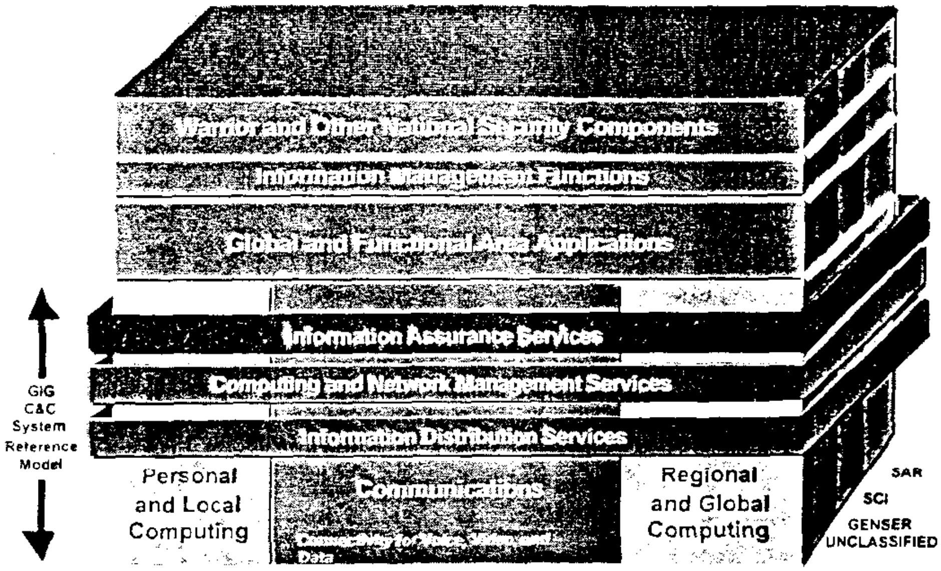
E 1.24 **Regional Computing Environment** is a computing capability that supports regionally centralized application or data processing and includes the following types of servers: application, web, database, document, video, mail, and print.

E 1.25 **Service Level Agreement** is any type of management vehicle between a service provider and a customer that specifies performance requirements, measures, reporting, cost, and recourse.

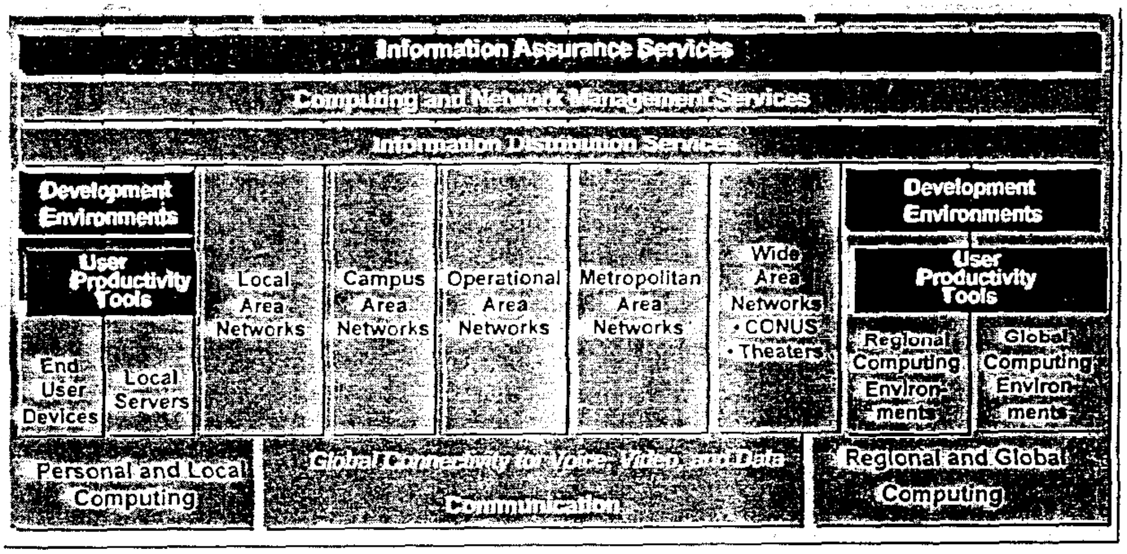
E 1.26 **Service Provider** is any type of organization, internal or external to DoD, who has designated responsibility for the operation of one or more components of the GIG Communications and Computing System Reference Model. In the case of this policy, this includes global, regional, local, and personal computing service providers.

E 1.27 **Standard Configuration** is a template providing an interoperable and secure design of technology components within the overall GIG Computing and Communications System Reference Model. These design templates may include elements of hardware and software (excluding applications systems) in addition to standards.

Enclosure 2: Global Information Grid Systems Reference Model


Warrior and Other National Security Components
Information Management Functions
Global and Functional Area Applications
Information Assurance Services
Computing and Network Management Services
Information Distribution Services
GIG C&C System Reference Model
Personal and Local Computing
Communications
Connectivity for Voice, Video and Data
Regional and Global Computing
SAR
SCI
GENSER
UNCLASSIFIED

Top Level Global Information Grid Systems Reference Model


Information Assurance Services
Computing and Network Management Services
Information Distribution Services
Development Environments
User Productivity Tools
End User Devices
Local Servers
Local Area Networks
Campus Area Networks
Operational Area Networks
Metropolitan Area Networks
Wide Area Networks
• CONUS
• Theaters
Development Environments
User Productivity Tools
Regional Computing Environments
Global Computing Environments
Personal and Local Computing
Global Connectivity for Voice, Video, and Data Communication
Regional and Global Computing

Global Information Grid Computing & Communications (C&C) Systems Reference Model