



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



AUG 24 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. 7-8170-082400 - Global Information Grid
Information Management

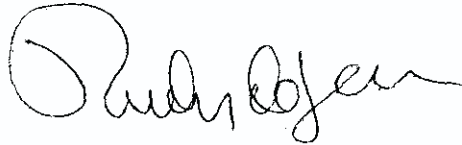
In a memorandum, "Global Information Grid," dated September 22, 1999, the DoD CIO issued guidance on the definition and scope of the Global Information Grid (GIG). In essence, the GIG is "a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting,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

U10705 /00

The attached guidance establishes DoD policies and assigns responsibilities to improve the accessibility, availability, dissemination, and use of information. Its focus is on the information itself, and the management activities associated with the creation, dissemination, and use of information.

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, 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. In conjunction with this effort, the DoD CIO will publish high-level procedural guidance regarding the implementation of key aspects of this policy.

A handwritten signature in black ink, appearing to read "Rudy de Leon". The signature is fluid and cursive, with a large initial "R" and a long, sweeping underline.

Rudy de Leon

Attachment
As stated

**Guidance and Policy
for
Department of Defense (DoD)
Global Information Grid (GIG)
Information Management (IM)**

- References:
- (a) Title 10, Section 2223, United States Code
 - (b) The Clinger-Cohen Act of 1996, as amended (Division E of P.L. 104-106)
 - (c) DoD Directive 8000.1, "Defense Information (IM) Program," October 27, 1992
 - (d) "DoD Information Management (IM) Strategic Plan," Version 2.0, October 1999
 - (e) DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001-March 31, 2000-Global Information Grid, dated March 31, 2000"
 - (f) through (m), see enclosure 1

1. PURPOSE:

This guidance and policy establishes Department of Defense (DoD) policy and assigns responsibilities to improve the accessibility, availability, dissemination, use and disposition of information necessary to execute the DoD mission. It:

1.1. Implements the authorities of the DoD Chief Information Officer (CIO) and Military Department CIOs established in references (a) and (b).

1.2. Interprets and supplements guidance on the management of information as a resource contained in references (c), (d), and (e).

1.3. Continues the integration of Information Management (IM) policies associated with the Global Information Grid (GIG) into operational priorities presented in reference (f).

1.4. Recognizes the unique requirements for Records Management contained in references (g) and (h), and the correlation of these to the effective implementation of other aspects of GIG information management.

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 Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies and Offices (see Enclosure 2), the DoD Field Activities, and all other DoD organizations (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. The management of information that satisfies the definition of a record as defined in reference (g), and as managed in accordance with reference (h).

3. DEFINITIONS:

Terms used in this issuance are defined in enclosure 2.

4. POLICY:

It is DoD policy that:

4.1. Information requirements associated with the GIG shall be identified, documented, and validated by information users (hereinafter referred to as information consumers), and understood and acted upon by information creators and compilers (hereinafter referred to as information producers). Accordingly:

4.1.1. Information requirements shall be described through approved architectures and documented in appropriate operational and strategic plans, and be consistent with the DoD IM Strategic Plan and other strategic doctrine such as Joint Vision 2020.

4.1.2. Information requirements shall be established through the use of DoD standard content and format (profiles) mechanisms or ad hoc requests for information based on validated mission needs.

4.1.3. The Requirements Generation System (reference (i)) shall be used to identify long-term information requirements against which capital planning, programming, and investment decisions are made.

4.1.4. Information requirements that may require an investment in information technology shall conform to the requirements validation and approval processes established in reference (i).

4.2. Consumers shall be enabled to easily discover, retrieve, and manage the flow of information based upon its characteristics as advertised by producers, in conformance with security requirements, and consistent with organizational priorities. Accordingly:

4.2.1. Information producers shall advertise information availability and accessibility using DoD standard meta-data, data schema, and producer profiling mechanisms to facilitate consumer research and requests for information.

4.2.2. Information awareness, access and delivery shall be facilitated through the use of common mechanisms such as producer profiles and source registries. These mechanisms shall include permanently attached attributes, such as authority, classification, and handling restrictions that enforce effective access and delivery, and minimize the risk of improper use of information.

4.2.3. Authoritative information repositories shall be established, and organizations shall be identified and authorized to create, compile, distribute, and dispose of data and meta-data in these repositories in accordance with applicable industry, Federal and DoD standards.

4.2.4. Information producers shall make information available at the lowest possible security level to ensure the greatest possible use of the information.

4.3. Mechanisms for access and delivery shall be implemented that: are interoperable; adhere to the views of the GIG architecture and other industry, Federal, and DoD standards, as applicable; provide adequate access control; and ensure that the required information is easily accessed and delivered consistent with security requirements. In this regard:

4.3.1. Information access and delivery mechanisms and procedures shall follow DoD Information Assurance and security policies and procedures, as well as other regulations requiring the special handling of certain types of information.

4.3.2. Information requirements shall be satisfied from advertised information over GIG network assets to ensure DoD quality of service and information assurance requirements are met.

4.3.3. Enterprise-wide mechanisms for information access and delivery priorities shall be established, to the maximum extent practicable.

4.3.4. Access and delivery mechanisms shall support rapidly changing operational needs. Consumer profiles, and access and delivery priorities shall be able to accommodate changing environments.

4.3.5. Access and delivery mechanisms shall enable timely information collaboration between consumers and producers and across functional communities, consistent with consumer requirements.

4.4. Processes and methods shall be used to facilitate the proper understanding and use of information. Accordingly:

4.4.1. Interoperable tools that are consistent with DoD approved standards (e.g., Joint Technical Architecture (reference (j))) shall be used and maintained to facilitate the discovery, dissemination, and use of information throughout its life-cycle.

4.4.2. Information management processes shall be monitored and re-engineered, as justified, to ensure common and effective understanding of delivered information.

4.4.3. Following functional activity process improvement or re-engineering DoD-wide automated applications shall be used, where practicable and cost effective.

4.5. Performance measures, associated metrics, and reporting processes shall be established for information dissemination management against which mission performance will be evaluated, and deficiencies remedied.

4.6. Information contained in records shall be viewed as a critical resource that provides an authoritative source of valid information for current and future operations, plans, exercises and resourcing.

4.7. Information contained in records shall be preserved, maintained, protected, and disposed of in accordance with applicable records regulations.

5. RESPONSIBILITIES:

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

5.1.1. Consistent with reference(k), ensure improvements to DoD work processes and supportive information management resources, in coordination with the OSD Principal Staff Assistants.

5.1.2. Establish and enforce standards for meta-data, data schema, and data and records management that enable effective and efficient information management.

5.1.3. Ensure that common and interoperable information mechanisms and standards are established.

5.1.4. Establish DoD information management priorities based on architectures, and the DoD IM Strategic Plan and other plans that directly affect the DoD progress toward achieving its Information Superiority goal.

5.1.5. Refine the information management business process and establish process improvement methods (e.g., Benchmarking, COTS solutions, Business Case, Unit Costing, and tracking of lessons learned) to evaluate DoD information management.

5.1.6. Provide for an environment that supports improvements in the awareness, access, delivery, and understanding of appropriate information across security boundaries, including the information needs of Allied and Coalition partners.

5.1.7. Establish common protocols, standards and guidelines for producers regarding information quality, replication, and integrity to support all operational uses and minimize the risk of misuse of the information.

5.1.8. Ensure information management awareness, training, and educational opportunities are made available to personnel to effectively manage and implement, and strengthen IM activities.

5.1.9. Consult, where appropriate, with the OSD Principal Staff Assistants and the IC CIO on matters of GIG policy, acquisition, implementation, and operation.

5.2. The Chairman of the Joint Chiefs of Staff shall:

5.2.1. Establish joint procedures for the development, coordination, review, and approval of joint information requirements.

5.2.2. Establish joint policies and procedures for control of information access and delivery including prioritization, precedence and preemption.

5.2.3. Develop, approve, and issue joint doctrinal concepts and associated operational procedures and guidance to ensure the satisfaction of mission essential information requirements of U.S. military forces and, as applicable, with coalition and allied forces.

5.3 The OSD Principal Staff Assistants (PSAs) shall improve operations and procedures for managing information in their functional area; improve their business processes, as needed; and ensure compliance with and implementation of the policies contained herein.

5.4. The Heads of the DoD Components shall:

5.4.1. Establish procedures for the development, coordination, review, prioritization and approval of information requirements in their mission areas.

5.4.2. Ensure that information requirements are documented validated, and funded in accordance with DoD policy, including approved architecture processes and frameworks.

5.4.3. Specify IM requirements and standards in the design, acquisition, installation, and operation of information systems and infrastructure.

5.4.4. Perform assessments on the satisfaction of their information requirements.

5.4.5. Ensure IM awareness, training, and educational opportunities are made available to personnel to effectively manage and implement IM functions

5.4.6. Establish, implement, and enforce IM policies and procedures for their Component consistent with this policy. These policies shall include guidance for information producers, information consumers, and records managers such that:

5.4.6.1. Information producers identify information attributes based on standards; justify need; establish authoritative repositories of information in accordance with mission and functional responsibilities; advertise information holdings and provide responsive service to validated information requirements; and commit records created to the Component's records management system.

5.4.6.2 Records managers review and ensure that records are in compliance with applicable DoD regulations and guidance.

5.4.6.3 Information consumers document and validate information requirements in accordance with standards and procedures developed under this policy; and handle information provided in accordance with attributes assigned by the information producer.

5.4.7 Plan, budget, and execute adequate resources in support of information management.

5.5. The Intelligence Community Chief Information Officer (CIO), on behalf of the DCI pursuant to reference (l) and (m), 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 guidance and policy is effective immediately.

Enclosure 1: References

- (f) Joint Vision 2020, "America's Military: Preparing for Tomorrow," May 30, 2000
- (g) Title 44, Section 3301, United States Code
- (h) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000
- (i) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01A, "Requirements Generation System," August 10, 1999
- (j) DoD Joint Technical Architecture (JTA),, Version 3.0, November 29, 1999
- (k) Secretary of Defense Memorandum, Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106), June 2, 1997
- (l) DCI Directive 1/6, "The Intelligence Community Chief Information Officer," February 4, 2000
- (m) DCI Directive 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," June 5, 1999

Enclosure 2: Definitions

- E2.1 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.
- E2.2 Access and Delivery Mechanisms:** Hardware, software, IT standards, and processes that enable information to be readily located, accessed, and delivered in a secure manner, in the right format, when and where needed. They provide for the processing of information in common ways to meet common uses; for the search, retrieval, filtering, summarization, and mining of information from existing holdings; for the dissemination of information as it is created; and for the delivery and integrity of information. These mechanisms help to manage "information overload."
- E2.3 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 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.
- E2.4 Enterprise:** The Office of the Secretary of Defense, the Military Departments and their respective Services, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies and Offices, the DoD Field Activities, and all other DoD organizations.
- E2.5 Global Information Grid:** 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.

- E2.6 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.
- E2.7 Information:** Any communications or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms
- E2.8 Information Consumer:** A person, group organization, system, or process that accesses and receives information enabling the execution of authorized missions and functions.
- E2.9 Information Dissemination Management:** A set of integrated applications, processes, and services that provide the capability for producers and consumers to locate, retrieve, and send/receive information by the most effective and efficient means, and in a manner consistent with policy guidance and priorities.
- E2.10 Information Life-Cycle:** The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.
- E2.11 Information Management:** The planning, budgeting, manipulating, and controlling of information throughout its life cycle.
- E2.12 Information Producer:** A person, group, organization, system, or process that creates, compiles, updates, distributes, and retires information based on their authorized/assigned missions and functions.

- E2.13 Information Profile:** The expression of the requirement for or availability of data, information, or reports enabling the execution of authorized/assigned missions and functions.
- E2.14 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.
- E2.15 Meta-data:** Information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings.
- E2.16 OSD Principal Staff Assistants (PSA):** 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 of the Deputy Secretary of Defense.
- E2.17 Record:** Records include all books, papers, maps, photographs, machine-readable materials, and other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included (See 44 U.S.C. 3301).