Department of Defense

DIRECTIVE

NUMBER 8100.1

September 19, 2002

Certified Current as of November 21, 2003

ASD(C3I)

SUBJECT: Global Information Grid (GIG) Overarching Policy

References: (a) Section 2223 of title 10, United States Code
(b) Section 1401 et seq. of title 40, United States Code
(c) Secretary of Defense Memorandum, "Implementation of Subdivision E of the Clinger-Cohen Act of 1996," June 2, 1997
(d) DoD Directive 7045.14, "Planning, Programming, and Budgeting System (PPBS)," May 22, 1984
(e) through (k), see enclosure 1

1. PURPOSE

This Directive:

1.1. Implements references (a) and (b).

1.2. Establishes policy and assigns responsibilities under reference (c) for GIG configuration management, architecture, and the relationships with the Intelligence Community (IC) and defense intelligence components.

2. APPLICABILITY AND SCOPE

This Directive 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 Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field

Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.2. Information technology (IT) and its operation by the DoD intelligence agencies, the Service intelligence elements and the other intelligence activities engaged in direct support of Defense missions. GIG implementation must comply with policy and responsibilities established in sections 4. and 5., below, and, wherever applicable, separate and coordinated Director of Central Intelligence directives and IC policy.

2.3. All DoD acquisitions and procurements of GIG assets and services, consistent with 10 U.S.C. 2223, 40 U.S.C. 1401 et seq., and Secretary of Defense Memorandum (references (a) through (c)).

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. The GIG shall support all DoD missions with information technology, for national security systems, joint operations, joint task force (JTF), and/or combined-task force commands, that offers the most effective, efficient, and assured information handling capabilities available, consistent with national military strategy, operational requirements, and best-value enterprise-level business practices.

4.2. The GIG shall be planned, resourced, acquired, and implemented in accordance with the DoD Directives System 5000 series for DoD issuances; DoD Directive 7045.14 (reference (d)), and planning, programming, and budgeting system (PPBS). The Department of Defense's Information Management Strategic Plan (reference (e)), as updated and reissued, shall implement GIG policy.

4.3. GIG assets shall be interoperable, in accordance with approved requirements documents, and compliant with the operational, system, and technical views (reference (f)) of the GIG architecture (reference (g)).

4.4. The GIG 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 consistent with NSTISSP No. 11 (reference (h)).

4.5. GIG plans, architectures, designs, hardware, software, and supporting organizational resource details shall be available and accessible for the applicable level of review to ensure the appropriate security and effective management, engineering, operations, maintenance, and sustainment of the GIG.

4.6. Reference (g) shall be the sound and integrated information technology architecture required by section 5125(b)(2) of the Clinger-Cohen Act of 1996 (reference (b)).

4.7. Major GIG investment decisions shall be in accordance with the Defense Planning Guidance, the GIG Capstone Requirements Document (CRD) (reference i)), and other recognized statements of DoD missions, goals, and outcomes in support of the warfighters, policy makers, and support personnel.

4.8. GIG program investments, corresponding to the computing and communications capabilities defined by reference (g), shall be reviewed annually to support the synchronization of resources among and in constituent programs through the DoD PPBS and to ensure synchronization and integration among programs with interdependencies (e.g., technical, functional, infrastructure, application, configuration management, training, and sustainment).

4.9. An enterprise-wide inventory of GIG assets shall be established and maintained.

4.10. All applications shall be planned, designed, and implemented to use common GIG assets to the extent defined by reference (g).

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, as the DoD Chief Information Officer, shall:

5.1.1. Annually update and reissue the "DoD Information Management (IM) Strategic Plan" (reference (e)) and ensure that related strategic plans reflect reference (g).

5.1.2. Develop, maintain, and enforce compliance with reference (g), in consultation with the DoD Chief Information Officer (DoD CIO) Executive Board; the Under Secretary of Defense (Acquisition, Technology and Logistics) (USD (AT&L));

and the Joint Staff, Director J-6, as applicable, and direct the development of associated implementation and transition plans.

5.1.3. In consultation with the Joint Staff and the USD(AT&L), provide a DoD-wide mission area architecture framework that shall be used by the DoD Components to build integrated operational, technical, and systems architecture views. Ensure that the operational views are integrated across Joint Mission Areas.

5.1.4. Provide recommendations to the Joint Requirements Oversight Council for the development of DoD GIG requirements. Provide direction to the Joint Chiefs of Staff for satisfying non-DoD GIG requirements validated by the Secretary of Defense.

5.1.5. Establish GIG compliance and enforcement mechanisms to achieve IT and National Security Systems (NSS) interoperability and information assurance, while minimizing needless duplication of IT and NSS.

5.1.6. Develop Information Assurance standards and conventions in support of the GIG in coordination with the National Institute of Standards and Technology (NIST).

5.1.7. The Director, Defense Information Systems Agency, under the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), besides the responsibilities specified in paragraph 5.7., below, shall:

5.1.7.1. Develop, coordinate, and maintain the DoD Joint Technical Architecture (reference (j)) in coordination with the OSD Principal Staff Assistants (PSAs), Combatant Commands, Military Departments, Defense Agencies, Defense Field Activities, and the Joint Staff, Director, J-6.

5.1.7.2. Coordinate and maintain, in consultation with the Combatant Commands, the Military Departments, the Defense Agencies, and the Defense Field Activities, the Common Operating Environment, for use by command and control, combat support, combat service support, and intelligence information systems directly supporting a JTF and the Combatant Commands.

5.1.7.3. In consultation with the Joint Staff, the Combatant Commands, the Military Departments, the Defense Agencies, and the Defense Field Activities, evolve the Common Operating Environment to meet the enterprise-wide requirements as defined by reference (g) and the GIG CRD.

5.2. The OSD Principal Staff Assistants, besides the responsibilities in paragraph 5.7., below, shall 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 GIG assets.

5.3. The Under Secretary of Defense for Acquisition, Technology and Logistics, besides the responsibilities specified in paragraphs 5.2., above, and 5.7., below, shall ensure that acquisition programs fully consider documented GIG requirements and architecture in the development of C4I Support Plans as well as at all acquisition milestones and for advanced concept technology demonstrations in the management and transition plans.

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

5.5. The Director, Operational Test and Evaluation shall ensure that GIG-related operational test and evaluation addresses all critical operational issues, including interoperability and information assurance.

5.6. The Chairman of the Joint Chiefs of Staff, besides the responsibilities specified in paragraph 5.7., below, shall:

5.6.1. Ensure that the Commanders of the Combatant Commands identify GIG 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 Commands accurately reflect and utilize current and planned common GIG assets. Combatant Command requirements and architectures shall be included in the DoD Component and DoD IM strategic plans.

5.6.2. Develop joint doctrine and associated joint tactics, techniques, and procedures for the GIG and ensure the compatibility of the Chairman of the Joint Chiefs of Staff Instructions with GIG policy and guidance.

5.6.3. Develop the Joint Operational Architecture that describes key information elements, information flow, and information exchanges that shall occur in support of combined and/or 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 GIG asset inventory.

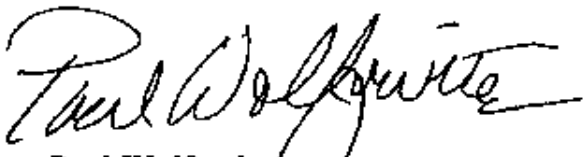
5.7.2. Ensure that the DoD Component architectures are developed and maintained consistent with the GIG architecture.

5.7.3. Require the use of GIG common computing and communications assets within their functional areas and within their Component.

5.7.4. Ensure all Component-leased, -owned, -operated, or -managed GIG systems, services, upgrades, or expansions to existing systems or services are acquired or procured in compliance with reference (g).

6. EFFECTIVE DATE

This Directive is effective immediately.



Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 2
E1. References, continued
E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Information Management (IM) Strategic Plan, Version 2.0,[1] October 1999
(f) C4ISR Architecture Framework, Version 2.0,[2] December 18, 1997
(g) Global Information Grid Architecture,[3] current version
(h) NSTISSP No. 11,[4] "National Policy Governing Information Assurance and Information Assurance Enabled Information Technology Products," January 2000
(i) Global Information Grid Capstone Requirements Document,[5] JROCM 134-01, August 30, 2001
(j) DoD Joint Technical Architecture (JTA),[6] current version
(k) Joint Vision 2020,[7] "Future Warfare," June 2000

---

[1] Copies may be obtained via Internet at http://www.c3i.osd.mil/org/cio/ciolinks/references/itmstpln/itmstpln-memo.html

[2] Copies may be obtained via Internet at http://www.c3i.osd.mil/org/cio/i3/AWG_Digital_Library/index.htm

[3] This CD-ROM may be obtained from the DoD Office of the Chief Information Officer, Architecture & Interoperability Directorate (703) 607-0233.

[4] Not releasable to the public.

[5] Copies may be obtained via Internet at http://www.dsc.osd.mil/gig/GIG_Arch_v1.0_(Final)/GIG_CRD_(Final).pdf

[6] Copies may be obtained via Internet at http://www-jta.itsi.disa.mil/

[7] Copies may be obtained via Internet at http://www.dtic.mil/jv2020/

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Global Information Grid (GIG)

E2.1.1.1. 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 (reference (b)). 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.

E2.1.1.2. Includes any system, equipment, software, or service that meets one or more of the following criteria:

E2.1.1.2.1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

E2.1.1.2.2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

E2.1.1.2.3. Processes data or information for use by other equipment, software, or services.

E2.1.1.3. Non-GIG IT. Stand-alone, self-contained, or embedded IT that is not and will not be connected to the enterprise network.

E2.1.2. 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. (See Joint Vision 2020, reference (k).)

E2.1.3. Information Technology (IT). 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 that:

E2.1.3.1. Requires the use of such equipment; or

E2.1.3.2. 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. (See Section 1401 et seq. of title 40, United States Code, reference (b).)