Department of Defense
DIRECTIVE

NUMBER 8000.01
February 10, 2009

ASD(NII)/DoD CIO

SUBJECT: Management of the Department of Defense Information Enterprise

References: See Enclosure 1

1. PURPOSE. This Directive:

a. Reissues and renames DoD Directive (DoDD) 8000.01 (Reference (a)), and assigns oversight responsibilities for DoD information management activities to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO), consistent with DoDD 5144.1 (Reference (b)).

b. Implements sections 2223 and 2224 of title 10, United States Code (U.S.C.) (Reference (c)); Chapter 113 of title 40, U.S.C. (Reference (d)); Chapters 35 and 36 of title 44, U.S.C. (Reference (e)); and Office of Management and Budget Circular A-130 (Reference (f)) by establishing and reissuing policies for the management of the Department of Defense Information Enterprise.

c. Provides direction on creating an information advantage for DoD personnel and mission partners, and establishing and defining roles for CIOs at various levels within the Department of Defense consistent with References (c), (d), and (e).

d. Provides direction for information sharing among all DoD Components and with mission partners, consistent with the National Strategy for Information Sharing (Reference (g)).

e. Cancels DoDD 8100.01 (Reference (h)).

2. APPLICABILITY. This Directive applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint 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 within the Department of Defense (hereafter referred to collectively as the “DoD Components”).

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. Information shall be considered a strategic asset to the Department of Defense; it shall be appropriately secured, shared, and made available throughout the information life cycle to any DoD user or mission partner to the maximum extent allowed by law and DoD policy.

b. Functional processes shall be simplified or otherwise redesigned to improve effectiveness and reduce cost before, or in conjunction with, making significant investments in information technology.

c. Each DoD Component shall have a CIO who reports directly to the Head of the Component. CIOs may also be designated at subordinate levels, but a reporting mechanism through the Component CIO must be maintained to ensure continuity of purpose.

d. Information solutions shall provide reliable, timely, accurate information that is protected, secure, and resilient against information warfare, terrorism, criminal activities, natural disasters, and accidents consistent with Reference (e).

e. All aspects of the Department of Defense Information Enterprise, including the Global Information Grid (GIG) infrastructure and enterprise services and solutions, shall be planned, designed, developed, configured, acquired, managed, operated, and protected to achieve a net-centric environment, as envisioned in the National Defense Strategy of the United States of America (Reference (i)), capable of effectively and efficiently supporting the Department's outcome goals and priorities.

f. The DoD Enterprise Architecture, which is consistent with Reference (f) and composed of DoD enterprise and Component levels, shall be maintained and applied to guide investment portfolio strategies and decisions, define capability and interoperability requirements, establish and enforce standards, guide security and information assurance requirements across the Department of Defense, and provide a sound basis for transition from the existing environment to the future.

g. Investments in information solutions shall be managed through a capital planning and investment control process that:

(1) Is performance- and results-based.

(2) Provides for analyzing, selecting, controlling, and evaluating investments, as well as assessing and managing associated risks.

(3) Interfaces with the DoD key decision support systems for capability identification; planning, programming, budgeting, and execution; and acquisition.

(4) Requires the review of all information technology (IT) investments for compliance with architectures, IT standards, and related policy requirements.

h. Consistent with DoDD 5000.01 (Reference (j)) and DoDI 5000.02 (Reference (k)), acquisition strategies shall appropriately allocate risk between the Government and contractor; effectively use competition; tie contract payments to performance; and, where practicable, take maximum advantage of commercial off-the-shelf and non-developmental item technology. Information solutions shall be structured into useful segments that are as narrow in scope and brief in duration as practical; each segment shall solve a specific part of an overall mission problem and deliver a measurable net benefit independent of future segments.

i. Pilots, modeling and simulation, experimentation, and prototype projects shall be encouraged, especially when large, high-risk investments in information solutions are involved. However, these projects shall be appropriately sized to achieve desired objectives, and shall not be used in lieu of testing or acquisition processes to implement the production version of the information solution.

j. A well-trained core of highly qualified information management, information technology, and information assurance professionals shall be developed who can accept, anticipate, and generate the changes that the evolution of the Department of Defense Information Enterprise will enable in net-centric operations. The entire DoD workforce will similarly need to be trained and ready to take advantage of the Department of Defense Information Enterprise.

k. Disabled DoD employees or members of the public seeking information or services from the Department of Defense shall have access to and use of information and data comparable to the access and use by individuals who are not disabled, unless an undue burden would be imposed, to the extent required by section 794d of title 29, U.S.C. (Reference (l)).

5. RESPONSIBILITIES. See Enclosure 2.

6. RELEASABILITY. UNLIMITED. This Directive is approved for public release and is available on the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This Directive is effective immediately.

Gordon England
Deputy Secretary of Defense

Enclosures

ENCLOSURE 1

REFERENCES

(a) DoDD 8000.01, "Management of DoD Information Resources and Information Technology," February 27, 2002 (hereby canceled)
(b) DoDD 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
(c) Sections 2223 and 2224 of title 10, U.S.C.
(d) Sections 11101 and 11316, and Chapter 113 of title 40, U.S.C.
(e) Chapters 35 and 36 of title 44, U.S.C.
(f) Office of Management and Budget Circular A-130, "Management of Federal Information Resources," November 28, 2000
(g) National Strategy for Information Sharing, October 2007[1]
(h) DoDD 8100.01, "Global Information Grid (GIG) Overarching Policy," September 19, 2002 (hereby canceled)
(i) The National Defense Strategy of the United States of America, September 2002[2]
(j) DoDD 5000.01, "The Defense Acquisition System," May 12, 2003
(k) DoDI 5000.02, "Operation of the Defense Acquisition System," December 8, 2008
(l) Section 794d of title 29, U.S.C. (Section 508 of the Rehabilitation Act of 1973, as amended)

[1] http://www.whitehouse.gov/nsc/infosharing/index.html
[2] http://www.whitehouse.gov/nsc/nss.pdf

ENCLOSURE 2

RESPONSIBILITIES

1. ASD(NII)/DoD CIO. The ASD(NII)/DoD CIO shall:

a. Lead the Department of Defense Information Enterprise:

(1) Exercise responsibilities as described in Reference (b).

(2) Serve as the DoD senior official for information resources management matters related to References (c), (d), (e), and (f).

(3) Report to and advise the Secretary and Deputy Secretary of Defense on the information resources implications of strategic planning decisions.

(4) Develop and maintain a strategic plan that describes how information resources management activities help accomplish the DoD mission, in accordance with Reference (e).

b. Provide standards for developing, maintaining, and implementing a DoD Enterprise Architecture. Establish mechanisms to ensure compliance with these standards.

c. Ensure information policy and functional requirements are reflected in architectures and plans across the DoD enterprise and Component levels as a means to ensure information sharing, visibility, assurance, and interoperability.

d. Ensure the integration and synchronization of the Department of Defense Information Enterprise activities.

e. Establish mechanisms to facilitate organizationally-tiered compliance reviews for all IT investments to ensure they comply with all enterprise architectures, IT standards and related policy requirements; and act as the oversight authority for IT compliance.

2. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE (USD(C)/CFO). The USD(C)/CFO shall, pursuant to section 11316 of Reference (d) and in coordination with the ASD(NII)/DoD CIO and the Under Secretary of Defense for Acquisition, Technology, and Logistics, establish policies and procedures to ensure that accounting, financial, and asset management systems and other related DoD information solutions are designed, developed, maintained, and used effectively to provide financial data reliably, consistently, and expeditiously, and support programmatic investment decisions.

3. HEADS OF THE OSD COMPONENTS AND CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Heads of the OSD Components and Chairman of the Joint Chiefs of Staff, according to their responsibility and authority for assigned functional areas, including supporting information resources, shall:

a. Improve DoD operations and procedures by ensuring the application of sound business practices and compliance with this Directive.

b. Exercise oversight for the evaluation and improvement of functional processes before making significant investments in information technology:

(1) Determine whether the function that IT will support is central to, or a priority for, the Department's mission.

(2) Determine whether the private sector or another Government agency can perform the function more effectively or at less cost.

(3) Outsource non-core and non-inherently governmental functions to another Government agency or the private sector when it makes good business sense to do so.

(4) Benchmark functional area processes against models of excellence in other Government agencies or the private sector to develop, reengineer, simplify, or otherwise improve functional processes when the decision is made to retain the function in-house.

c. Participate in the OSD acquisition oversight process for major automated information systems and ensure functional leadership, management, and control of these systems throughout their life cycles.

d. Ensure information policy and functional requirements are reflected in architectures and plans across the DoD enterprise and Component levels as a means to ensure information sharing, visibility, assurance, and interoperability.

4. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. In addition to the responsibilities in paragraphs 3 and 5 of this enclosure, the Chairman of the Joint Chiefs of Staff shall appoint a Joint Community CIO.

5. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Appoint a DoD Component CIO who shall have core knowledge, skills, abilities, and experiences to carry out the requirements of References (c), (d), (e), and (f).

b. Clearly delineate the DoD Component CIO's role, responsibilities, and authority vis-à-vis those of the DoD Component Comptroller, the DoD Component Acquisition Executive or a similar position, functional area managers, and subordinate-level CIOs.

c. Take advantage of the opportunities that information management and IT can provide and ensure that the IT infrastructure will support enterprise, mission, functional, and Component strategies by positioning the DoD Component CIO to participate in that Component's strategic planning process.

d. Promote and forge a strong partnership among the Component's CIO and Comptroller, DoD Component Acquisition Executive or similar position, as well as other key senior managers and external mission partners when making and executing Component strategic decisions.

e. Designate, or authorize the designation of, subordinate-level CIOs, as needed, and ensure that the subordinate CIOs have a reporting mechanism through the Component CIO.

f. Ensure that the Component's IT investment portfolio aligns with the Department of Defense Information Enterprise policies and guidance, as required.

6. DoD COMPONENT CIOs. The DoD Component CIOs shall:

a. Have responsibilities and authorities as delegated in this Directive. Military Department CIOs shall have additional responsibilities as defined in Reference (c).

b. Head an office responsible for ensuring that the Component complies with, and promptly, efficiently, and effectively implements the policies and responsibilities in this Directive and the requirements of References (c), (d), (e), and (f).

c. Provide advice and other assistance to the Component Head and other Component senior management personnel to ensure that information resources are acquired, used, and managed by the Component according to References (c), (d), (e), and (f).

d. Participate in ASD(NII)/DoD CIO-led forums for governing the Department of Defense Information Enterprise.

e. Advise the ASD(NII)/DoD CIO and ensure that the policies and guidance issued by the ASD(NII)/DoD CIO are implemented; and contribute to the DoD strategic information resources management plan.

f. Establish programs to hire, train, and retain the information management, IT, and information assurance workforce consistent with this Directive.

g. Ensure information policy and functional requirements are reflected in architectures and plans across the DoD enterprise and Component levels as a means to ensure information sharing, visibility, assurance, and interoperability.

h. Conduct organizationally-tiered reviews within their respective Components to ensure IT investments are in compliance with architectures at various levels, IT standards, and related policy requirements; and act as the Component's oversight authority for IT compliance.

GLOSSARY

Department of Defense Information Enterprise. The DoD information resources, assets, and processes required to achieve an information advantage and share information across the Department of Defense and with mission partners. It includes: (a) the information itself and the Department's management over the information life cycle; (b) the processes, including risk management, associated with managing information to accomplish the DoD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and IT, including national security systems.

DoD enterprise-level. Relating to policy, guidance, or other overarching leadership provided by OSD Officials and the Chairman of the Joint Chiefs of Staff in exercising authority, direction, and control of their respective elements of the Department of Defense on behalf of the Secretary of Defense.

DoD Enterprise Architecture. A federation of descriptions that provide context and rules for accomplishing the mission of the Department. These descriptions are developed and maintained at the Department, Capability Area, and Component levels and collectively define the people, processes, and technology required in the "current" and "target" environments; and the roadmap for transition to the target environment.

enterprise services. A common set of information resource capabilities designed to provide awareness of, access to, and delivery of information.

enterprise solution. The action of solving a problem or satisfying a requirement that affects the entire organization (e.g., Department of Defense).

GIG. The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

information advantage. The superior position or condition derived from the ability to securely access, share, and collaborate via trusted information while exploiting or denying an adversary's ability to do the same.

information life cycle. The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

information technology. Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

mission partners. Those with whom the Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector.

National Security System. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which

involves intelligence activities;

involves cryptologic activities related to national security;

involves command and control of military forces;

involves 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 does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

net-centric. Relating to or representing the attributes of a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data are shared timely and seamlessly among users, applications, and platforms.