DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAR 22 2004

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Information Technology Portfolio Management

Attachment establishes DoD policies and assigns responsibilities for managing information technology (IT) investments as portfolios. Decisions on what IT investments to make, modify or terminate shall be based on architectures, risk tolerance levels, potential returns, outcome goals and performance. While the guidance specifically addresses IT portfolios and a process for making tradeoffs among IT projects, the IT portfolio is part of the Department's broader portfolio of investments. In this larger context, tradeoffs will have to be made between IT and non-IT investments in other agency processes.

This guidance applies to the six Joint Warfighting Capability Assessment areas (i.e., Battlespace Awareness, Command and Control, Force Application, Protection, Focused Logistics, and Net Centricity), the six Business Domains (i.e., Accounting and Finance, Acquisition, Human Resources Management, Installations and Environment, Logistics, and Strategic Planning and Budgeting), and the underlying Enterprise Information Environment. Improved and timely IT investment policies are a cornerstone to enable change throughout the Department, assure that we have the right IT capabilities to perform our mission and conduct effective information operations, eliminate outdated ways of doing business, and achieve our net-centricity goals. While the attached policy is effective immediately, to ensure that this policy is institutionalized, I ask that the DoD Chief Information Officer, in coordination with the Director, Administration and Management, incorporate it into the DoD Directive System within 180 days.

Paul Wolfowitz

Attachment:
As stated

Department of Defense

ASD(NII)/DoD CIO

SUBJECT: Information Technology Portfolio Management

References: (a) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," Revised, (Transmittal Memorandum No. 4), November 28, 2000
(b) DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," March 20, 2002
(c) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(d) Chairman of the Joint Chiefs of Staff Instruction 3170.01, "Joint Capabilities Integration and Development System," June 24, 2003
(e) DoD Directive 5000.1, The Defense Acquisition System," May 12, 2003
(f) DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), January 11, 2002

1. PURPOSE

This document:

1.1. Consistent with references (a) and (b) and (c), establishes policies and assigns responsibilities for the management of DoD information technology (IT) and associated investments as portfolios.

1.2. Provides fundamental concepts for managing a portfolio of IT investments that focus on improving business and warfighting outcomes and capabilities.

2. APPLICABILITY AND SCOPE

2.1. This document applies to:

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

2.1.2. Joint Warfighting Capability Assessment areas, Business Domains, and the underlying Enterprise Information Environment.

2.1.3. All current and planned IT resources that enable the achievement of Enterprise outcome goals.

3. DEFINITIONS

Terms used in this document are defined in enclosure 1.

4. POLICY

It is DoD policy that:

4.1. Information technology (IT) investments shall be managed as portfolios. Decisions on what IT investments to make, modify or terminate shall be based on the Global Information Grid (GIG) Integrated Architecture, mission area goals, architectures, risk tolerance levels, potential returns, outcome goals and performance.

4.2. Portfolios shall be managed using integrated strategic planning, integrated architectures, measures of performance, risk management techniques, transition plans, and portfolio investments strategies.

4.3. Portfolio management processes shall be established and comprised of the following core activities:

4.3.1. Analysis that links Mission Area goals to DoD Enterprise vision, goals, objectives, priorities, capabilities, as well as how these will be achieved and measured; identifies gaps and opportunities; identifies risks and how these will be mitigated; provides for continuous process improvement; and determines strategic direction for mission area activities and processes.

4.3.2. Selection that identifies the best mix of IT investments to achieve outcome goals and plans as well as transition to "to-be" architectures.

4.3.3. Control that ensures a portfolio and individual projects in the portfolio are acquired in accordance with cost, schedule, performance and risk baselines and documented technical criteria, and remain consistent with the current approved version of the GIG Integrated Architecture.

4.3.4. Evaluation that routinely and systematically assesses and measures actual contributions of the portfolio as well as supports adjustments to the mix of portfolio projects, as necessary.

4.4. Integrated Architectures with Enterprise-, Mission Area-, Domain and DoD Component-level perspectives shall be developed, maintained and applied to gain a better understanding of the organization, and the capability gaps between the current and future environments (warfighting and business); assess process improvement opportunities within and across the levels; determine

interoperability and capability requirements; promote standards; identify and implement information assurance requirements; formulate and target investments to improve data and information management; and identify the required capabilities of the technical infrastructure.

4.5. Portfolios shall be nested and integrated at the Enterprise, Mission Area, Domain and DoD Component levels and shall be based on the principles of centralized guidance and oversight, stakeholder participation, collaborative decision making, and decentralized execution.

4.6. Portfolio management processes shall leverage each of the Department's principal decision support systems (i.e., the Joint Capabilities Integration and Development System (reference (d)); Planning, Programming, Budgeting and Execution process; and Defense Acquisition System (reference (e)).

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration, as the DoD Chief Information Officer (DoD CIO), shall:

5.1.1. Establish a process for maximizing the value and assessing and managing the risks of DoD IT investments, consistent with this policy and reference (b).

5.1.2. In coordination with the OSD Principal Staff Assistants, and the Chairman of the Joint Chiefs of Staff, issue procedures for the policies contained herein. This shall include a core set of uniformly applied criteria for portfolio selection and evaluation.

5.1.3. Ensure that integrated architectures (warfighting and business), and their component parts, comply with the GIG Integrated Architecture (reference (c)).

5.1.4. Develop and maintain the DoD Information Resources Management Strategic Plan.

5.1.5. Provide for the enterprise information environment and ensure that its capabilities are synchronized with requirements for these capabilities. This shall include providing for a common set of Enterprise capabilities that enable users (consumers and providers) to discover, access, post, process, advertise, retrieve and fuse data, and make sense of data gathered.

5.1.6. Establish and co-chair, with other senior officials, executive-level governance forums that provide strategic direction, identify opportunities and resolve cross-functional issues that are in the best interest of the Enterprise.

5.2. The Under Secretary of Defense (Comptroller)/Chief Financial Officer shall:

5.2.1. Establish policies and procedures to ensure that accounting, financial and asset management, and other related DoD IT business systems are designed, developed, maintained, and

used effectively by the DoD Components to provide financial data reliably, consistently and expeditiously, and support programmatic IT investment decisions, consistent with this policy and reference (b).

5.2.2. In coordination with the DoD CIO and the Principal Staff Assistants, develop and maintain the DoD Business Enterprise Architecture (BEA) and associated Business Enterprise Transition Plan as a component of the GIG Integrated Architecture.

5.2.3. Identify and manage the resolution of cross-cutting issues, facilitate future BEA development, and review budgets and make recommendations to ensure that funds are budgeted to implement the portfolio of BEA projects.

5.2.4. Establish and co-chair, with the DoD CIO, executive-level governance forums that provide strategic direction, identify opportunities and resolve cross-functional issues affecting the business community.

5.3. The Under Secretary of Defense for Acquisition, Technology and Logistics shall ensure policies and procedures contained herein are effectively implemented, consistent with this policy and references (b) and (e).

5.4. The OSD Principal Staff Assistants shall, according to their responsibility and authority for assigned business areas:

5.4.1. Designate Business Domains, in coordination with the DoD CIO and the USD(C)/CFO, and ensure that the following tasks are executed consistent with business enterprise guidance and direction:

5.4.1.1. Establish a repeatable IT portfolio management process, including governance structure(s), consistent with the policies contained herein. This process shall include the core activities described in paragraph 4.3 above, and shall be communicated widely and cascaded down to the DoD Components so that they can understand expectations and effectively participate in the process.

5.4.1.2. Participate in business enterprise governance forums aimed at identifying opportunities for commonality in portfolio management techniques, and providing solutions to problems that are in the best interest of the Enterprise.

5.4.2. In coordination with the DoD CIO, issue policies and procedures that implement the policies contained herein.

5.5. The Director of Program Analysis and Evaluation shall review and issue programming and budgeting guidance that reflects (warfighting and business) portfolio recommendations to continue, modify, terminate or initiate funding for IT projects/programs to ensure compliance with the GIG Integrated Architecture and associated applications.

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

5.6.1. Perform warfighting mission area control and oversight of supporting information systems, and ensure warfighting mission area leadership throughout the systems' life-cycle phases, consistent with this policy and reference (b).

5.6.2. In coordination with the DoD CIO, issue policies and procedures that implement the policies contained herein, and participate in warfighting enterprise governance forums aimed at identifying opportunities for commonality in portfolio management techniques and providing solutions to problems that are in the best interest of the Enterprise.

5.7. The Heads of the DoD Components shall, as appropriate, execute the tasks described in Paragraphs 5.4 and 5.6 above.

5.8. The DoD Component Chief Information Officers shall 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 DoD Component consistent with the policies contained herein.

6. EFFECTIVE DATE: This document is effective immediately.

E1. ENCLOSURE 1

DEFINITIONS

E1.1.1. Enterprise Information Environment: The common, integrated computing and communications environment of the Global Information Grid. The GIG EIE is composed of GIG assets that operate as or that assure local area networks, campus area networks, tactical networks, operational area networks, metropolitan area networks and wide area networks. The GIG EIE is also composed of GIG assets that operate as or that assure end user devices, work stations and servers that provide local, organizational, regional or global computing capabilities. The GIG EIE includes all software associated with the operation of EIE assets and the development environments and user productivity tools used in the GIG. The GIG EIE includes a common set of Enterprise and mission specific services, called GIG Enterprise Services, which provide awareness of, access to and delivery of information on the GIG.

E1.1.2. Global Information Grid Integrated Architecture. The DoD-wide enterprise architecture that depicts warfighting and business domains.

E1.1.3. Information Resources. Information and related resources, such as personnel, equipment, funds, and information technology.

E1.1.4. Information Resources Management. The process of managing information resources to accomplish Agency missions and improve Agency performance, including through the reduction of information collection burdens on the public.

E1.1.5. 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 DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that (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 "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It also includes National Security Systems as defined in reference (b). Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

E1.1.6. Integrated Architecture. An architecture consisting of multiple views or perspectives (operational view, system view, and technical view) that facilitates integration and promotes interoperability across Family-Of-Systems / System-of Systems and compatibility among related mission area architectures (ref (f)).

E1.1.7. Mission Area: A defined area of responsibility whose functions and processes contribute to accomplishment of the mission.