Department of Defense
DIRECTIVE

NUMBER 5101.7

May 21, 2004

DA&M

SUBJECT: DoD Executive Agent for Information Technology Standards

References: (a) Assistant Secretary of Defense for Command, Control,
Communications, and Intelligence Memorandum, "Executive Agent for
DoD Information Standards," September 3, 1991 (hereby canceled)
(b) Section 2223 of title 10, United States Code
(c) DoD Directive 5101.1, "DoD Executive Agent," September 3, 2002
(d) DoD Directive 4630.5, "Interoperability and Supportability of
Information Technology (IT) and National Security Systems (NSS),"
May 5, 2004
(e) through (n), see enclosure 1

1. PURPOSE

This Directive:

1.1. Supersedes reference (a).

1.2. Assigns responsibilities and authorities to fulfill Department of Defense
(DoD) Chief Information Officer (CIO) responsibilities, pursuant to reference (b), for
developing, prescribing, and implementing Information Technology (IT), including
National Security Systems (NSS), standards that apply throughout the Department of
Defense.

1.3. Designates, pursuant to reference (c), the Director, Defense Information
Systems Agency (DISA) as the DoD Executive Agent for IT Standards to implement
references (b) and (d), as well as DoD Instruction 4630.8 (reference (e)).

1

2. APPLICABILITY

This Directive applies to 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 collectively referred to as the "DoD Components").

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. MISSION

The DoD Executive Agent for IT Standards shall, in coordination with the Heads of the DoD Components, identify and propose IT standards that apply throughout the Department of Defense. To fulfill this mission, the DoD Executive Agent for IT Standards shall develop and execute a clear standards management strategy and identify focused actions to achieve interoperable and net-centric enabled IT and NSS.

5. POLICY

It is DoD policy that:

5.1. Uniform IT standards shall be used throughout the Department in a manner that achieves and enhances interoperable and net-centric enabled IT and NSS.

5.2. Inter-Service support agreements in accordance with DoD Instruction 4000.19 (reference (f)), Memoranda of Understanding, and other necessary arrangements, as required, may be used to fulfill assigned responsibilities, functions, and authorities delineated in this Directive and DoD Directive 5101.1 (reference (c)).

5.3. Cooperation and support shall be provided to the DoD Executive Agent for IT Standards in a manner that ensures the effective and efficient use of resources and facilitates the mission of the DoD Executive Agent for IT Standards.

6. RESPONSIBILITIES

6.1. The Director, Defense Information Systems Agency is hereby designated as the DoD Executive Agent for Information Technology Standards and in that role shall:

6.1.1. Ensure, consistent with the provisions of references (b), (d), (e), Sections 2451 and 2452 of title 10 (reference (g)), DoD Instruction 4120.24 (reference (h)), and DoD 4120.24-M (reference (i)), that administrative and resource support is timely and fully adequate for accomplishing the mission assigned to the DoD Executive Agent for IT Standards.

6.1.2. Develop, for the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) approval, and with the Heads of the DoD Components, a standards management strategy and program plan, which implements the requirements of references (b), (d), and (e) and promotes the importance of IT standards in achieving interoperable IT and NSS, net-centric capabilities, and achieving decision superiority in support of net-centric operations.   This strategy shall address:

6.1.2.1. IT standards management organization and required resources;

6.1.2.2. IT standards identification, coordination, implementation, and configuration control processes; and

6.1.2.3. Procedures for posting approved IT standards.

6.1.3. Plan, program, and allocate resources as necessary to fulfill DoD Executive Agent for IT Standards roles and responsibilities, including the annual update of planning documents.

6.1.4. Prepare, implement, and maintain IT standards management and program plans. These plans shall be updated annually and submitted to the ASD(NII)/DoD CIO for approval.

6.1.5. Establish and provide access to a single DISA focal point, reporting to the ASD(NII)/DoD CIO, responsible for identifying, proposing, and posting IT standards.

6.1.6. Identify, with the Heads of the DoD Components, forward-looking IT standards (either commercial or non-governmental, or military standards, if required) to facilitate the implementation of net-centric concepts and capabilities.

6.1.7. Lead, with the Heads of the DoD Components and the Defense Standardization Program (DSP) Office, DoD IT standards efforts within the DSP in accordance with references (h) and (i).

6.1.8. Track, coordinate, and integrate all DoD IT standards activities. Participate in commercial, Federal Government, and DoD IT standards forums, as well as North Atlantic Treaty Organization (NATO), allied, and coalition standards bodies.

6.1.9. Facilitate the commercialization of DoD IT requirements by influencing the development of commercial standards through participation in commercial standards bodies. Serve as the primary IT standards representative and liaison on behalf of the Department of Defense within allied and coalition bodies, activities, and related standard forums internationally.

6.1.10. Promote adoption of selected non-Government (national and international) standards as Federal standards, in coordination with the National Institute of Standards and Technology (NIST). Manage the process for coordinating DoD positions on IT standards with the NIST and other Federal Agencies. Facilitate the harmonization and consolidation of IT standards agreements and Memoranda of Understanding/Memoranda of Agreement on behalf of the Department of Defense for the purpose of nation-to-nation and multinational systems interoperability. Encourage the use of Government-Off-The-Shelf, Non-Developmental Items, and Commercial-Off-The-Shelf products wherever possible in accordance with reference (e).

6.1.11. Develop, with the Heads of the DoD Components, IT military standards under DISA's purview only when non-Government standards or Federal standards fail to meet DoD requirements. The DoD Executive Agent for IT Standards shall conduct validation testing on all standards for which they are the Standards Development Organization or Standards Setting Organization.

6.1.12. Maintain the DoD IT Standards Registry (DISR) consisting of approved IT standards and standards profiles to aid program and project managers, acquisition authorities, and systems and technical architects in the development and fielding of interoperable and net-centric enabled systems and products. Establish process and procedures for life-cycle configuration management of IT standards contained in the DISR. Provide on-line Non-Classified IP Router Network and Secret IP Router Network access to the DISR.

6.1.13. Facilitate the use of IT standards by identifying and proposing the appropriate set of standards and associated standards profiles (e.g., Global Information Grid (GIG) Key Interface Profiles (KIPs)) to be used throughout the Department of Defense. The technical architecture view of the GIG Architecture shall also specify appropriate standards and standards profiles for use within the Department of Defense.

6.1.14. Assist in the development of a set of IT standards profiles that shall facilitate DoD Components, joint, allied, and coalition experimentation with new and innovative net-centric enabled concepts and capabilities.

6.1.15. Chair and provide staff and administrative support to the IT Standards Committee for identification, cross-functional integration, and technical collaboration of IT standards.

6.2. The Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer shall:

6.2.1. Prescribe IT standards that apply throughout the Department of Defense pursuant to reference (b).

6.2.2. Maintain this Directive, in coordination with the Heads of the DoD Components, to codify the policies and responsibilities necessary for identifying, adopting, and implementing IT standards that apply throughout the Department of Defense.

6.2.3. Serve as the OSD Principal Staff Assistant (PSA) responsible for oversight and direction of the DoD Executive Agent for IT Standards.

6.2.4. Require the Director, DISA to allocate sufficient resources to fulfill responsibilities as DoD Executive Agent for IT Standards.

6.2.5. Establish a governance structure for identifying, prescribing, and implementing IT standards that apply throughout the Department of Defense and shall establish an IT Standards Oversight Panel (ISOP), consisting of senior DoD representatives, to provide direction, oversight, priorities, and issue resolution for IT standards matters.

6.2.6. Serve, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Chairman of the Joint Chiefs of Staff, as the final resolution authority for DoD IT standards issues. The CIO Executive Board, Military Communications-Electronics Board (MCEB), and the ISOP shall provide recommendations to the DoD CIO for resolution of IT standards issues.

6.3. The <u>Under Secretary of Defense for Acquisition, Technology, and Logistics</u> shall:

6.3.1. Prescribe policies and procedures for implementing the Defense Standardization Program per references (g), (h), and (i).

6.3.2. Coordinate, with the ASD(NII)/DoD CIO and the DoD Executive Agent for IT Standards, on IT standards matters consistent with references (b), (d), (e), (g), (h), and (i).

6.3.3. Ensure, with the ASD (NII)/DoD CIO, that IT standards identified and proposed by the DoD Executive Agent for IT Standards adhere to Office of Management and Budget Circular No. A-119 (reference (j)) requirements and DoD standards reform policy.

6.4. The <u>Under Secretary of Defense (Comptroller)/Chief Financial Officer</u> shall, in accordance with reference (c):

6.4.1. Ensure that the budget submissions are integrated into the DoD Planning, Programming, Budgeting, and Execution process.

6.4.2. Ensure that all funds and costs required to support the DoD Executive Agent for IT Standards are included in appropriate budged exhibit submissions.

6.5. The <u>Director of Administration and Management</u> shall review this Directive pursuant to reference (c), in coordination with the ASD(NII)/DoD CIO, 3 years after signature. Unless a compelling requirement exists, the responsibilities of this DoD Executive Agent arrangement shall be incorporated into the organizational directive for the DISA at that time or shall be allowed to expire if the requirement no longer exists.

6.6. The <u>Heads of the DoD Components</u> shall:

6.6.1. Require program managers for IT and NSS acquisitions and procurements include a standards profile and a summary list of all systems interfaces in the Information Support Plan (ISP). ISPs (containing these standards profiles) for

Acquisition Category (ACAT) I, II, and III programs shall be forwarded to the Chairman of the Joint Chiefs of Staff for validation and verification. ISPs for non-ACAT programs shall be approved by the Milestone Decision Authority or cognizant fielding activity.

6.6.2. Enforce implementation of approved DoD IT standards.

6.6.3. Submit change requests to add, remove, replace, or update IT Standards contained in the DISR to the DoD Executive Agent for IT Standards.

6.6.4. Include DISA-approved standards conformance testing events and procedures in interoperability test plans.

6.6.5. Participate in DoD efforts to influence development of commercial, Federal Government, and DoD, as well as NATO, allied, and coalition IT standards.

6.6.6. Participate in configuration management of IT interfaces (system, technical, and GIG KIPs) and interface standards.

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

6.7.1. Validate and certify IT standards compliance in requirements and capabilities documents.

6.7.2. Establish, with the DoD Executive Agent for IT Standards, processes and procedures for joint interoperability certification testing to evaluate conformance with DoD-approved IT standards.

6.7.3. Provide an assessment of sufficiency of IT standards to meet military requirements.

6.7.4. Provide the ASD(NII)/DoD CIO with military priorities for development and selection of IT standards.

6.7.5. Consider, pursuant to DoD Directive 5100.35 (reference (k)), military communications-electronics matters, including those associated with NSS, as defined in Chapter 25 of title 40, United States Code (reference (l)), referred to it by the Secretary of Defense, the ASD(NII)/DoD CIO, and other DoD Components through the MCEB.

6.7.5.1. Coordinate IT standards issues presented to the MCEB among the DoD Components, between the Department of Defense and other Government

Departments and Agencies, and between the Department of Defense and representatives of foreign nations.

6.7.5.2. Coordinate with the Heads of the DoD Components to resolve IT standards conformance issues. If resolution of IT standards issues cannot be achieved within the MCEB process, the MCEB shall refer it to the ASD(NII)/DoD CIO for review.

6.8. Nothing herein shall be interpreted to subsume or replace the functions, responsibilities, or authorities of the OSD PSAs or the Heads of the DoD Components, as prescribed by law or DoD guidance.

7. RELATIONSHIPS

7.1. In performing assigned responsibilities, the DoD Executive Agent for IT Standards is subject to the authority, direction, and control of the Secretary of Defense through the ASD(NII)/DoD CIO. The Secretary of Defense shall normally communicate to the DoD Executive Agent for IT Standards through the ASD(NII)/DoD CIO.

7.2. The DoD Executive Agent for IT Standards shall maintain close communications with the Heads of the DoD Components and OSD PSAs regarding IT standards. Matters pertaining to IT standards shall be coordinated, as appropriate, with these officials to ensure their needs are met.

8. AUTHORITIES

The DoD Executive Agent for IT Standards is hereby delegated authority to:

8.1. Obtain reports, information, advice, and assistance consistent with DoD Directive 8910.1 (reference (m)), as necessary, in carrying out assigned functions.

8.2. Communicate directly with the Heads of the DoD Components, as necessary, to carry out assigned functions, to include the transmission of requests for advice and assistance. Communications to the Military Departments shall be transmitted through the Secretaries of the Military Departments, their designees, or as otherwise provided in law or directed by the Secretary of Defense in other DoD issuances. Communications to the Combatant Commanders, except in unusual circumstances, shall be transmitted through the Chairman of the Joint Chiefs of Staff.
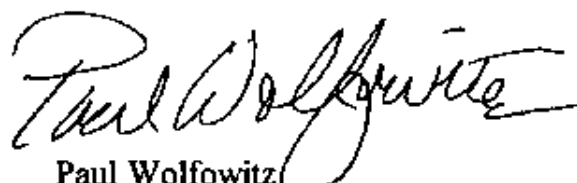
8.3. Communicate with other Government officials, representatives of the Legislative Branch, members of the public, and representatives of foreign governments, as appropriate, in carrying out assigned functions.

8.4. Develop, coordinate, and issue DoD manuals, regulations, or guidebooks, pursuant to DoD Directive 5025.1 (reference (n)) in carrying out assigned functions.

9. <u>EFFECTIVE DATE</u>

This Directive is effective immediately and remains in effect until 3 years after signature.

Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 2
　　E1. Reference, continued
　　E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of
    Information Technology (IT) and National Security Systems (NSS)," May 2, 2002

(f) DoD Instruction 4000.19, "Interservice and Intergovernmental Support,"
    August 9, 1995

(g) Section 2451 and 2452 of title 10, United States Code

(h) DoD Instruction 4120.24, "Defense Standardization Program (DSP)," June 18, 1998

(i) DoD 4120.24-M, "Defense Standardization Program (DSP) Policies and
    Procedures," March 9, 2000

(j) Office of Management and Budget Circular No. A-119, February 10, 1998

(k) DoD Directive 5100.35, "Military Communications-Electronics Board (MCEB),"
    March 10, 1998

(l) Chapter 25 of title 40, United States Code

(m) DoD Directive 8910.1, "Management and Control of Information Requirements,"
    June 11, 1993

(n) DoD Directive 5025.1, "DoD Directives System," July 27, 2000

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Global Information Grid (GIG) Key Interface Profiles (KIPs). GIG KIPs provide a net-centric oriented approach for managing interoperability across the GIG based on the configuration control of key interfaces. The KIP is the set of documentation produced as a result of interface analysis that: designates an interface as key; analyzes it to understand its architectural, interoperability, test, and configuration management characteristics; and documents those characteristics in conjunction with solution sets for issues identified during the analysis. GIG KIPs provide a description of required operational functionality, systems functionality, and technical specifications for the interface. The profile consists of refined operational and systems view products, Interface Control Document/Specifications, Engineering Management Plan, Configuration Management Plan, Technical Standards View with Systems View-Technical Standards View Bridge, and procedures for standards conformance and interoperability testing. An interface is designated as a key interface when one or more the following criteria are met:

E2.1.1.1. The interface spans organizational boundaries.

E2.1.1.2. The interface is mission critical.

E2.1.1.3. The interface is difficult or complex to manage.

E2.1.1.4. There are capability, interoperability, or efficiency issues associated with the interface.

E2.1.1.5. The interface impacts multiple acquisition programs.

E2.1.1.6. The interface is vulnerable or important from a security perspective.

E2.1.2. 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 DoD Component directly, or used by a contractor under a contract with the Component, which:

E2.1.2.1. Requires the use of such equipment; or

E2.1.2.2. Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

E2.1.2.3. The term "IT" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "IT" does not include any equipment that is acquired by a Federal contractor incident to a Federal contract. The term "IT" includes National Security Systems (NSS).

E2.1.3. Interoperability. Interoperability is the ability of systems, units or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. IT and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It impacts systems, processes, procedures, organizations, and missions over the life cycle and it must be balanced with Information Assurance.

E2.1.4. National Security System (NSS). Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which:

E2.1.4.1. Involves intelligence activities.

E2.1.4.2. Involves cryptologic activities related to national security.

E2.1.4.3. Involves command and control of military forces.

E2.1.4.4. Involves equipment that is an integral part of a weapon or weapons system.

E2.1.4.5. Is critical to the direct fulfillment of military or intelligence missions. This does not include automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

E2.1.5. Standard. A document that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. Standards may also establish requirements for selection, application, and design criteria of material.

E2.1.6. <u>Standards Compliance</u>.   Confirmation that an IT system and NSS satisfy policy, doctrine and interoperability requirements.

E2.1.7. <u>Standards Conformance Testing</u>.   Confirmation by DISA that an IT system and NSS have implemented required IT standards correctly.

E2.1.8. <u>Standards Validation</u>.   Validation testing ensures that the standard itself is complete, correct, and internally consistent.