Downloaded from http://www.everyspec.com

Department of Defense

DIRECTIVE

NUMBER 4630.5

May 5, 2004

ASD(NII)/DoD CIO

SUBJECT: Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

References: (a) DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," January 11, 2002 (hereby canceled)
(b) Subtitle III of title 40, United States Code, as amended
(c) Sections 2223 and 2224 of title 10, United States Code, as amended
(d) DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003
(e) through (n), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update DoD policy and responsibilities for interoperability and supportability of Information Technology (IT), including National Security Systems (NSS), and implements DoD Chief Information Officer's (DoD CIOs) responsibilities contained in references (b) and (c).

1.2. Defines a capability-focused, effects-based approach to advance IT and NSS interoperability and supportability across the Department of Defense.

1.3. Establishes the Net-Ready Key Performance Parameter (NR-KPP) to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP and incorporates net-centric concepts for achieving IT and NSS interoperability and supportability.

Downloaded from http://www.everyspec.com

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 Inspector General of the Department of Defense, the Defense Agencies (see paragraph E2.1.5.), the DoD Field Activities, and all other organizational entities in the Department of Defense (referred to collectively as "the DoD Components").

2.2. All IT, including NSS (referred to hereafter as IT and NSS), acquired, procured (systems or services), or operated by any DoD Component, to include:

2.2.1. All IT and NSS defense acquisition programs, defense technology IT and NSS projects, and IT and NSS pre-acquisition demonstrations (e.g., Advanced Concept Technology Demonstrations, Advanced Technology Demonstrations, and Joint Warrior Interoperability Demonstrations when selected for acquisition or procurement), Joint Experimentation, and Joint Tests and Evaluations; non-5000 Series IT and NSS acquisitions or procurements (e.g., the Combatant Command and Control Initiatives Program, Combatant Commander Initiatives Fund, Combatant Commander Field Assessments, Military Exploitation of Reconnaissance and Technology Programs, and Tactical Exploitation of National Capabilities Programs); and post-acquisition (fielded) IT and NSS systems.

2.2.2. All inter- and intra-DoD Component IT and NSS that exchange and use information to enable units or forces to operate in joint, combined, coalition, and interagency operations.

2.2.3. All DoD Component IT and NSS supporting business areas and domains within the Department of Defense.

2.2.4. All IT and NSS acquired, procured, or operated by DoD intelligence agencies, DoD Component intelligence elements, and other DoD intelligence activities engaged in direct support of DoD missions. This Directive recognizes that special measures may be required for protection and handling of foreign intelligence or counterintelligence information, or other need to know information. Accordingly, implementation of this Directive must be tailored to comply with coordinated Director of Central Intelligence Directives and Intelligence Community policies.

Downloaded from http://www.everyspec.com

2.2.5. All DoD IT and NSS that share information with other external U.S. Government Departments and Agencies, combined and coalition partners, and multinational alliances (e.g., North Atlantic Treaty Organization).

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. IT and NSS employed by U.S. Forces shall, where required (based on capability context), interoperate with existing and planned, systems and equipment, of joint, combined and coalition forces and with other U.S. Government Departments and Agencies, as appropriate. The Department of Defense shall achieve and maintain decision superiority for the warfighter and decision-maker by developing, acquiring, procuring, maintaining, and leveraging interoperable and supportable IT and NSS.

4.2. IT and NSS, of the DoD Global Information Grid (GIG), shall provide for easy access to information, anytime and anyplace, with attendant information assurance. The GIG architecture shall be used as the organizing construct for achieving net-centric operations and warfare.

4.3. IT and NSS interoperability and supportability needs shall be derived using Joint Operating Concepts, Joint Functional Concepts, and associated integrated architectures and shall be updated as necessary throughout the system's life. For IT and NSS supporting DoD business areas and domains, the GIG Architecture shall be used to determine interoperability and capability needs. IT and NSS interoperability and supportability needs, for a given capability, shall be identified through the following:

4.3.1. The Defense Acquisition System (as defined in the 5000 series of DoD issuances (references (d) and (e)))

4.3.2. The Joint Capabilities Integration and Development System (JCIDS) process.

4.3.3. The Doctrine, Organization, Training, Materiel, Leadership and education, Personnel and Facilities (DOTMLPF) change recommendation process.

Downloaded from http://www.everyspec.com

4.4. A capability-focused, effects-based interoperability process for improving IT and NSS interoperability and supportability shall incorporate both materiel (acquisition or procurement) and non-materiel (doctrine, organization, training, leadership and education, personnel, and facilities) solution sets. The operational community shall identify, prioritize, and synchronize non-materiel solutions with materiel solutions to resolve interoperability and supportability issues.

4.5. IT and NSS interoperability shall be verified early, and with sufficient frequency throughout a system's life, or upon changes affecting interoperability or supportability, to assess, evaluate, and certify its overall interoperability and supportability within a given capability. Joint interoperability certification testing shall be as comprehensive as possible, while still being cost effective, and shall be completed prior to fielding of a new IT and NSS capability or upgrade to existing IT and NSS.

4.6. A NR-KPP, consisting of verifiable performance measures and metrics, shall be used to assess information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange.

4.7. IT and NSS interoperability and supportability needs shall be managed, evaluated, and reported over the life of the system using an Information Support Plan (ISP).

4.8. Interoperability and supportability needs shall be balanced with requirements for Information Assurance (IA).

5. RESPONSIBILITIES

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

5.1.1. Maintain this Directive, with the other DoD Components, to implement the policies and responsibilities necessary to advance interoperability and supportability of IT and NSS throughout the Department of Defense.

5.1.2. Advise the Deputy Secretary of Defense, in coordination with the affected DoD Components, regarding alternative solutions and funding needs to meet interoperability and supportability shortfalls.

Downloaded from http://www.everyspec.com

5.1.3. Provide policy, guidance, and oversight, with the DoD Components, to ensure that IT and NSS are interoperable and supportable with other relevant IT and NSS internal and external (to include combined and coalition systems) to the Department of Defense.

5.1.4. Ensure, with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)); the Under Secretary of Defense for Policy; the Under Secretary of Defense (Comptroller) (USD(C))/Chief Financial Officer (CFO); the Under Secretary of Defense for Intelligence (USD(I)); the Director, Program Analysis and Evaluation (DPA&E); the Director, Operational Test and Evaluation (DOT&E); the Chairman of the Joint Chiefs of Staff; the Commander, U.S. Joint Forces Command (USJFCOM); and the other DoD Components, that IT and NSS interoperability and supportability issues are addressed during the acquisition or procurement process. Ensure interoperability and supportability needs, particularly cross-system and cross-Service, are identified and recommended for programming and budgeting.

5.1.5. Ensure the development, implementation and maintenance of the GIG Architecture per DoD Directive 8100.1 (reference (f)), as the sound and integrated Information Technology Architecture required by reference (b).

5.1.6. Ensure, with the USD(AT&L), the USD(C)/CFO, the USD(I), the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the other DoD Components, that integrated architectures, underpinned by the GIG Architecture, are defined, developed, integrated, coordinated, validated, synchronized, and implemented.

5.1.7. Establish and maintain responsibilities and procedures, with the USD(AT&L), the USD(I), the USD(C)/CFO, the DPA&E, the DOT&E, the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the other DoD Components, to ensure verification and certification of IT and NSS interoperability and supportability throughout a system's life. The Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD CIO, with the DoD Components, shall also ensure user-defined, capability-focused, effects-based performance measures are established for verifying the NR-KPP.

5.1.8. Ensure that the Director, Defense Information Systems Agency (DISA), maintains an IT and NSS test, assessment, evaluation, and certification process for verifying interoperability and supportability in collaboration with the DoD Components. Results from DISA interoperability tests, assessments, evaluations, and certifications shall conform to applicable security classification guidance to avoid potential

Downloaded from http://www.everyspec.com

compromise of information that may reveal component and/or system susceptibilities and vulnerabilities.

5.1.9. Define, with the USD(AT&L), the DOT&E, the Chairman of the Joint Chiefs of Staff, and the other DoD Components, policy, procedures, format, and content for the ISP to facilitate analysis and planning for IT and NSS interoperability, supportability, and sufficiency over a system's life.

5.1.10. Define, organize, and approve, with the USD(AT&L), the Chairman of the Joint Chiefs of Staff, and the DoD Components, Universal Reference Resources (URRs) for developing and using integrated architectures throughout the Department of Defense.

5.1.11. Ensure, with the USD(I) and the Chairman of the Joint Chiefs of Staff, that approved integrated architecture framework concepts and products are incorporated into information assurance guidance and policy.

5.1.12. Maintain a consolidated inventory for DoD Mission Critical Information Systems and Mission Essential Information Systems.

5.1.13. Establish and maintain, with the DoD Components, policy and processes for identifying, prescribing, and implementing IT and NSS standards, consistent with references (b), (c), and DoD Instruction 4120.24 (reference (g)), that apply across the Department of Defense.

5.1.14. Review, assess, and evaluate IT and NSS acquisitions and procurements, and, with the DoD Components, propose recommendations to the Secretary of Defense for the elimination of unnecessary duplication of IT and NSS within and among the DoD Components.

5.1.15. Propose to the Deputy Secretary of Defense, with the USD(AT&L), the USD(C)/CFO, the USD(I), the DPA&E, the DOT&E, the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the other DoD Components, materiel and non-materiel recommendations for resolving critical IT and NSS interoperability and supportability issues. These recommendations shall be prioritized and phased for acquisition (or procurement) and implementation.

5.1.16. As the Chairman of the Committee on National Security Systems, consider requests for release of IA products or associated IA information to a foreign government or an international organization when required to achieve combined or coalition interoperability.

Downloaded from http://www.everyspec.com

5.2. The Under Secretary of Defense for Acquisition, Technology, and Logistics shall:

5.2.1. As the Department of Defense Acquisition Executive (reference (h)), ensure the policies outlined in section 4., above, are reflected in the 5000 series of DoD issuances (references (d) and (e)) and addressed during systems acquisition, as appropriate.

5.2.2. For all acquisition matters, with the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the affected DoD Components, approve tradeoffs among operational effectiveness, operational suitability, information assurance, and IT and NSS interoperability and supportability.

5.2.3. Assign responsibilities and establish procedures, with the ASD(NII)/DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM, for assessing and verifying IT and NSS interoperability and supportability throughout a system's life. Ensure capability-focused, effects-based performance measures are established for verifying the NR-KPP.

5.2.4. Ensure, with the ASD(NII)/DoD CIO and the Chairman of the Joint Chiefs of Staff, that approved integrated architecture framework concepts and products are incorporated into acquisition guidance and policy.

5.2.5. Emphasize robust verification of IT and NSS interoperability and supportability in applicable capability environments as early as possible during a system's development.

5.3. The Under Secretary of Defense for Policy shall ensure the Assistant Secretary for Homeland Defense:

5.3.1. Represents the Department of Defense on all homeland defense-related matters with designated Lead Federal Agencies, the Executive Office of the President, the Department of Homeland Security, other Executive Departments and Federal Agencies, and State and local entities to ensure that homeland defense IT and NSS interoperability and supportability issues are identified to the ASD(NII)/DoD CIO.

5.3.2. Establishes procedures in coordination with the ASD(NII)/DoD CIO to assess and verify IT and NSS interoperability and supportability needs, that are homeland defense-related, requested by Federal, State, and local entities external to the Department of Defense.

Downloaded from http://www.everyspec.com

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

5.4.1. Ensure, with the affected DoD Components, IT and NSS interoperability and supportability funding issues resulting from the requirements of this Directive are addressed in the budgetary process.

5.4.2. Provide the Deputy Secretary of Defense, with the USD(AT&L), the USD(I), the ASD(NII)/DoD CIO, the DPA&E, the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the other DoD Components, budget recommendations for addressing critical IT and NSS interoperability and supportability issues.

5.5. The Under Secretary of Defense for Intelligence shall:

5.5.1. Ensure the Director, National Security Agency/Central Security Service prescribes information assurance policy and procedures for safeguarding IT and NSS capabilities.

5.5.2. Ensure, with the ASD(NII)/DoD CIO, interoperability and supportability for DoD and interagency IT and NSS interfacing with, or supporting the intelligence community.

5.6. The Director of Program Analysis and Evaluation shall:

5.6.1. Provide guidance to the DoD Components for conducting Analysis of Alternatives (AoAs) for IT and NSS capability gaps identified through the JCIDS process. Ensure interoperability and supportability needs are considered and addressed as part of the AoA.

5.6.2. Provide, with the affected DoD Components, recommendations to the Deputy Secretary of Defense for addressing, through the Planning, Programming, Budgeting, and Execution process, critical IT and NSS interoperability and supportability issues.

5.7. The Director of Operational Test and Evaluation shall:

5.7.1. Coordinate with the Chairman of the Joint Chiefs of Staff and the Commander, USJFCOM, to ensure the NR-KPP specified in JCIDS documents is verifiable through testing or analysis, and contributes to the evaluation of a system's operational effectiveness and suitability.

Downloaded from http://www.everyspec.com

5.7.2. Develop policy, processes, practices, and test infrastructure, with the USD(AT&L) and the ASD(NII)/DoD CIO, to ensure IT and NSS interoperability and supportability are evaluated as a measure of operational effectiveness throughout all test programs. Ensure interoperability test requirements are identified in test and evaluation master plans and operational test plans. Emphasize evaluation of IT and NSS interoperability and supportability, in applicable capability environments, as early as possible during a system's development.

5.7.3. Provide an assessment of interoperability and related supportability at acquisition milestones. Report results of these interoperability and supportability assessments as part of the DOT&E Annual Report to the Congress.

5.7.4. Assist the DoD Components with test planning for verifying the NR-KPP.

5.8. The Heads of the DoD Components shall:

5.8.1. Ensure the requirements of this Directive are implemented, including establishing procedures for: the development, coordination, review, and verification of the NR-KPP; IT and NSS acquisition or procurement; and testing within respective functional areas.

5.8.2. Ensure required interoperability and supportability is designed, developed, incorporated, tested, and evaluated for all DoD Component IT and NSS. When necessary, recommend tradeoffs among operational effectiveness, operational suitability, information assurance, and IT and NSS interoperability and supportability to the USD(AT&L), the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM.

5.8.3. Ensure IT and NSS interoperability and supportability requirements are identified and accommodated in the respective DoD Components' budgets. When necessary, propose alternative programmatic, technical, and funding solutions to meet IT and NSS interoperability and supportability shortfalls to the USD(AT&L), the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM.

5.8.4. Comply with DoD Directive 8500.1, DoD Instruction 8500.2, DoD Instruction 5200.40, and NSTISSP No. 11 (references (i) through (l)) requirements for IA certification and accreditation. According to DCI Directive 6/3 (reference (m)), certain systems processing intelligence information or components of such systems must be accredited by the appropriate Designated Approval Authority depending upon

Downloaded from http://www.everyspec.com

the level of information protection required. For Top Secret/Sensitive Compartmented Information and Special Access Program systems, comply with references (m) and Office of the Intelligence Community (IC) Chief Information Officer (CIO), "Top Secret/Sensitive Compartmented Information and Below Interoperability (TSABI) Policy," (reference (n)) requirements for IA certification and accreditation.

5.8.5. Implement procedures to ensure the use and implementation of approved standards contained in the DoD Information Technology Standards Registry for programs under the DoD Components' cognizance.

5.8.6. Ensure test and evaluation plans are prepared for all IT and NSS acquisitions and procurements.

5.8.7. Develop procedures for all IT and NSS acquisitions and procurements to document, manage, evaluate, and report on IT and NSS interoperability, supportability, and sufficiency throughout a system's life using an ISP.

5.8.8. Provide results of developmental and operational joint interoperability assessments, tests, and evaluations, where significant interoperability issues have been identified, to the USD(AT&L), the ASD(NII)/DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM.

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

5.9.1. Establish policy and procedures, with the Commander, USJFCOM and the other DoD Components, for the development, coordination, review, and approval of IT and NSS interoperability and supportability needs.

5.9.2. Direct the use of integrated architectures to facilitate the identification of IT and NSS interoperability and supportability needs within a capability-focused, effects-based context.

5.9.3. Develop, approve, and issue joint concepts and associated operational procedures to achieve interoperability and supportability of IT and NSS employed by U.S. Military Forces and, where required, with: joint, combined, and coalition forces; and with other U.S. Government Departments and Agencies.

5.9.4. Review, certify, and validate sufficiency of the NR-KPP.

Downloaded from http://www.everyspec.com

5.9.5. Maintain, with the USD(AT&L), the ASD(NII)/DoD CIO, the DOT&E, and the Commander, USJFCOM, procedures for verification and certification of interoperability based on meeting the requirements of the NR-KPP, for both new and fielded IT and NSS, throughout a system's life.

5.9.6. Ensure, with the USD(AT&L), the ASD(NII)/DoD CIO, the DOT&E, the Commander, USJFCOM, and the other DoD Components, that insights gained from Service, combined, joint, and coalition exercises, demonstrations, experiments, and operations are included in JCIDS analysis to facilitate improvements in IT and NSS interoperability and supportability.

5.10. The Commander, U.S. Joint Forces Command shall:

5.10.1. Serve as the Chief Advocate for Interoperability.

5.10.1.1. Assess IT and NSS interoperability and supportability from the warfighter's perspective.

5.10.1.2. Review and comment on the sufficiency of the NR-KPP.

5.10.1.3. Ensure systems, within a given capability, address interoperability and supportability from inception throughout a system's life.

5.10.2. Solicit from the Combatant Commanders joint, combined, and coalition IT and NSS interoperability and supportability issues.

5.10.3. Identify, consolidate, and prioritize IT and NSS interoperability and supportability issues affecting fielded systems in coordination with the Combatant Commanders.

5.10.4. Provide operationally prioritized and programmatically synchronized materiel and non-materiel recommendations for resolving IT and NSS interoperability and supportability issues to the Chairman of the Joint Chiefs of Staff. Coordinate recommendations with the USD(AT&L), the USD(C)/CFO, the ASD(NII)/DoD CIO, and the Chairman of the Joint Chiefs of Staff.

5.10.5. Identify, consolidate, and prioritize IT and NSS interoperability and supportability issues affecting fielded systems for the Standing Joint Forces Headquarters, in coordination with the Combatant Commanders.

Downloaded from http://www.everyspec.com

6. EFFECTIVE DATE

This Directive is effective immediately.

Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 2
E1. References, continued
E2. Definitions

Downloaded from http://www.everyspec.com

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003

(f) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002

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

(h) Section 133 of title 10, United States Code

(i) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002

(j) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

(k) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997

(l) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products," June 2003 [1]

(m) DCI Directive 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," June 5, 1999

(n) Office of the Intelligence Community (IC) Chief Information Officer (CIO), "Top Secret/Sensitive Compartmented Information and Below Interoperability (TSABI) Policy," v4.20, November 24, 2003 [2]

---

[1] Available at: http://www.nstissc.gov/Assets/pdf/NSTISSP_11_revised_fst.pdf

[2] Available on JWICS at: http://www.iccio.ic.gov/docs/side_menu/security/tsabi/

Downloaded from http://www.everyspec.com

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Architectures. The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.

E2.1.2. Capability. The ability to execute a specified course of action. It is defined by an operational user and expressed in broad operational terms. A capability includes the doctrine, organization, training, materiel, leadership and education, personnel, and facilities required to achieve a specified course of action.

E2.1.3. Capability-Focused, Effects-Based Interoperability. An interoperability process that:

E2.1.3.1. Includes experts from the operational community to identify, consolidate and prioritize interoperability needs; and synchronize non-materiel solutions with materiel solutions for both new and fielded capabilities.

E2.1.3.2. Characterizes IT and NSS interoperability needs in a capability-focused, effects-based context using integrated architectures derived from Joint Operating Concepts (JOCs) and Joint Functional Concepts (JFCs).

E2.1.3.3. Assesses net-readiness; information assurance requirements; and both the technical exchange of information and the end-to-end operational effectiveness of that exchange using the NR-KPP.

E2.1.3.4. Incorporates both materiel (acquisition or procurement) and non-materiel (doctrine, organization, training, leadership and education, personnel, or facilities) solutions.

E2.1.3.5. Verifies interoperability solutions in formal tests or operational exercises.

E2.1.3.6. Continuously verifies the NR-KPP and evaluates overall IT and NSS interoperability, within a given capability, throughout a system's life.

E2.1.4. Decision Superiority. The state at which better decisions are arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission.

Downloaded from http://www.everyspec.com

E2.1.5. Defense Agencies. All agencies and offices of the Department of Defense including the Missile Defense Agency, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit 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 Geospatial-Intelligence Agency, National Reconnaissance Office, and National Security Agency/Central Security Service.

E2.1.6. DoD Information Technology Standards Registry (DISR). The DISR provides the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. It defines the service areas, interfaces, standards (DISR elements), and standards profiles applicable to all DoD systems. Use of the DISR is mandated for the development and acquisition of new or modified fielded IT and NSS systems throughout the Department of Defense. The DISR replaced the Joint Technical Architecture.

E2.1.7. Global Information Grid (GIG)

E2.1.7.1. 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 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.

E2.1.7.2. Includes any system, equipment, software, or service that meets one or more of the following criteria:

E2.1.7.2.1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

Downloaded from http://www.everyspec.com

E2.1.7.2.2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

E2.1.7.2.3. Processes data or information for use by other equipment, software, or services.

E2.1.7.3. Non-GIG IT. Stand-alone, self-contained, or embedded IT that is not and shall not be connected to the enterprise network.

E2.1.8. Information Assurance (IA). Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.9. Information Needs. A condition or situation requiring knowledge or intelligence derived from received, stored, or processed facts and data.

E2.1.10. 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 DoD Component, which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. 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 incidental to a Federal contract. The term "IT" includes National Security Systems (NSS).

E2.1.11. Information Technology Architecture. An integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the Agency's strategic goals and information resources management goals.

E2.1.12. Information Timeliness. Occurring at a suitable or appropriate time for a particular condition or situation.

Downloaded from http://www.everyspec.com

E2.1.13. Integrated Architecture. An architecture consisting of multiple views or perspectives (operational view, systems view, and technical standards view) that facilitates integration and promotes interoperability across capabilities and among related integrated architectures.

E2.1.13.1. The operational architecture view is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions.

E2.1.13.2. The systems architecture view is a description, including graphics, of systems and interconnections providing for, or supporting, DoD functions.

E2.1.13.3. The technical standards architecture view is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

E2.1.14. Interoperability. 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 includes systems, processes, procedures, organizations and missions over the life cycle and must be balanced with information assurance.

E2.1.15. Interoperability and Supportability Needs. A condition, situation, or capability in which interoperability and supportability deficiencies have been identified, based on an approved or established rule set, test, or measure of value for judging interoperability and supportability sufficiency of IT and NSS.

E2.1.16. Joint Capabilities Integration and Development System (JCIDS). A Chairman of the Joint Chiefs of Staff process to identify, assess, and prioritize joint military capability needs. The JCIDS process is a collaborative effort that uses joint concepts and integrated architectures to identify prioritized capability gaps and integrated DOTMLPF solutions (materiel and non-materiel) to resolve those gaps.

E2.1.17. Joint Functional Concept (JFC). An articulation of how a future Joint Force Commander shall integrate a set of related military tasks to attain capabilities

Downloaded from http://www.everyspec.com

required across the range of military operations. Although broadly described within the Joint Operations Concepts, JFCs derive specific context from the joint operating concepts and promote common attributes in sufficient detail to conduct experimentation and measure effectiveness.

E2.1.18. Joint Operating Concept (JOC). An articulation of how a future Joint Force Commander shall plan, prepare, deploy, employ, and sustain a joint force against potential adversaries' capabilities or crisis situations specified within the range of military operations. JOCs guide the development and integration of JFCs to provide joint capabilities. JOCs articulate the measurable detail needed to conduct experimentation and allow decision makers to compare alternatives.

E2.1.19. Joint Operations Concepts. A concept that describes how the Joint Force intends to operate 15 to 20 years from now. It provides the operational context for the transformation of the Armed Forces of the United States by linking strategic guidance with the integrated application of Joint Force capabilities.

E2.1.20. Key Performance Parameters (KPPs). Those minimum attributes or characteristics considered most essential for an effective military capability. KPPs are validated by the Chairman of the Joint Chiefs of Staff.

E2.1.21. Materiel Solution. Correction of a deficiency, satisfaction of a capability gap, or incorporation of new technology that results in the development, acquisition, procurement, or fielding of a new item (including ships, tanks, self-propelled weapons, aircraft, etc., and related software, spares, repair parts, and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without disruption as to its application for administrative or combat purposes.

E2.1.22. Mission Critical Information Systems. A system that meets the definitions of "information system" and "national security system" in reference (b), the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. The designation of mission critical shall be made by a DoD Component Head, a Combatant Commander, or their designee. A Mission Critical Information Technology System has the same meaning as a Mission Critical Information System.

Downloaded from http://www.everyspec.com

E2.1.23. Mission Essential Information Systems. A system that meets the definition of "information system" in reference (b), that the acquiring DoD Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. The designation of mission essential shall be made by a DoD Component Head, a Combatant Commander, or their designee.

E2.1.24. National Security System (NSS). Any telecommunications or information system operated by the United States Government, the function, operation, or use of which:

E2.1.24.1. Involves intelligence activities.

E2.1.24.2. Involves cryptologic activities related to national security.

E2.1.24.3. Involves command and control of military forces.

E2.1.24.4. Involves equipment that is an integral part of a weapon or weapons system.

E2.1.24.5. 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).

E2.1.25. Net-Centric Operations and Warfare (NCOW) Reference Model (RM). The NCOW RM describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities (core services, Community of Interest services, and environment control services), and the enterprise management components. It also describes a selected set of key standards that shall be needed as the NCOW capabilities of the GIG are realized.

E2.1.26. Net-Ready. The continuous ability to interface and interoperate to achieve operationally secure exchanges of information in conformance with enterprise constraints. The NR-KPP assesses the net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange.

E2.1.27. Net-Ready Key Performance Parameter (NR-KPP). The NR-KPP assesses information needs, information timeliness, information assurance, and

Downloaded from http://www.everyspec.com

net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following elements:

E2.1.27.1. Compliance with the NCOW RM.

E2.1.27.2. Compliance with applicable GIG Key Interface Profiles.

E2.1.27.3. Verification of compliance with DoD information assurance requirements.

E2.1.27.4. Supporting integrated architecture products required to assess information exchange and use for a given capability.

E2.1.28. Non-Materiel Solution. Changes in doctrine, organization, training, leadership and education, personnel, or facilities that satisfy identified capability gaps.

E2.1.29. Supportability. The ability of systems and infrastructure components, external to IT or NSS, to achieve, aid, protect, complement, or sustain design, development, testing, training, or operations of the IT or NSS to its required capability.

E2.1.30. Universal Reference Resources (URRs). Reference models and information standards which serve as sources for guidelines and attributes that must be consulted in building integrated architecture products. The following are the currently listed URRs: DoD Architecture Framework; DoD Core Architecture Data Model; Universal Joint Task List; Technical Reference Model; Global Information Grid (GIG) Architecture; DoD Net-Centric Data Strategy; DoD Metadata Registry; Net-Centric Operations Warfare (NCOW) Reference Model (RM); and the DoD Information Technology Standards Registry.