



Department of Defense

DIRECTIVE

NUMBER 5105.19

July 25, 2006

DA&M

SUBJECT: Defense Information Systems Agency (DISA)

- References:
- (a) Title 10, United States Code
 - (b) DoD Directive 5105.19, "Defense Information Systems Agency (DISA)," June 25, 1991 (hereby canceled)
 - (c) National Security Presidential Directive – 28, "United States Nuclear Weapons Command and Control, Safety, and Security," June 20, 2003¹
 - (d) Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," as amended by E.O. 13286 of February 28, 2003
 - (e) through (ac), see Enclosure 1

1. REISSUANCE AND PURPOSE

Under the authority vested in the Secretary of Defense by sections 113, 191, and 193 of Reference (a), this Directive reissues Reference (b) to update the mission, responsibilities, functions, relationships, and authorities of the DISA, under the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO).

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components"). The term "Military Services," as used herein, refers to the Army, the Navy, the Air Force, and the Marine Corps.

2.2. This Directive does not alter or supersede existing authorities such as that of the Director of National Intelligence and policies in public law, Executive Order, and regulation regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence.

¹ This NSPD is held within the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.

3. DEFINITIONS

For the purpose of this Directive, terms used are defined in Enclosure 2.

4. MISSION

The DISA shall be responsible for planning, engineering, acquiring, testing, fielding, and supporting global net-centric information and communications solutions to serve the needs of the President, the Vice President, the Secretary of Defense, and the DoD Components, under all conditions of peace and war. The DISA supports national security communications requirements as identified in the National Security Presidential Directive – 28 (Reference (c)) and Executive Order 12472 (as amended) (Reference (d)). The DISA functions within the following eight broad core areas:

4.1. Communications. Provides DoD transport services that are used for voice, data, and video services through a combination of terrestrial and satellite assets and services.

4.2. Command and Control (C2) Capabilities. Provides enterprise-level development, integration, and management services for interagency, strategic, allied, multinational, coalition, joint and combined C2, and combat support capabilities.

4.3. Information Assurance (IA). Works, in conjunction with other DoD Components, to ensure the security of DoD enterprise systems and supports the Commanders of the Combatant Commands and deployed forces by designing and deploying proactive protections, deploying attack detection, and performing other necessary security functions.

4.4. Computing Services. Provides and/or hosts legacy and net-centric enterprise services, mainframe and server computer operations, web services, production support, technical services, and end user assistance for command and control, combat support, and eBusiness functions throughout the Department of Defense.

4.5. Interoperability, Testing, and Standards. Provides standards, interoperability testing, spectrum support and deconfliction, and integrated architecture development for the DoD net-centric enterprise information environment.

4.6. Global Information Grid (GIG) Enterprise Services. Provides the DoD enterprise with a net-centric, service-based, shared enterprise infrastructure that supports ubiquitous user access to reliable capabilities and decision-quality information.

4.7. Engineering. Provides enterprise-wide systems engineering support for the GIG to ensure that it is planned, acquired, operated, maintained, managed, and improved effectively and efficiently for end-to-end interoperability down to the tactical edge.

4.8. Acquisition. Provides acquisition leadership for the implementation of the net-centric vision. Provides tailored acquisition policies, processes, procedures, tools, lifecycle oversight, and a qualified workforce that acquires quality products and services to satisfy user needs and provide improvements to mission capabilities.

5. ORGANIZATION AND MANAGEMENT

5.1. The DISA is a Defense Agency under the authority, direction, and control of the ASD(NII)/DoD CIO, in accordance with DoD Directive 5144.1 (Reference (e)). The DISA is designated as a Combat Support Agency in accordance with section 193 of Reference (a). It shall consist of a Director and such subordinate organizational elements as are established by the Director within the resources assigned by the Secretary of Defense.

5.2. The Director, DISA, has additional responsibilities as outlined in Secretary of Defense and Acting Deputy Secretary of Defense memoranda (References (f) and (g)) to include serving as the Commander, Joint Task Force-Global Network Operations (JTF-GNO).

6. RESPONSIBILITIES AND FUNCTIONS

6.1. The Director, DISA, shall:

6.1.1. Plan, organize, direct, and manage DISA and all assigned resources consistent with responsibilities outlined in this Directive and guidance issued by the ASD(NII)/DoD CIO.

6.1.2. Provide support to the ASD(NII)/DoD CIO in the implementation of the responsibilities outlined in Reference (e), DoD Directive 8000.1 (Reference (h)), and DoD Directive 8100.1 (Reference (i)).

6.1.3. Provide to the ASD/(NII)/DoD CIO technical support to include representation to international and North Atlantic Treaty Organization (NATO) fora.

6.1.4. In the core area of Communications:

6.1.4.1. Perform systems engineering for the GIG to include the Defense Information Systems Network (DISN) to ensure that it is planned, operated, maintained, managed, and improved effectively and efficiently for end-to-end interoperability and mission capable architecture. The Director, DISA, shall exercise program management (with management control) over the activities of the DoD Components that directly support the DISN.

6.1.4.2. Provide forces to the JTF-GNO, under the direction of United States Strategic Command (USSTRATCOM), to operate and defend the GIG, in accordance with References (e), (f), and (i).

6.1.4.3. Acquire commercial communications services including commercial satellite network assets for the Department of Defense, in accordance with Deputy Secretary of Defense memorandum (Reference (j)), and other Federal Agencies, as directed. The Director, DISA, shall also maintain the Telecommunications Service/Enterprise Acquisition Services (a working capital fund) and shall initiate and manage actions relating to regulatory and tariff matters and rates for commercial communications services.

6.1.4.4. In consultation with the Heads of the DoD Components, analyze user requirements and maintain the user requirements database.

6.1.4.5. Define system performance criteria for Military Satellite Communications (MILSATCOM) systems and, through coordination with the DoD Components, develop and perform general systems engineering to achieve a long term, interoperable, mission capable system. The Director, DISA, shall continually analyze Military Department programs, plans, budgets, and MILSATCOM systems performance to identify areas of deficiency and shall recommend or initiate corrective action, as appropriate. The Director, DISA, shall provide MILSATCOM technical support to ASD(NII)/DoD CIO to include representation to international and NATO fora.

6.1.4.6. Provide for continuity of communications and support the National Security Emergency Preparedness (NSEP) Telecommunications Functions of the National Communications System (NCS) as described in Enclosure 3.

6.1.4.7. Provide support for White House communications requirements for the National Security Council, White House Military Office and the White House Communications Agency (WHCA). The Director, DISA, shall manage all WHCA funding as a sub-activity under DISA's appropriation. The Director, DISA, shall manage all personnel actions for all WHCA officers and civilians and provide required administrative services and evaluations for all WHCA personnel. The Director, DISA, shall also provide WHCA with program management and contracting support as required.

6.1.4.8. Provide liaison with, and communications support for, the United States Secret Service, in accordance with DoD Directive 3025.13 (Reference (k)).

6.1.4.9. Provide communications systems support for congressionally assigned detection and monitoring functions aimed at interdicting illegal drugs entering the United States, in accordance with Deputy Secretary of Defense memoranda (References (l) and (m)).

6.1.4.10. Operate the Department of Defense Domain Name Service (.MIL) for DoD Networks. Serve as the registrar for .MIL and maintain the .MIL registration database. Ensure public Internet access to .MIL to support E-Government responsibilities of the Department of Defense, in accordance with the E-Government Act of 2002 (Reference (n)). Manage domain name registration and IP address allocation on an enterprise basis to promote interoperability and security.

6.1.5. In the core area of Command and Control Capabilities:

6.1.5.1. Provide net-centric services and support for interagency, strategic, allied, multinational, coalition, joint, and combined command and control capabilities, in accordance with Presidential direction, memoranda of agreement, treaties, and international agreements.

6.1.5.2. Provide management advice and technical services for the design, development, deployment, and evolution of combat command center systems, to include support for the National Military Command System and supporting communications, especially connectivity to nuclear forces, as required by DoD Directive S-5100.44 (Reference (o)).

6.1.5.3. Manage, design, develop, maintain, test, and evaluate standard operating systems, applications software, and services based capabilities for current and future combat command center systems and the supporting net-centric capabilities. Provide guidance, direction, and support to developers of combat command center systems to include definition and development of integrated architectures, technical concepts, and performance characteristics and specifications.

6.1.5.4. Provide automated information systems, analytical, and other technical support to Chairman of the Joint Chiefs of Staff- and OSD-directed programs.

6.1.5.5. Assist the Chairman of the Joint Chiefs of Staff, the Under Secretary of Defense for Acquisition, Technology, and Logistics, and the ASD(NII)/DoD CIO in developing nuclear command and control standards and evaluating Nuclear Command and Control System (NCCS) program performance, consistent with DoD Directive S-5210.81 (Reference (p)).

6.1.6. In the core area of IA:

6.1.6.1. Provide support to the ASD (NII)/DoD CIO to achieve DoD IA in coordination with the Chairman of the Joint Chiefs of Staff, the National Security Agency (NSA), and the Defense Intelligence Agency (DIA), in accordance with DoD Directive 8500.1 (Reference (q)). This support shall focus on implementation of a defense-in-depth that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare with specific attention upon performance of tasks identified in Reference (q).

6.1.6.2. Coordinate with the Director, NSA/Central Security Service and the Secretaries of the Military Departments to develop strategic and tactical, interoperable secure communications architectures as an integral part of the overall joint architecture, in accordance with DoD Directive C-5200.5 (Reference (r)).

6.1.6.3. In support of USSTRATCOM and in the capacity as Commander, JTF-GNO consistent with References (f) and (g), isolate, disconnect, and/or shutdown information systems (including websites) owned, operated, sponsored, or funded by the Department of Defense that are in violation of applicable security policies, when so directed by appropriate authority in accordance with established procedures.

6.1.6.4. Serve as GIG Defense Sector Lead Agent for the Defense Critical Infrastructure Program, and execute responsibilities in compliance with DoD Directive 3020.40 (Reference (s)).

6.1.7. In the core area of Computing Services:

6.1.7.1. Provide mainframe and cross-component computing for the Department of Defense.

6.1.7.2. Provide the Department of Defense with computer processing for combat support and C2 functions such as transportation, logistics, maintenance, munitions, acquisition, finance, medicine, and military personnel readiness.

6.1.7.3. Provide the Department of Defense with computer processing services which include computer operations, data storage, systems administration, security management, capacity management, system engineering, web and portal hosting, architectural development, and performance monitoring.

6.1.8. In the core area of Interoperability, Testing, and Standards:

6.1.8.1. Develop integrated architectures based on the DoD architectural framework and provide systems engineering support for Command, Control, Communications, and Computer (C4) and information systems.

6.1.8.2. Serve as the DoD Executive Agent for Information Technology (IT) Standards, in accordance with DoD Directive 5101.7 and DoD Directive 5101.1 (References (t) and (u)), with responsibilities for integrating, through standards, DoD information systems and networks serving both U.S. and authorized foreign partners. Consistent with this assignment, the Director, DISA, shall organize, chair, and participate in U.S. military IT standards bodies to develop, publish, and maintain established and developmental interoperability standards; consistent with guidance of the ASD(NII)/DoD CIO, the Director, DISA, shall also represent Department of Defense interests in Federal, nongovernmental, international, and allied IT standards bodies.

6.1.8.3. Serve as the DoD authority for certifying the interoperability of National Security Systems (NSS) and IT systems, developing and publishing key interface profiles, and maintaining configuration management of the GIG, in accordance with References (i) and (t) and DoD Directive 4630.5 (Reference (v)). Monitor NSS/IT programs over which DISA has responsibility and monitor other programs affecting NSS/IT interoperability.

6.1.8.4. Maintain a major field independent operational test capability through the Joint Interoperability Test Command (JITC). Under the direction of the Director, DISA, the JITC shall conduct operational test and evaluation, consistent with DoD Directive 5000.1 and DoD Instruction 5000.2 (References (w) and (x)).

6.1.8.5. Provide support to spectrum policy and operational spectrum management to the OSD Principal Staff Assistants (PSAs), the Chairman of the Joint Chiefs of Staff, and the Commanders of the Combatant Commands to enable effective and efficient use of the electromagnetic spectrum and control of electromagnetic environmental effects in support of national and military objectives.

6.1.8.6. Provide acquisition, systems engineering, testing, fielding, deployment, and operations leadership supporting DoD net-centric goals and objectives according to ASD(NII)/DoD CIO guidance defining the enterprise information environment and net-centric enterprise capabilities.

6.1.9. Ensure DISA programs and activities are designed and managed to improve standards of performance, economy, and efficiency and demonstrate DISA's attention to the requirements of its organizational customers, both internal and external to the Department of Defense.

6.1.10. Develop, integrate, operate, and sustain net-centric core enterprise services to include the DoD Enterprise Service Directory and the requisite GIG portals. Issue guidance and set standards for development and implementation of enterprise services and other enterprise service-related tools and infrastructure for the Department.

6.1.11. Perform such other duties as may be assigned by the Secretary of Defense or the ASD(NII)/DoD CIO.

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

6.2.1. Provide guidance and direction to the Director, DISA, on policies, programs, and procedures related to the development and operation of the networks, command and control, communications, enterprise-wide integration of DoD information matters, network operations, IA, electro-magnetic spectrum, and IT systems, services and capabilities provided by the DISA.

6.2.2. Consult with the Chairman of the Joint Chiefs of Staff, to obtain recommendations and develop guidance and direction for the DISA to ensure that all services and capabilities provided by the DISA are operated and maintained at levels that meet the operational readiness and warfighting requirements of the Commanders of the Combatant Commands.

6.2.3. Provide guidance and direction to the Director, DISA, as required to implement statutory and regulatory responsibilities as the DoD CIO.

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

6.3.1. Review DISN planning and programming documents, and assess their responsiveness to operational, developmental, and training requirements.

6.3.2. Review and assess the responsiveness and readiness of the DISA to support operating forces in the event of war or threats to national security and make any recommendations the Chairman of the Joint Chiefs of Staff considers appropriate, in accordance with Section 193 of Reference (a) and the “Unified Command Plan” (Reference (y)). The Chairman of the Joint Chiefs of Staff shall facilitate communications with the Commanders of the Combatant Commands to improve the adequacy and effectiveness of communications, C2, IA, computing services, interoperability and standardization, GIG enterprise services, engineering and acquisition functions prescribed herein and consistent with Sections 164, 167, and 167a of Reference (a).

6.3.3. Advise the Secretary of Defense on C4 and information systems requirements and priorities in coordination with ASD(NII)/DoD CIO.

6.3.4. Assist the ASD(NII)/DoD CIO in developing guidance for the DISA and the Commanders of the Combatant Commands that will serve as the basis for interrelationships between these organizations.

6.3.5. Provide for DISA participation in joint training exercises and monitor performance.

6.4. The Heads of the DoD Components shall:

6.4.1. Advise the Director, DISA, of funding shortfalls that would prevent effective operations and maintenance of existing systems, or prevent or delay scheduled implementation of new subsystems or projects.

6.4.2. Coordinate with the Director, DISA, on all program activities that include or are related to C4 and information systems. Provide programmatic documents and technical specifications to DISA for prior review and coordination for all C4 and information systems for which DISA has execution, review, development, integration, testing, or support responsibilities. Obtain the Director, DISA, concurrence for programmatic or technical changes impacting funding or interoperability of C4 and information systems for which DISA has primary responsibility.

6.4.2.1. Provide, for review and approval before execution, technical specifications and standards, statements of work, and proposed contract changes impacting on configuration, cost, performance, or schedules for all systems for which DISA is responsible.

6.4.2.2. Coordinate with the Director, DISA, on draft acquisition plans. Request DISA representation on source selection advisory councils and evaluation boards for C4 and information systems, subsystems, and programs that impact systems for which DISA is responsible.

6.4.3. Identify requirements for DISA support for networks, telecommunications, and IT systems, services, and capabilities to the Director, DISA. Where so identified and as appropriate, Component Heads shall provide planning, programming, and budgeting support. The Heads of the DoD Component shall ensure adequate preparation of doctrine, organization, training, material, leadership, personnel, and facilities to support fielding capabilities or services.

7. RELATIONSHIPS

7.1. In the performance of assigned responsibilities and functions, the Director, DISA, shall:

7.1.1. Report directly to the ASD(NII)/DoD CIO.

7.1.2. Be responsible to the Chairman of the Joint Chiefs of Staff for operational matters as well as requirements associated with the joint planning process, subject to the authority, direction, and control of the ASD(NII)/DoD CIO. For these purposes, the Chairman of the Joint Chiefs of Staff is authorized to communicate directly with the Director, DISA, and may task the Director, DISA, to the extent authorized by the ASD(NII)/DoD CIO.

7.1.3. Maintain liaison to exchange information and coordinate actions, as appropriate, with other DoD Components and those Departments and Agencies of the Federal Government having related functions. Coordinate with the Director, NSA, on all National Security Directive -42 (Reference (z)) related issues and activities. Coordinate with the Director, DIA, on systems engineering responsibilities of DIA for the Joint Worldwide Intelligence Communications System, the SCI portions of the DISN, and the GIG.

7.1.4. Use established systems, facilities, and services of the Department of Defense or other Federal Departments and Agencies, when possible, to achieve maximum efficiency and economy.

7.1.5. Support NCS Committee of Principals activities affecting DoD NSEP responsibilities as authorized by the ASD(NII)/DoD CIO.

7.1.6. Serve on the Military Communications Electronics Board, and as a Technical Advisor on the DoD CIO Executive Board.

7.2. The OSD PSAs and the Heads of the other DoD Components shall coordinate with the Director, DISA, on all matters related to the authorities, responsibilities, and functions assigned in this Directive.

8. AUTHORITIES

The Director, DISA, is hereby delegated the authority to:

8.1. Communicate directly with the Heads of the DoD Components as necessary, to carry out assigned functions and responsibilities, including the transmission of requests for advice and assistance. Communications to the Military Departments shall be transmitted through the Secretaries of the Military Department, their designees, or as otherwise provided in law or directed by the Secretary of Defense in other DoD issuances. Communications to the Commanders of the Combatant Commands normally shall be transmitted through the Chairman of the Joint Chiefs of Staff.

8.2. 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 responsibilities and functions. Communications with representatives of the Legislative Branch shall be coordinated with the Assistant Secretary of Defense for Legislative Affairs or the Under Secretary of Defense (Comptroller)/Chief Financial Officer, as appropriate, and be consistent with the DoD Legislative Program.

8.3. Obtain reports and information consistent with DoD Directive 8910.1 (Reference (aa)), as necessary to carry out assigned responsibilities and functions.

8.4. Exercise the administrative authorities contained in Enclosure 4.

9. ADMINISTRATION

9.1. The Director, DISA, shall be an active duty, commissioned officer in the Armed Forces of the United States of General or Flag grade, recommended to the President by the Secretary of Defense with the advice of the Chairman of the Joint Chiefs of Staff and the ASD(NII)/DoD CIO. The Vice Director, DISA, shall be appointed by the Secretary of Defense.

9.2. The Secretaries of the Military Departments shall assign military personnel to the DISA in accordance with approved authorizations and procedures for assignment to joint duty. The Chairman of the Joint Chiefs of Staff shall review and provide recommendations on the DISA joint manpower program to the ASD(NII)/DoD CIO, as appropriate.

10. EFFECTIVE DATE

This Directive is effective immediately.



Gordon England 7/25/06

Enclosures – 4

- E1. References, continued
- E2. Definitions
- E3. Continuity of Communications
- E4. Delegations of Authority

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
- (f) Secretary of Defense Memorandum, "Assignment and Delegation of Authority to Director Defense Information Systems Agency," June 18, 2004
- (g) Acting Deputy Secretary of Defense Memorandum, "Designation of the Director, Defense Information Systems Agency (DISA), as Commander, Joint Task Force-Global Network Operations (JTF-GNO)," November 17, 2005
- (h) DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," February 27, 2002
- (i) DoD Directive 8100.1, "Global Information Grid Overarching Policy," September 19, 2002
- (j) Deputy Secretary of Defense Memorandum, "DoD CIO, Guidance and Policy Memorandum 4-8460 - DoD Global Information Grid Networks," August 24, 2000
- (k) DoD Directive 3025.13, "Employment of Department of Defense Resources in Support of the United States Secret Service," September 13, 1985
- (l) Deputy Secretary of Defense Memorandum, "Designation of the Lead Agency for Communications Integration Within DoD Counternarcotics Effort," October 26, 1989
- (m) Deputy Secretary of Defense Memorandum, "Department of Defense Counternarcotics Policy," July 31, 2002
- (n) E-Government Act of 2002 (Public Law 107-347), December 17, 2002
- (o) DoD Directive S-5100.44, "Master Plan for the National Military Command System (NMCS) (U)," June 9, 1964
- (p) DoD Directive S-5210.81, "United States Nuclear Weapons Command and Control, Safety and Security (U)," August 8, 2005
- (q) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
- (r) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," April 21, 1990
- (s) DoD Directive 3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005
- (t) DoD Directive 5101.7, "DoD Executive Agent for Information Technology Standards," May 21, 2004
- (u) DoD Directive 5101.1, "DoD Executive Agent," September 3, 2002
- (v) DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004
- (w) DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003
- (x) DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003
- (y) O-Memorandum for the Secretary of Defense from the President, "Unified Command Plan," March 1, 2005
- (z) National Security Directive-42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990
- (aa) DoD Directive 8910.1, "Management and Control of Information Requirements," June 30, 1998
- (ab) Subtitle III of title 40, United States Code
- (ac) DoD Directive 3020.26, "Defense Continuity Program (DCP)," September 8, 2004

E2. ENCLOSURE 2

DEFINITIONS

E2.1. Defense Information Systems Network (DISN)

E2.1.1. The DISN is a composite of DoD-owned and leased telecommunications subsystems and networks comprised of facilities, personnel, and material under the management control and operational direction of the DISA. It provides the long-haul, point-to-point, and switched network telecommunications needed to satisfy the requirements of the Department of Defense and certain other Departments and Agencies, including those required to interconnect the President, the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Commanders of the Combatant Commands with the general-purpose networks. DISN assets are part of the Defense Communications System (DCS) and are DoD's NSEP communications assets within the Government-wide NCS.

E2.1.2. The vast majority of the Department of Defense's C2 traffic, voice conferencing, intelligence dissemination, and combat support traffic rides over the joint networks provided by DISA. The aggregate of these networks is referred to as the DISN. It is the key wide-area communications component of the GIG. Specific subsystems include the Defense Red Switch for classified voice conferencing, the Secret Internet Protocol Router Network, the unclassified Internet Protocol Router Network, Enhanced Mobile Satellite Services, the Defense Satellite Communications System, the Defense Switched Network (voice traffic), and DISA Video Service. In addition, DISA provides tailored Community of Interest Networks for specific functional communities that accrue the economic advantage of shared transport and the operational advantages of enhanced security and interoperability with the larger enterprise.

E2.1.3. Although the DISA specifies the interconnection and interface standards when operated with DISN networks, the DISN does not include: Mobile and/or transportable communications facilities and assets organic to the Military Services (unless specifically designated as components of the DISN); platform specific and other tactical telecommunications; post, camp, base, and station user and/or subscriber facilities and terminals; on-site telecommunications facilities associated with or integral to weapons systems and to missile launch complexes; consoles and display devices integral to the Command Centers of the Combatant Commands, their DoD Component Headquarters, and the Military Services' operations centers.

E2.2. Global Information Grid (GIG)

E2.2.1. The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in Section 11103

of title 40, United States Code (U.S.C.) (Reference (ab)). The GIG supports all DoD, 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.

E2.2.2. Includes any system, equipment, software, or service that meets one or more of the following criteria:

E2.2.2.1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

E2.2.2.2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

E2.2.2.3. Processes data or information for use by other equipment, software, or services.

E2.2.3. Non-GIG IT. Stand-alone, self-contained, or embedded IT that is not and will not be connected to the enterprise network.

E3. ENCLOSURE 3

CONTINUITY OF COMMUNICATIONS

E3.1 Requirement for Continuity of Communications. The Department of Defense plays a major role in interagency, intergovernmental, and international communications. Among the responsibilities assigned to the ASD(NII)/DoD (CIO) is ensuring continuity of essential DoD communications capabilities through oversight of information systems and networks that are critical to the performance of mission essential functions during continuity threats or events, in accordance with DoD Directive 3020.26 (Reference (ac)).

E3.2 NSEP Communications. The NSEP functions, prescribed by Reference (d), are integral parts of DoD continuity of communications efforts. DISA shall support NSEP functions of the administrative structure of the NCS as directed by ASD(NII)/DoD CIO. The NCS administrative structure, which includes the Executive Agent, the NCS Committee of Principals and the Manager, is an organizational element of the Department of Homeland Security. The DISA shall perform circuit and service-level engineering and allocation and direct restoration as required. The DISA shall perform systems engineering for the DCS (DoD's component of the interagency NCS communications infrastructure), and ensure that the DCS is planned, improved, maintained, and managed effectively and efficiently. As a key service provider, the DISA shall work in concert with the JTF-GNO to ensure the Department of Defense exercises operational direction and management control of the DCS (in conjunction with the Secretaries of the Military Departments and Commanders of the Combatant Commands), as well as providing for prompt restoration of any portions of the DCS, in coordination with the NCS's National Coordinating Center.

E4. ENCLOSURE 4

DELEGATIONS OF AUTHORITY

E4.1. Under the authority vested in the Secretary of Defense, and subject to the authority, direction, and control of the ASD(NII)/DoD CIO, and in accordance with DoD policies, DoD Directives, and DoD Instructions; the Director, DISA, or in the absence of the Director, the person acting for the Director, is hereby delegated authority as required in the administration and operation of the DISA to:

E4.1.1. Exercise the powers vested in the Secretary of Defense by 5 U.S.C. 301, 302(b), 3101, and 5107 on the employment, direction, and general administration of DISA civilian personnel.

E4.1.2. Fix rates of pay for wage-rate employees exempted from the Classification Act of 1949 by 5 U.S.C. 5102 on the basis of rates established under the Federal Wage System. In fixing such rates, the Director, DISA, shall follow the wage schedule established by the DoD Wage Fixing Authority.

E4.1.3. Establish advisory committees and employ temporary or intermittent experts or consultants for the performance of DISA functions consistent with the 10 U.S.C. 173 and 174; 5 U.S.C. 3109(b); DoD Directive 5105.4; and DoD Directive 5105.18.

E4.1.4. Administer oaths of office to those entering the Executive Branch of the Federal Government or any other oath required by law in connection with employment therein, in accordance with 5 U.S.C. 2903, and designate in writing, as may be necessary, officers and employees of the DISA to perform this function.

E4.1.5. Establish a DISA Incentive Awards Board and authorize cash awards to, and incur necessary expenses for the honorary recognition of, civilian employees of the Government whose suggestions, inventions, superior accomplishments, or other personal efforts, including special acts or services, benefit or affect the DISA or its subordinate activities, in accordance with 5 U.S.C. 4503, Office of Personnel Management (OPM) regulations, and DoD 1400.25-M.

E4.1.6. Enforce regulatory procedures in accordance with Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953; Executive Order 12333, "United States Intelligence Activities," December 4, 1981; and Executive Order 12968, "Access to Classified Information," August 2, 1995; and DoD Directive 5200.2, as appropriate:

E4.1.6.1. Designate any position in the DISA as a "sensitive" position.

E4.1.6.2. Authorize, in case of an emergency, the appointment of a person to a sensitive position in the DISA for a limited period of time even though a full field investigation or other appropriate investigation, including the National Agency Check, has not been completed.

E4.1.6.3. Authorize the suspension or termination, of a DISA employee in the interest of national security.

E4.1.6.4. Initiate personnel security investigations and, if necessary, in the interest of national security, suspend access to classified information for personnel assigned, detailed to, or employed by DISA. Any action under this paragraph shall be in accordance with procedures described in DoD 5200.2-R.

E4.1.7. Act as agent for the collection and payment of employment taxes imposed by Chapter 21 of the Internal Revenue Code of 1954, as amended; and, as such agent, make all determinations and certifications required or provided for under the Internal Revenue Code of 1954, as amended (26 U.S.C 3122), and the Social Security Act, as amended (42 U.S.C. 405(p)(1) and (2)), with respect to DISA employees.

E4.1.8. Authorize and approve:

E4.1.8.1. Temporary duty travel for assigned or detailed DISA military personnel in accordance with Volume 1, Joint Federal Travel Regulations, "Uniformed Service Members," current edition.

E4.1.8.2. Travel for DISA civilian personnel in accordance with Joint Travel Regulations (JTR), Volume 2, "DoD Civilian Personnel," current edition.

E4.1.8.3. Invitational travel to non-DoD persons whose consultative, advisory, or other highly specialized technical services are required in a capacity that is directly related to, or in connection with, DISA activities, in accordance with the JTR, Volume 2.

E4.1.8.4. Overtime work for DISA civilian employees in accordance with Subchapter V of Chapter 55 of 5 U.S.C. and applicable OPM regulations.

E4.1.9. Approve the expenditure of funds available for travel by assigned or detailed DISA military personnel for expenses incident to attending meetings of technical, scientific, professional, or other similar organizations when the approval of the Secretary of Defense, or a designee, is required by 37 U.S.C. 412, and 5 U.S.C. 4110 and 4111.

E4.1.10. Develop, establish, and maintain an active and continuing Records Management Program, pursuant to 44 U.S.C. 3102 and DoD Directive 5015.2.

E4.1.11. Utilize the Government purchase card for making small purchases of material and services, other than personal services, for the DISA, when it is determined more advantageous and consistent with the best interests of the Government.

E4.1.12. Authorize the publication of advertisements, notices, or proposals in newspapers, magazines, or other public periodicals as required for DISA administration and operation, consistent with 44 U.S.C. 3702.

E4.1.13. Establish and maintain appropriate property accounts for the DISA and appoint Boards of Survey, approve reports of survey, relieve personal liability, and drop accountability for DISA property contained in the authorized property accounts that has been lost, damaged, stolen, destroyed, or otherwise rendered unserviceable, in accordance with applicable laws and regulations.

E4.1.14. Promulgate the necessary security regulations for the protection of property and places under the jurisdiction of the Director, DISA, pursuant to DoD Directive 5200.8.

E4.1.15. Establish and maintain, for the functions assigned, an appropriate publications system for the promulgation of common supply and service regulations, instructions, and reference documents, and changes thereto, pursuant to the policies and procedures prescribed in DoD 5025.1-M.

E4.1.16. Enter into support and service agreements and performance-based agreements with the Military Departments, the other DoD Components, other Federal Government Agencies, and foreign governments consistent with DoD Directive 5530.3, as required for the effective performance of DISA functions and responsibilities.

E4.1.17. Exercise the authority delegated to the Secretary of Defense by the Administrator of the General Services Administration under Federal Management Regulation 102-75.1055 for the disposal of surplus personal property.

E4.1.18. Enter into and administer contracts, directly or through a Military Department, a DoD contract administration services component, or other Federal Agency, as appropriate, for supplies, equipment, and services required to accomplish the mission of the DISA. To the extent that any law or Executive Order specifically limits the exercise of such authority to persons at the Secretarial level of a Military Department, such authority shall be exercised by the appropriate Under Secretary or Assistant Secretary of Defense.

E4.1.19. Award contracts for the procurement and lease of commercial C4 capabilities.

E4.1.20. Lease property under the control of the DISA under terms that will promote the national defense or that will be in the public interest, pursuant to 10 U.S.C. 2667.

E4.1.21. Maintain an official seal and attest to the authenticity of official DISA records under that seal.

E4.2. The Director, DISA, may redelegate these authorities, as appropriate, and in writing, except as otherwise provided by law or regulation.