DoD Directive 5105.19

Defense Information Systems Agency

Originating Component:	Office of the Director of Administration and Management
Effective:	February 15, 2022
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Directive 5105.19, "Defense Information Systems Agency (DISA)," July 25, 2006
Approved by:	Kathleen H. Hicks, Deputy Secretary of Defense

Purpose: This issuance updates the mission, organization and management, administration, responsibilities and functions, relationships, and authorities of the Defense Information Systems Agency (DISA), pursuant to the authority vested in the Secretary of Defense (SecDef) by Sections 113 and 191 of Title 10, United States Code (U.S.C.).

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to OSD, the Military Departments (MILDEPs), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands (CCMDs), the Office of Inspector General of the Department of Defense (DoD IG), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

1.2. MISSION.

To conduct Department of Defense Information Network (DoDIN) operations for the joint warfighter to enable lethality across all warfighting domains in defense of the United States. The DISA plans, engineers, acquires, tests, fields, operates, and assures information-sharing capabilities, command and control (C2) solutions, and a global enterprise infrastructure to support DoD and national-level leadership.

1.3. ORGANIZATION AND MANAGEMENT.

The DISA:

a. Is established as a Defense Agency, pursuant to Section 191 of Title 10, U.S.C.

b. Is a combat support agency (CSA), pursuant to Section 193 of Title 10, U.S.C., and in accordance with DoD Directive (DoDD) 3000.06.

c. Consists of a Director, DISA, who is under the authority, direction, and control of the Chief Information Officer of the Department of Defense (DoD CIO), pursuant to Section 192 of Title 10, U.S.C. The Director, DISA exercises authority, direction, and control over DISA and all assigned resources.

d. Consists of such subordinate organizational elements established by the Director, DISA within resources assigned by the SecDef. Subordinate organizational elements include mission support organizations and various production centers. Subordinate organizations are globally dispersed, including data centers, field commands and offices, network operations centers, and support facilities.

1.4. ADMINISTRATION.

a. The Director, DISA is an active duty commissioned officer in the rank of lieutenant general or, in the case of an officer of the Navy, vice admiral. The position of Director, DISA is designated as a position of importance and responsibility pursuant to Section 601 of Title 10, U.S.C. The SecDef recommends an officer for this position to the President with the advice of the CJCS and the DoD CIO.

b. The Secretaries of the MILDEPs assign military active duty and Reserve personnel to DISA according to approved authorizations and established procedures for assignment to joint duty.

SECTION 2: RESPONSIBILITIES AND FUNCTIONS

The Director, DISA:

a. Plans, manages, and directs DISA, its subordinate elements, and all assigned resources.

b. Supports the DoD CIO with implementation of the responsibilities outlined in DoDDs 5144.02 and 8000.01 to help achieve an information advantage and full spectrum superiority, increase mission assurance, improve mission effectiveness, and realize information technology (IT) efficiencies for DoD personnel and mission partners.

c. Fulfills the responsibilities of a CSA in accordance with Section 193 of Title 10, U.S.C., including:

(1) Supporting the CJCS reporting requirement to determine DISA's readiness and responsiveness to support operating forces in the event of war or threat to national security at least every 2 years. The reporting requirement process includes the Combatant Commanders (CCDRs) and the Secretaries of the MILDEPs.

(2) Participating in the joint and deliberate planning processes, joint training exercises, and joint assessments to ensure DISA can perform support missions during war or threats to national security. Receiving CJCS performance assessments of joint training and implementing any guidance in accordance with DoDD 3000.06.

d. Exercises the authority and fulfills the responsibilities and functions applicable to its designation as a CSA, in accordance with DoDD 3000.06, including:

(1) Extending the Defense Information Systems Network (DISN), data centers, and enterprise services to support requests from CCDRs and their DoD contingency operations around the world.

(2) Supporting CCMD planning focused on developing and implementing technical solutions to close joint capability gaps identified through the Joint Capabilities and Integration Development System process.

(3) Contributing to readiness and mission assurance assessments.

(4) Deploying DISA capabilities, including personnel and equipment, to a CCDR area of responsibility in response to validated CCMD requests for support and deployment authorization by the SecDef.

e. Exercises authority, direction, and control over the Joint Service Provider for the Pentagon Reservation and DoD organizations in the National Capital Region, in accordance with the May 1, 2015 Deputy Secretary of Defense Memorandum.

f. As applicable, provides budget, staffing, contracting, programmatic, and administrative support for the White House Communications Agency, the Joint Force Headquarters-Department of Defense Information Network, the Joint Artificial Intelligence Center, the White House Situation Room Support Staff, and SecDef Communications.

g. Supports, on a reimbursable basis, DoD Component requests for mission partner use of DISA-provided enterprise services where the request is approved by the DoD CIO, in accordance with DoD Instruction (DoDI) 8010.01.

h. Develops and executes DISA programs and budgets necessary to achieve national defense objectives, and provides day-to-day management of resources under DISA control, in accordance with the DoD Planning, Programming, Budgeting, and Execution process, as described in DoDD 7045.14.

i. For communications:

(1) Provides:

(a) IT and communications services to the President, Vice President, and National Security Council staff, and provides support for White House communications requirements for the National Security Council, including the White House Situation Room.

(b) Fixed and mobile telecommunications support for the United States Secret Service, in accordance with DoDD 3025.13.

(c) Continuity of communications and support for the national security and emergency preparedness telecommunications functions of the National Security and Emergency Preparedness Communications Executive Committee, as described in Executive Order (E.O.) 13618.

(d) DoD information enterprise transport through a robust combination of terrestrial, mobile, line-of-sight, undersea, and satellite services.

(e) Operation of the Department of Defense Domain Name System (.MIL) for DoD Networks. Serves as the registrar for .MIL and maintains the .MIL registration database. Oversees public internet access to .MIL to support E-Government responsibilities of the DoD, in accordance with Public Law 107-347, also known as the E-Government Act of 2002. Manages domain name registration and Internet Protocol address allocation on an enterprise basis to promote interoperability and security.

(2) Defines system performance criteria for military satellite communications (SATCOM) terrestrial gateways and, through coordination with the DoD Components, develops and performs general systems engineering to achieve a long-term, interoperable, and cyberspace resilient mission-capable system.

(3) Executes continuity of operations planning responsibilities, in accordance with DoDD 3020.26 and DoDI 3020.42, and provides continuity of operations in accordance with Presidential Policy Directive 40.

(4) Supports the DoD CIO in the execution of responsibilities for select National Leadership Command Capability (NLCC) systems, which will be determined through synchronization with other relevant stakeholders within the NLCC community and the Council on Oversight of the National Leadership Command, Control, and Communications System.

j. For operation, maintenance, and security of the DISA portion of the DoDIN:

(1) Executes DoDIN operations and defensive cyberspace operations-internal defensive measures on DISA-managed elements of the DoDIN. Takes necessary action to isolate, disconnect, and shutdown information systems (including websites) on the DoDIN posing a threat or potential threat to operations and security of the DoDIN, in support of the Commander, United States Cyber Command (USCYBERCOM), consistent with DoDIs 8010.01 and 8510.01.

(2) Plans, engineers, tests, procures, operates, secures, maintains, and manages DISN capabilities and their access points and boundary protections to meet DoD mission requirements for end-to-end interoperability through technical refreshes, technical evolution, and sustainment.

(3) Provides network operations for DoD-wide operational, organizational, and technical capabilities for operating and defending the DISN.

(4) Executes defensive cyberspace operations-internal defensive measures to secure the DISN and DISN services from cyberspace intrusion, exploitation, and exfiltration.

(5) Operates and evolves a cybersecurity service provider program to service the DoD, in accordance with DoDI 8530.01.

(6) Executes C2 to operate and defend DISA's portion of the DoDIN for networks and network services, computing, enterprise services, cybersecurity, senior leadership communications, warfighting C2 communications, and information-sharing capabilities.

(7) Provides situational awareness to make informed C2 decisions by tracking network incidents, outages, anomalies, and intelligence, for example, in support of OSD, Joint Staff, CCMDs, and MILDEPs. Network operations and SATCOM situational awareness is obtained through the operational and technical integration of enterprise management and defensive actions and activities across all levels of command, in accordance with DoDIs 8410.02 and 8420.02.

(8) Provides critical time dissemination services to meet system timing requirements throughout the DoDIN, in accordance with CJCS Instruction 6130.01G.

(9) Provides engineering, architecture, and provisioning support for integrated DoDIN operations, including enterprise management, content management, and mission assurance, in accordance with Joint Publication 3-12.

k. For cybersecurity:

(1) Plans, engineers, acquires, tests, and fields enterprise cybersecurity capabilities to support DoD mission requirements.

(2) Integrates cybersecurity activities into DISA operations; acquisition programs; acquisition of systems and services containing IT; and exercises, plans, doctrine, strategies, policies, and architectures. Conducts and reports cybersecurity activities in accordance with DoDD 5240.06 and DoDIs 5000.82, 8500.01, 8510.01, and 8530.01.

(3) Supports the DoD CIO to:

(a) Achieve DoD cybersecurity, in coordination with the CJCS; the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS); the Director, Defense Intelligence Agency; and the Commander, USCYBERCOM, in accordance with DoDI 8500.01. This support focuses on the implementation of a cybersecurity program that integrates the enterprise cybersecurity capabilities of personnel, operations, and technology and supports the evolution of DoDIN operations with specific attention on the performance of tasks identified in DoDIs 8530.01 and 8500.01.

(b) Develop guidance and oversight processes for the recruiting, retention, training, and professional development of the DoD IT and cybersecurity workforce in accordance with DoDD 8140.01.

(c) Establish an overarching enterprise security architecture that provides for tiered cyber defenses to protect DoD systems, information, and data from cyber threats.

(d) Develop or acquire solutions that support cybersecurity objectives for use throughout DoD.

(e) Develop cybersecurity guidance and processes to support the secure implementation of DoD cybersecurity policies, standards, and architectures, in accordance with DoDI 8500.01.

(f) Collect and make available cybersecurity data for analysis and management.

(4) Develops strategic and tactical cyberspace resilient information architecture as an integral part of the overall joint architecture, in coordination with the DIRNSA/CHCSS; the Commander, USCYBERCOM; and the Secretaries of the MILDEPs, in accordance with DoDIs 8523.01 and 8500.01.

(5) Oversees the mission assurance office of primary responsibility for both the DoDIN and cyberspace capability supply chain risk management, and executes responsibilities, in accordance with DoDD 3020.40 and DoDI 5200.44.

(6) Collaborates with other DoD Component heads to defend the DoDIN, and supports the CCDRs and deployed forces by designing and implementing proactive protections, deploying attack detection, and performing other security functions to support cyberspace resiliency.

l. For cloud, computing, and storage services:

(1) Provides a set of consolidated and interconnected core computing centers that deliver secure, defendable, and resilient on-demand services, including cloud-based web services,

production support, technical services, and end-user assistance for C2, combat support, and business functions to all DoD users and devices throughout the DoD.

(2) Delivers an assured cloud-computing environment at multiple classification levels capable of ensuring continued mission execution in the face of persistent threats.

(3) Plans, engineers, tests, procures, operates, secures, maintains, and manages cloud capabilities, their access points, and boundary protections to meet DoD mission requirements for end-to-end interoperability through technical refreshes, technical evolution, and sustainment.

(4) Supports the DoD CIO by authoring and maintaining the Cloud Computing Security Requirements Guides and Tenant Configuration Guides for the DoD.

(5) Provides high-speed network connectivity from the DoDIN to the various commercial cloud providers authorized by a DoD Provisional Authority to process DoD data.

(6) Provides government cybersecurity services for DoD and commercial cloud initiatives. Executes Defensive Cyberspace Operations-Internal Defensive Measures to secure the cloud and cloud services from cyberspace intrusion, exploitation, and exfiltration. Responsible for coordinating and maintaining information sharing with the commercial cloud service providers and USCYBERCOM to address, mitigate, and resolve cybersecurity threats that transit between the cloud environments and the DoDIN.

m. For enterprise services:

(1) Provides:

(a) Ordering and fulfillment services to deliver IT and communications services for the DoD Components.

(b) Enterprise applications, foundational services, core mission services, cybersecurity services, data services, and associated infrastructure commonly used across the DoD Components that provide optimized and integrated enterprise service offerings enabling DoD-wide efficiencies, effectiveness, and improved responsiveness to dynamic joint and coalition mission partner needs.

(c) IT enterprise services to the DoD Components, in accordance with DoDDs 5144.02 and 5205.07, DoDI 5205.11, and the DoD CIO DoD Special Access Program IT Programs Strategy 2017-2022.

(2) Develops, integrates, operates, and sustains secure and operationally resilient core enterprise services; issues guidance and sets standards for the development, testing, and implementation of enterprise services and other enterprise service-related tools and infrastructure for the DoD.

(3) Defines system performance criteria for DISA-engineered, -designed, -acquired, -tested, and -managed DoD information enterprise systems through coordination with the DoD Components. Develops and performs general systems engineering to achieve a long-term,

interoperable, secure, and cyberspace resilient mission-capable system. Analyzes DoD information systems and services regarding performance under benign and cyberspace threat conditions, as well as their associated plans, programs, and budgets, to identify areas of deficiency, and makes recommendations or initiates corrective action, as appropriate.

n. For C2 capabilities, in accordance with DoDD 3700.01 and DoDI 5000.02:

(1) Leads system engineering support to sustain and modernize the DoD information enterprise that supports DoD C2 enabling capabilities.

(2) Ensures system integration, interoperability, and standardization of DoD C2 capabilities among the DoD Components.

(3) Provides:

(a) IT capabilities in support of the DoD's deliberate planning, crisis action planning, resource allocation, program execution, and global force management processes and C2 mission.

(b) Management advice and technical services for the design, development, deployment, and evolution of CCMD center systems, to include support for the National Military Command System and supporting communications.

(c) Centralized management and configuration control of select National Leadership Command, Control, and Communications System and National Military Command System C2 capabilities as directed by the DoD CIO and Council on Oversight of National Leadership Command, Control, and Communications Systems.

o. For NLCC:

(1) Plans, engineers, programs, budgets, finances, executes, installs, implements, operates, sustains, modernizes, and manages the configuration for select NLCC systems in coordination with the DoD CIO, including continuity of government communications, in accordance with Presidential Policy Directive 40.

(2) Adheres to communications requirements and continuity policy, as directed by the Under Secretary of Defense for Policy.

p. Regarding plans, programs, budgets, finances for DoD IT modernization and reform, designs, develops, implements, operates, and sustains:

(1) Network and service optimization reform initiatives (e.g., Joint Service Provider and Fourth Estate Network Optimization), in accordance with DoD strategies (e.g., the DoD Cyber Strategy, DoD Digital Modernization Strategy, and the National Defense Business Operations Plan), including selling supplies integral to the provision of computing and telecommunications services.

(2) Cloud and Data Center optimization reform initiatives, enterprise collaboration, and IT tools reform initiatives, in accordance with the DoD Digital Modernization Strategy and the National Defense Business Operations Plan.

q. For joint interoperability, testing, and standards:

(1) Develops integrated architectures based on the DoD architectural framework and provides systems engineering support for command, control, and communications (C3) and cyberspace capabilities.

(2) Provides IT standards, testing, and evaluation for standards conformance and joint interoperability. Conducts radio waveform standards conformance testing and serves as the radio waveform standards conformance certification authority.

(3) Serves as the DoD authority for certifying the interoperability of IT systems, including National Security Systems, and evaluates and certifies joint, multinational, and interagency IT interoperability, consistent with DoDIs 8100.04 and 8330.01, through the Joint Interoperability Test Command.

(4) Maintains an independent operational test agency to adequately plan, execute, and report on operational test and evaluation, in accordance with DoDI 5000.89.

(5) Oversees IT standards for DoD and integrates DoD information systems and networks serving both U.S. and authorized foreign partners. Organizes, chairs, and participates in U.S. military and commercial IT standards bodies to develop, publish, and maintain established and developmental interoperability standards, in accordance with DoDI 8310.01. Represents DoD interests in Federal, nongovernmental, international, and allied IT standards bodies, consistent with the guidance of the DoD CIO.

(6) Maintains the DoD IT Standards Registry, which can be accessed online through DISA's Global Information Grid Technical Guidance Federation using DISA's homepage.

(7) Participates with the DoD CIO in the development of DoD IT enterprise architecture products, including reference design, reference architectures, and solution architectures.

r. For electromagnetic spectrum operations:

(1) Develops integrated spectrum plans and strategies, in coordination with the DoD CIO, the CJCS, the CCDRs, and the Secretaries of the MILDEPs to develop and maintain joint electromagnetic spectrum operations architectures to address current and future needs for DoD electromagnetic spectrum operational access.

(2) Provides spectrum operations and management support to the DoD CIO, the CJCS, the CCDRs, the Secretaries of MILDEPs, and the Directors of the Defense Agencies.

(3) Provides engineering support and acquisition advice to the DoD CIO for the analysis of spectrum-dependent system technology, including new and emerging spectrum technologies

that improve the Department's ability to be agile, effective, and efficient within the electromagnetic spectrum.

(4) Establishes and maintains the capability to perform required electromagnetic compatibility analyses and studies to support effective use of the spectrum-dependent systems in electromagnetic environments and accomplish national security and military objectives, in accordance with DoDIs 3222.03, 4650.01, and 8330.01.

(5) Develops, maintains, and enhances DoD joint enterprise spectrum management information systems and components, including data capture of DoD spectrum management and operations-related information into the Joint Spectrum Data Repository, and other analytical tools and capabilities accessible to DoD and OSD Components for information sharing, in accordance with DoDI 8320.05.

(6) Provides engineering, regulatory, and legislative support to the DoD CIO on national and international spectrum issues.

(7) Provides, as directed by the DoD CIO, representation to national and international spectrum organizations, bodies, and forums, including treaty level delegations and bilateral and multinational processes, as appropriate.

(8) Supports DoD CIO in the development and coordination of DoD positions and technical work as part of the U.S. preparatory process for the International Telecommunication Union Study Groups leading up to the World Radiocommunication Conference (WRC) engagements and participates in other international spectrum forums. Provides a DoD enterprise-level collaboration and risk reporting capability in support of the DoD WRC preparatory process. Assists DoD in conducting mission capabilities spectrum risk assessments, international outreach and coalition building, North Atlantic Treaty Organization WRC preparatory process and position development in accordance with DoDI 4650.01.

(9) Supports the DoD CIO in the development of DoD national and international satellite registration, coordination processes, policies, and activities impacting DoD satellites, and represents the DoD at national and international satellite coordination forums. Coordinates, as necessary, with the Assistant Secretary of Defense for Space Policy through the DoD CIO.

s. For acquisition and procurement:

(1) Streamlines acquisition and contracting processes to support the DoDIN enterprise.

(2) Implements acquisition and procurement best practices that allow for agility in development and rapid deployment of capabilities to the warfighter.

(3) Effectively researches, identifies, acquires, tests, and delivers commercial advanced technology and services in support of DISA IT systems and operations when most advantageous and cost effective.

(4) Provides tailored acquisition and procurement policies, processes, procedures, tools, products, life-cycle oversight, and a qualified workforce that acquires quality products and services to satisfy user needs and provide improvements to mission capabilities.

(5) Procures IT solutions for requirements accepted by the Defense Information Technology Contracting Organization, which include IT equipment and services, cyberspace technology such as fiber optics, long-haul telecommunications, and testing requirements in support of mission objectives.

(6) Coordinates, as necessary, on acquisition matters with the Under Secretary of Defense for Acquisition and Sustainment, through the DoD CIO.

t. Performs DoD SATCOM program management activities in accordance with DoDI 8420.02, including enterprise SATCOM management and control capability development, integration, and hosting, and SATCOM gateway modernization, sustainment, and synchronization. Coordinates, as necessary, with the Assistant Secretary of Defense for Space Policy through the DoD CIO.

u. Uses existing systems, facilities, and services of the DoD or other Federal departments and agencies, when possible, to achieve maximum efficiency and economy.

v. Participates, as appropriate, in the periodic review of Defense Agencies and DoD Field Activities, in accordance with Section 192(c) of Title 10, U.S.C.

w. Designs and manages DISA programs and activities to improve performance, economy, and efficiency, with particular attention to the requirements of DISA's organizational customers, internal and external to the DoD.

x. Performs other duties as assigned by the SecDef or the DoD CIO.

SECTION 3: RELATIONSHIPS

3.1. DIRECTOR, DISA.

Under the authority, direction, and control of the DoD CIO, the Director, DISA:

a. Reports directly to the DoD CIO.

b. As the Commander, Joint Force Headquarters-Department of Defense Information Network, serves under the operational control of the Commander, USCYBERCOM, pursuant to the November 13, 2014 CJCS Execute Order.

c. Maintains appropriate liaison with the other DoD Components, OSD Components, agencies, and departments of the Executive Branch; State and local government organizations; foreign governments; and international organizations to exchange information and integrate efforts on programs and activities related to assigned responsibilities. Communications with foreign governments with the purpose of entering into international agreements must be coordinated with the General Counsel of the Department of Defense and be conducted in accordance with DoDI 5530.03.

d. Provides advice and technical support to the DoD CIO, including representation to international and North Atlantic Treaty Organization forums, as well as the DoD CIO Executive Board and the Digital Modernization Infrastructure Executive Committee, as directed by the DoD CIO.

e. Coordinates with:

(1) The DIRNSA/CHCSS on all National Security Directive 42 matters.

(2) The Director, Defense Intelligence Agency on systems engineering and cybersecurity-related responsibilities of the Joint Worldwide Intelligence Communications System, DoD intelligence information systems, and non-cryptographic Sensitive Compartmented Information systems.

f. Supports Commander, USCYBERCOM orders and directives when securing, operating, and defending all DISA elements of the DoD information enterprise, providing C2 for DISA network operations centers.

g. Manages and collaborates with all organizational customers who receive DISA products and services in accordance with DISA's Defense Working Capital Fund processes.

3.2. DOD CIO.

In addition to Paragraph 3.4., the DoD CIO:

a. Provides guidance and direction to the Director, DISA on policies, programs, and procedures related to the development and operation of the networks, C3, enterprise-wide integration of DoD information matters, network operations, cybersecurity, electro-magnetic spectrum, and IT systems, services, and capabilities provided by the DISA.

b. Consults with the CJCS to obtain recommendations and develop guidance and direction for DISA to ensure all services and capabilities provided are operated and maintained at levels that meet the operational readiness and warfighting requirements of the CCDRs.

c. Provides guidance and direction to the Director, DISA as required to implement statutory and regulatory responsibilities.

3.3. CJCS.

In addition to Paragraphs 3.4. and 3.7., the CJCS:

a. Communicates directly with the Director, DISA regarding CSA matters.

b. Leads development of operational requirements for the layered protection of the DoD-wide elements of the DoD information enterprise as inputs to the DoD CIO and Commander, USCYBERCOM, for cybersecurity protective measures, tools, and capabilities.

c. Reviews and assesses the responsiveness and readiness of DISA to support operating forces in the event of war or threats to national security and makes recommendations, in accordance with Section 193 of Title 10, U.S.C., and the Unified Command Plan. Facilitates communications with the CCDRs to improve DISA support for the CCMDs.

d. Provides IT standards advice, support, and representation, in accordance with DoDI 8310.01.

e. Helps the DoD CIO develop guidance for the Director, DISA and the CCDRs to serve as the basis for interrelationships among these organizations.

f. Reviews and provides recommendations on the DISA military workforce program to the DoD CIO, as appropriate.

g. Advises the SecDef, in coordination with the DoD CIO, on behalf of the CCDRs, on C3 and cyberspace capabilities requirements and priorities fulfilled by DISA.

h. Provides to the Director, DISA, support and logistical planning information that affects the responsibilities and functions assigned to the Director, DISA.

3.4. OSD PRINCIPAL STAFF ASSISTANTS AND DOD COMPONENT HEADS.

The OSD Principal Staff Assistants and DoD Component heads coordinate with the Director, DISA on matters under their purview related to the authorities, responsibilities, and functions assigned to the Director, DISA.

3.5. CCDRS.

In addition to Paragraphs 3.4., and 3.7., the CCDRs advise and coordinate with the Director, DISA on plans, policies, intelligence, and decisions to synchronize the development of DoDIN requirements, and articulate CCMD requirements that affect DISA elements of the DoDIN.

3.6. COMMANDER, USCYBERCOM.

In addition to Paragraphs 3.4., 3.5., and 3.7., the Commander, USCYBERCOM:

a. Articulates USCYBERCOM requirements to enable DISA to plan and program resources adequately.

b. Collaborates with the Director, DISA to develop the appropriate concept of operations and supporting tactics, techniques, and procedures for DISA support to cyberspace operations.

c. Serves as the operational lead for the full spectrum of cyberspace operations coordinating and directing DoDIN operations and defense.

3.7. DOD COMPONENT HEADS.

In addition to Paragraph 3.4., the DoD Component heads:

a. Advise the Director, DISA of funding requirements for effective operations, maintenance, and scheduled implementation of new subsystems or projects.

b. Coordinate with the Director, DISA on all program activities that include or are related to C3 and cyberspace capabilities. Provide programmatic documents and technical specifications to DISA for prior review and coordination for all C3 and cyberspace capabilities for which DISA has execution, review, development, integration, testing, or support responsibilities. Obtain Director, DISA concurrence for programmatic or technical changes affecting funding or interoperability of C3 and cyberspace capabilities for which DISA has primary responsibility. To facilitate collaboration with DISA:

(1) Provide for review, and approval before execution, of the technical specifications and standards and related contract management requirements impacting configuration, cost, performance, or schedules for all systems for which DISA is responsible.

(2) Coordinate with the Director, DISA on draft acquisition plans and request DISA representation on source selection activities that impact systems for which DISA is responsible.

c. Identify requirements for DISA support for networks, telecommunications, IT systems, services, defensive cybersecurity operations, and capabilities to the Director, DISA. As appropriate, provide planning, programming, and budgeting support. Enable adequate preparation of doctrine, organization, training, material, leadership, personnel, and facilities to support fielding capabilities or services.

3.8. DIRNSA/CHCSS.

In addition to Paragraphs 3.4. and 3.7., the DIRNSA/CHCSS:

a. Provides foreign signals intelligence and cybersecurity products and services to support DISA and its subordinate elements to accomplish their assigned mission.

b. Provides technical expertise on boundary defense of the DoDIN, emerging threats, and the integration of new cyberspace defense capabilities.

c. Maintains a liaison to facilitate vital information exchange, coordinate actions, and partner on innovations to attain mission success.

SECTION 4: AUTHORITIES

The Director, DISA is delegated authority as described in this section.

4.1. GENERAL AUTHORITIES.

a. Communicate directly with the other DoD Component heads and OSD Component heads, as necessary, to carry out assigned responsibilities and functions, including the transmission of requests for advice and assistance. Communications to the MILDEPs must be transmitted through the Secretaries of the MILDEPs, their designees, or as otherwise provided in law or directed by the SecDef in other DoD issuances. Communicating to the CCDRs must be in accordance with DoDD 5100.01 or as otherwise stipulated in this directive.

b. Communicate with other Federal agencies and government officials, State and local officials, members of the public, and representatives of foreign governments, as appropriate, and pursuant to DoD policy, to carry out assigned responsibilities and functions. Communications with representatives of the Legislative Branch must be conducted through the Office of the Assistant Secretary of Defense for Legislative Affairs, except for communications with defense appropriations committees, which must be coordinated through the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense, and consistent with the DoD Legislative Program.

c. Obtain reports and information consistent with DoDI 8910.01, as necessary, to carry out assigned responsibilities and functions.

d. Direct, administer, and provide services to foreign governments under foreign military sales, in accordance with Sections 2151, et seq., and 2751, et seq., of Title 22, U.S.C., and the Defense Security Cooperation Agency Manual 5105.38-M.

e. Approve conferences, in accordance with the June 26, 2016 Assistant Deputy Chief Management Officer Memorandum.

f. Nothing in this issuance should infringe on DoD IG statutory independence and authority as articulated in Title 5, U.S.C., Appendix, also known as "the Inspector General Act of 1978, as amended." In the event of any conflict between this issuance and the Office of DoD IG statutory independence and authority, the Inspector General Act of 1978, as amended, takes precedence.

4.2. HUMAN RESOURCES.

a. Exercise the powers vested in the SecDef by Sections 301, 302(b), 3101, and 5107 of Title 5, U.S.C., and Chapter 81 of Title 10, U.S.C., as amended, on the employment, direction, and general administration of DISA civilian personnel.

b. Fix rates of pay for wage-grade employees exempted from Chapter 51 of Title 5, U.S.C., also known as "The Classification Act of 1949," by Section 5102 of Title 5, U.S.C., on the basis of rates established pursuant to the Federal wage system.

c. Administer oaths of office to those entering the DoD, or any other oath required by law in connection with employment therein, in accordance with Section 2903 of Title 5, U.S.C., and designate in writing, as necessary, officers and employees of DISA to perform this function.

d. Establish the DISA Incentive Awards Board and authorize cash awards to, and incur necessary expenses for the honorary recognition of, civilian employees of the U.S. Government whose suggestions, inventions, superior accomplishments, or other personal efforts, including special acts or services, benefit or affect DISA, or its subordinate activities, pursuant to Section 4503 of Title 5, U.S.C., applicable Office of Personnel Management regulations, and Volume 451 of DoDI 1400.25.

e. Use advisory committees and employ temporary or intermittent experts or consultants, as approved by the SecDef or the Director of Administration and Management, for the performance of Director, DISA responsibilities and functions, consistent with Sections 173 and 174 of Title 10, U.S.C.; Section 3109 of Title 5, U.S.C.; Section 2 of the Appendix of Title 5, U.S.C.; and DoDIs 5105.04 and 5105.18.

f. Authorize and approve:

(1) Travel for military and civilian personnel assigned or detailed to DISA, in accordance with Joint Travel Regulations.

(2) Invitational travel for non-DoD personnel 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 Joint Travel Regulations.

(3) Overtime work for DISA civilian personnel, in accordance with Section 5542 of Title 5, U.S.C., and Parts 550 and 551 of Title 5, Code of Federal Regulations.

(4) The expenditure of funds available for travel by military personnel, assigned or detailed to DISA, for expenses incident to attending meetings of technical, scientific, professional, or other similar organizations when the approval of the SecDef or a designee is required by Section 455 of Title 37, U.S.C.

(5) Waivers of indebtedness for DISA employees, in accordance with Section 5584 of Title 5, U.S.C.

4.3. SECURITY.

a. Designate positions within DISA using the Defense Counterintelligence and Security Agency Position Designation Automated Tool. All positions will be assigned a designation using the criteria found in Parts 731 and 732 of Title 5, Code of Federal Regulations and DoDI 5200.02, and will be documented in the Defense Civilian Personnel Data System, or other authorized DoD automated system. The Position Designation Automated Tool will be used to help assign a position designation and to identify the background investigation required of the position.

b. Establish and maintain an effective suitability and fitness determination program, in accordance with Volume 731 of DoDI 1400.25 and DoDI 1402.05.

c. Provide funding to cover requirements for personnel security investigations, adjudication, and recording of results to comply with the DoD Personnel Security Program.

d. Enforce requirements for prompt reporting of significant derogatory information, unfavorable administrative actions, and adverse actions to the appropriate personnel security, human resources, and counterintelligence official(s), as appropriate.

e. In accordance with E.O.s 10450, 12333, and 12968, and DoDI 5200.02, as appropriate:

(1) In exceptional circumstances where official functions must be performed before the completion of an investigation and adjudication process, authorize temporary access to a sensitive position in DISA for a limited period to individuals for whom an appropriate investigation has not been completed.

(2) Initiate personnel security investigations and, if necessary, in the interest of national security, suspend security access to classified information for personnel assigned, detailed to, or employed by DISA. Any action under this paragraph will be in accordance with procedures prescribed in DoD Manual (DoDM) 5200.02.

(3) Grant interim clearances for up to Top Secret eligibility and access to classified information when the requirements of DoDM 5200.02 have been met.

(4) In the interest of national security, and if necessary, suspend or terminate personnel assigned to, detailed to, or employed by DISA. Any actions pursuant to this paragraph must be taken in accordance with procedures in DoDM 5200.02.

f. Protect the security of DISA installations, activities, property, information, and personnel by appropriate means including the publication of necessary security regulations, in accordance with DoDIs 5200.01 and 5200.08.

g. Establish and maintain an insider threat program to comply with the requirements and minimum standards of DoDD 5205.16, to prevent, deter, detect, and mitigate the threat insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources.

h. Exercise responsibility for the generation, receipt, custody, distribution, safeguard, disposition or destruction, and accounting of communications security material entrusted to DISA's communications security account, in accordance with DoDI 8523.01 and other applicable DoD issuances and Federal laws.

4.4. PUBLICATIONS AND RECORDS.

a. Authorize the publication of advertisements, notices, or proposals in newspapers, magazines, internet publications, or other public periodicals, as required for the effective administration and operation of DISA, pursuant to Section 3702 of Title 44, U.S.C.

b. Establish and maintain, for the functions assigned, an appropriate publications system for the publication of DISA regulations, instructions, and reference documents, and changes thereto, similar to the policies and procedures prescribed in DoDI 5025.01.

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

d. Develop, establish, and maintain an active and continuing records management program, pursuant to Section 3102 of Title 44, U.S.C., and DoDI 5015.02.

4.5. ACQUISITION, PROCUREMENT, FINANCIAL MANAGEMENT, AND PROPERTY.

a. Enter into interdepartmental and intragovernmental support agreements, as the receiver or the supplier, with the other DoD Components, OSD Components, non-DoD Federal Government departments and agencies, and, to the extent permitted by law, State and local governments and non-Federal entities, as required for the effective performance of Director, DISA responsibilities and functions, in accordance with Section 1535 of Title 31, U.S.C., and DoDI 4000.19.

b. Enter into and administer contracts, directly or through a MILDEP, DoD contract administration services component, or other Federal agency, as appropriate, for supplies, equipment, and services required to accomplish the mission of DISA. To the extent that any law or E.O. specifically limits the exercise of such authority to persons at the secretarial level of a MILDEP, the appropriate Under Secretary or Assistant Secretary of Defense must exercise such contracts.

c. Exercise the delegated roles and responsibilities that are assigned to the Head of Contracting Activity and, if desired, re-delegate them to the official who is responsible for the selection and appointment of contracting officials, in accordance with the April 4, 2017 Director of Defense Procurement and Acquisition Policy Memorandum.

d. Exercise the acquisition program responsibilities of the component acquisition executive, as described in DoDI 5000.02, for DISA acquisition programs.

e. Establish and maintain appropriate property accountability for DISA and appoint boards of survey, approve reports of survey (or financial liability investigations of property loss), relieve personal liability, and drop accountability for DISA property contained in the authorized property accounts for property that has been lost, damaged, stolen, destroyed, or otherwise rendered unserviceable, in accordance with applicable laws and regulations.

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

g. Use the Government-Wide Purchase Card for making appropriate purchases of material and services, other than personal services, for DISA when it is determined more advantageous than other means of payment and consistent with the best interests of the U.S. Government.

GLOSSARY

ACRONYM	MEANING
C2	command and control
C3	command, control, and communications
CCDR	Combatant Commander
CCMD	Combatant Command
CJCS	Chairman of the Joint Chiefs of Staff
CSA	combat support agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD CIO	Chief Information Officer of the Department of Defense
DoDD	DoD directive
DoDI	DoD instruction
DoD IG	Inspector General of the Department of Defense
DoDIN	Department of Defense Information Network
DoDM	DoD manual
E.O.	Executive order
EXORD	execute order
IT	information technology
MILDEP	Military Department
NLCC	National Leadership Command Capability
SATCOM	satellite communications
SecDef	Secretary of Defense
U.S.C.	United States Code
USCYBERCOM	United States Cyber Command
WRC	World Radiocommunication Conference

REFERENCES

Assistant Deputy Chief Management Officer Memorandum, "Department of Defense Conference Guidance, Version 4.0," June 26, 2016

Chairman of the Joint Chiefs of Staff Instruction 6130.01G, "2019 Chairman of the Joint Chiefs of Staff Master Positioning, Navigation, and Timing Plan," current version[1]

Chief Management Officer, "FY2018-FY2022 National Defense Business Operations Plan," April 9, 2018

Code of Federal Regulations, Title 5

Defense Information Systems Agency, "DoD Cloud Computing Security Requirement Guide," March 6, 2017

Defense Security Cooperation Agency Manual 5105.38-M, "Security Assistance Management Manual (SAMM)," April 30, 2012, as amended

Deputy Secretary of Defense Memorandum, "Consolidation of Pentagon Information Technology Operations," May 1, 2015

Director of Defense Procurement and Acquisition Policy Memorandum, "Designation for the Selection and Appointment of Contracting Officers to the Head of the Contracting Authority," April 4, 2017

DoD Chief Information Officer "Special Access Program Information Technology Programs Strategy 2017-2022," March 2017[2]

DoD Cyber Strategy, August 30, 2018[3]

DoD Digital Modernization Strategy, "DoD Information Resource Management Strategic Plan FY 19-23," July 12, 2019

DoD Directive 3000.06, "Combat Support Agencies (CSAs)," June 27, 2013, as amended

DoD Directive 3020.26, "DoD Continuity Policy," February 14, 2018

DoD Directive 3020.40, "Mission Assurance (MA)," November 29, 2016, as amended

DoD Directive 3025.13, "Employment of DoD Capabilities in Support of the U.S. Secret Service (USSS), Department of Homeland Security (DHS)," October 8, 2010, as amended

DoD Directive 3700.01, "DoD Command and Control (C2) Enabling Capabilities," October 22, 2014, as amended

DoD Directive 5100.01, "Functions of the Department and Its Major Components," December 21, 2010, as amended

---

[1] The current version of CJCSI 6130.01 is accessible at the limited access (CAC-protected) Joint Staff directory at: https://jsportal.sp.pentagon.mil/sites/Matrix/DEL/CJCSJS%20Directives%20Limited/Forms/Instr_CJCSJS.aspx

[2] For access to this document, please contact osd.pentagon.dod-cio.mbx.cio-sap@mail.mil

[3] For access to this document, please contact the Office of Cyber Policy in the Office of the Under Secretary of Defense for Policy. An unclassified summary is available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010, as amended

DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, as amended

DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended

DoD Directive 7045.14, "The Planning, Programming, Budgeting, and Execution (PPBE) Process," January 25, 2013, as amended

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016, as amended

DoD Directive 8140.01, "Cyberspace Workforce Management," October 5, 2020

DoD Information Technology Standards Registry, current version[4]

DoD Instruction 1400.25, Volume 451, "DoD Civilian Personnel Management System: Awards," November 4, 2013

DoD Instruction 1400.25, Volume 731, "DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees," August 24, 2012

DoD Instruction 1402.05, "Background Checks on Individuals in DoD Child Care Services Programs," September 11, 2015, as amended.

DoD Instruction 3020.42, "Defense Continuity Plan Development," February 17, 2006

DoD Instruction 3222.03, "DoD Electromagnetic Environmental Effects (E3) Program," August 25, 2014, as amended

DoD Instruction 4000.19, "Support Agreements," December 16, 2020

DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," January 9, 2009, as amended

DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," January 23, 2020

DoD Instruction 5000.82, "Acquisition of Information Technology," April 21, 2020

DoD Instruction 5000.89, "Test and Evaluation," November 19, 2020

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5025.01, "DoD Issuances Program," August 1, 2016, as amended

DoD Instruction 5105.04, "Department of Defense Federal Advisory Committee Management Program," August 6, 2007

DoD Instruction 5105.18, "DoD Intergovernmental and Intragovernmental Committee Management Program," July 10, 2009, as amended

---

[4] The current version of the DoD Information Technology Standards Registry is accessible at DISA's limited access (CAC-protected) Global Information Grid Technical Guidance Federation at https://gtg.csd.disa.mil/uam/homepage.do.

DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended

DoD Instruction 5200.02, "DoD Personnel Security Program (PSP)," March 21, 2014, as amended

DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005, as amended

DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012, as amended

DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPS)," February 6, 2013, as amended

DoD Instruction 5530.03, "International Agreements," December 4, 2019

DoD Instruction 8010.01, "Department of Defense Information Network (DODIN) Transport," September 10, 2018

DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," December 9, 2010

DoD Instruction 8310.01, "Information Technology Standards in the DoD," February 2, 2015, as amended

DoD Instruction 8320.05, "Electromagnetic Spectrum Data Sharing," August 18, 2011, as amended

DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014, as amended

DoD Instruction 8410.02, "NetOps for the Global Information Grid (GIG)," December 19, 2008

DoD Instruction 8420.02, "DoD Satellite Communications," November 25, 2020

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

DoD Instruction 8523.01, "Communications Security," January 6, 2021

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

DoD Instruction 8910.01, "Information Collection and Reporting," May 19, 2014, as amended

DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017, as amended

Execute Order from the Chairman of the Joint Chiefs of Staff, "Modification (MOD) to EXORD to Implement Cyberspace Operations Command and Control (C2)," 141627Z November 13, 2014[5]

Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953, as amended

[5] CJCS EXORD can be found on Intelink at: https://intelshare.intelink.sgov.gov/sites/jointstaff/j3/ddgo/cod/Cyber%20C2%20Documents/Forms/Allitems.aspx

Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
Executive Order 12968, "Access to Classified Information," August 2, 1995, as amended
Executive Order 13618, "Assignment of National Security and Emergency Preparedness Communications Functions," July 6, 2012
Joint Publication 3-12, "Cyberspace Operations," June 8, 2018
Joint Travel Regulations, current edition
National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990
Presidential Policy Directive 40, "National Continuity Policy," July 15, 2016
Public Law 107-347, "E-Government Act of 2002," December 17, 2002
Unified Command Plan, as amended
United States Code, Title 5
United States Code, Title 10
United States Code, Title 22
United States Code, Title 31, Section 1535
United States Code, Title 37, Section 455
United States Code, Title 44