CJCSI 6211.02E
3 August 2026

DEFENSE INFORMATION SYSTEMS NETWORK

JOINT STAFF
WASHINGTON, D.C. 20318

(INTENTIONALLY BLANK)

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6211.02E
DISTRIBUTION: A, B, C, S 3 August 2026

DEFENSE INFORMATION SYSTEMS NETWORK

References:
See Enclosure C

1. Purpose. This instruction establishes policy and assigns responsibilities for the secure connection to and use of the Defense Information Systems Network (DISN) in accordance with (IAW) references (a) through (c). The DISN is the Department of War's (DoW's) worldwide enterprise-level telecommunications and computing infrastructure, providing the core transport and information services for the DoW Information Network (DoWIN) to support military operations. Any information system (IS) connected to the DISN is subject to the DoWIN's overarching operational and defensive framework IAW reference (d).

2. Superseded/Cancellation. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02D, 24 January 2012, "Defense Information Systems Network (DISN) Responsibilities" is hereby superseded. Nothing in this instruction shall supersede, reassign, or override DoW policy or DoW Chief Information Officer (CIO) authority for governance, approval, and risk acceptance of enterprise collaboration and productivity capabilities, except where explicitly and unambiguously stated.

3. Applicability

a. This instruction applies to Combatant Commands (CCMDs) and their subordinate commands, joint task forces, Services (including the U.S. Coast Guard (USCG) and National Guard Bureau), Defense agencies, the Joint Staff, and DoW field activities (hereafter referred to as C/S/As); as well as to mission partners, defense contractors, and partner nations, connecting to or using DISN-provided transport or information services transmitted over the DISN IAW references (d) and (e).

b. The USCG will adhere to DoW cybersecurity requirements, standards, and policies, and will be responsible to the direction of Commander, U.S. Cyber Command (CDRUSCYBERCOM) for USCG-operated DoWIN systems and networks and for USCG ISs and networks that directly affect the DoWIN and DoW mission assurance IAW reference (f), while complying with Department of Homeland Security oversight and compliance requirements for acquisition and financial audit reporting IAW references (g) and (h).

c. Information technology (IT), security, connection, and exception requirements for the Defense Research Engineering Network (DREN), SECRET Defense Research Engineering Network (SDREN), DoW Mission Partner Environment (MPE), or other DoW networks (e.g., standalone or training enclaves), when not connected to or seeking connection to the DISN, are outside the scope of this instruction. For guidance on these networks, contact the DoW CIO and/or network owners (e.g., Under Secretary of War for Acquisition and Sustainment for DREN and SDREN). For information on multinational networks, see references (e), (i), and (j).

4. Policy

a. Enclosure A provides guidance on the use of and connection to DISN-provided transport and information services.

b. All ISs and networks that connect to DISN-provided transport and/or information services will adhere to references (k) and (l).

c. Additional policies governing satellite communications are addressed in references (m) and (n).

d. Policy on Sensitive Compartmented Information (SCI) is covered in reference (o).

5. Definitions. See Glossary.

6. Responsibilities. See Enclosures B.

7. Summary of Changes. Changes to this instruction include:

a. Replacing the Joint Staff Directorate for Force Structure, Resources, and Assessment, J-8 with the Joint Staff Directorate for Command, Control, Communications and Computers/Cyber, J-6 to reflect the re-establishment of the Joint Staff J-6.

b. Removing duplicated content addressed in references (c), (d), (p), and (q).

c. Replaces and updates the policy related to internet protocol (IP) tunneling, Cybersecurity Service Provider (CSSP), DISN-provided transport services, and the voice precedence system.

d. Removes commercial internet service provider (CISP) and DoWIN waiver information (connected and non-connected to the DISN), now referred to as "Exceptions to Policy (E2P)."

8. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on the Non-classified Internet Protocol Router Network (NIPRNET). DoW components (to include the CCMDs) and other Federal agencies may obtain copies of this directive through the Internet from the CJCS directives electronic library at <https://dod365.sharepoint-mil.us/sites/JS-Matrix-DEL/SitePages/Home.aspx>. Joint Staff activities may also obtain access via the SECRET Internet Protocol Router Network (SIPRNET) directives electronic library web sites.

9. Effective Date. This INSTRUCTION is effective upon signature.

For the Chairman of the Joint Chiefs of Staff:

PAUL C. SPEDERO, Jr., VADM, USN
Director, Joint Staff

Enclosures
A – Policy
B – Responsibilities
C – References

(INTENTIONALLY BLANK)

DISTRIBUTION

Distribution A, B, C plus the following:

Chief Information Officer, Department of War
Under Secretary of War for Intelligence
Commandant of the Coast Guard
Director, Defense Information Systems Agency
Director, Defense Counterintelligence and Security Agency

The office of primary responsibility for the subject directive has chosen electronic distribution to the above organizations via e-mail. The Joint Staff Information Management Division has responsibility for publishing the subject directive to the SIPRNET and NIPRNET Joint Electronic Library web sites.

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

LIST OF TABLES

ENCLOSURE A

POLICY

1. General. The DISN provides functional, sustainable, and secure joint warfighting IT capabilities aligned with reference (r). Designated as a mission-critical National Security System (NSS), the DISN must be operated and protected IAW references (c) and (p).

a. DoW Information Network Transport. The DISN and DoW C/S/A enclaves are the two main network transport elements of the DoWIN IAW reference (d). The DoWIN comprises all DoW-owned and leased:

(1) Information capabilities for collecting, processing, storing, disseminating, and managing information.

(2) Telecommunications subsystems and networks, to include their associated facilities, personnel, and material IAW reference (d).

b. Defense Information Systems Network. The DISN provides enterprise capabilities for the DoWIN and is centrally managed and configured by DISA IAW references (s) and (d). The DISN does not encompass DoW component enclaves; it begins and ends at the equipment under the operational direction and management control of DISA, at the physical point at which DISN network equipment ends (network termination interface) and the DoW component enclave infrastructure begins. This is the demarcation of responsibility between DISA and the components and occurs in the installation gateway. The DISN:

(1) Provides an integrated network for all DoW activities and their authorized mission partners.

(2) Supports secure transport requirements and services for sub-networks such as the NIPRNET and SIPRNET, as well as other government agency networks.

(3) The DISN-provided transport infrastructure delivers information transfer services between C/S/A installations and facilities, connections to external mission partners and defense contractors, and connections to the deployed infrastructure (e.g., warfighter).

c. DoW C/S/A Enclave. Owned, managed, and operated under the authority of a DoW component, it provides information transfer and joint services to all

authorized users, networks, and systems to support the movement of information between deployed networks and services and may extend access to DISN services and other networks and ISs. For additional information, see reference (d).

(1) The sustaining base infrastructure (i.e., base, post, camp, station, and enclaves) interfaces with DISN-provided transport infrastructure to support strategic/fixed environment user requirements within the C/S/A's base infrastructure and deployed warfighters. The C/S/A is responsible for the sustaining base infrastructure, including providing adequate space, protected power, redundant heating ventilation and cooling, physical security, and timely access when required.

(2) Deployed warfighters and associated CCMD infrastructure support the joint task force and/or combined task force. The CCMD and subordinate Service components have primary responsibility for deployed warfighters and associated infrastructure within their theater.

2. Defense Information Systems Network Management. The DISN shall be managed, operated, and defended as an integral component of the unified DoW information enterprise IAW references (b) and (c) and consistent with reference (t). Direction of DoWIN operations and defense shall be IAW references (u) and (d).

a. The DoW shall use DISN-provided transport to satisfy DoW information transfer requirements between DoW installations and facilities, and for external connections to mission partner and defense contractor ISs and networks IAW reference (l). DISN-provided transport is DoW's standard enterprise transport for DoW mission requirements to support consistent application of cybersecurity controls, centralized monitoring, and efficient use of resources. This prioritization does not imply that DISN-provided transport is inherently trusted; all transport, including DISN and commercial, is treated as untrusted and must meet applicable security and documentation requirements. Current warfighter requirements for DISN-provided transport and information services are documented in reference (v).

b. DISN-provided transport and information services shall employ:

(1) Qualified cybersecurity personnel IAW references (w)–(y) and (llll).

(2) Strict change management processes and procedures—to include use of automated Security Technical Implementation Guides (STIGs) compliance tools and Enterprise Mission Assurance Support Service—to implement security requirements contained in applicable STIGs, security

requirement guides (SRGs), and protection profiles (protection profiles are available at reference (cccc)).

(3) Only those ports, protocols, and services that have successfully undergone a vulnerability assessment and authorization process IAW reference (z).

(4) IS configuration approved in the Joint Interoperability Certification IAW reference (aa) and the Authorization to Operate (ATO) package.

(5) Support for Internet Protocol Version 6 (IPv6) to accommodate new and modernized ISs and services IAW reference (bb).

c. Enterprise collaboration and e-services equipment and software that are leased, procured (whether ISs or services), or operated by the C/S/As shall comply with the Unified Capabilities Requirements (UCR) as specified in reference (l), or have an approved Information Support Plan IAW reference (cc) that includes enterprise collaboration and productivity services equipment or products.

d. C/S/As shall procure or operate enterprise collaboration and productivity services, unless granted an E2P, IAW reference (k) and (l).

e. Supply Chain Risk Management (SCRM) will be instituted IAW reference (dd).

3. Requirements for Connection to the Defense Information Systems Network. This section establishes the foundational policies that apply to all DoW ISs seeking connection to the DISN. These requirements form the baseline for secure and authorized network access. For detailed guidance, refer to the DISN Connection Process Guide (reference (k).

a. Core Connection and Authorization Process

(1) C/S/As shall submit all DISN connection requirements for transport and information services to DISA IAW reference (k).

(2) If DISA cannot fulfill the requirement, the C/S/A shall submit their connection request through the DISA Storefront/Marketplace.

(3) All ISs approved to connect to the DISN must be authorized to operate IAW applicable federal, Intelligence Community (IC), or DoW guidance and processes.

(4) The system owner (SO) is responsible for developing, documenting, and maintaining the security plan and compliance status for the deploying IS. This includes selecting and documenting all security controls, preparing the security authorization package, and maintaining the Plan of Action and Milestones (POA&M) IAW references (o), (p), and (ee), as applicable.

(5) The SO must oversee and manage the IS's cybersecurity, to include conducting inspections, scanning, and maintaining an authorized security posture IAW references (k), (q), and (ff).

(6) C/S/As will provide the CCMD a courtesy copy of all DISN connection requests and requirements for DoW systems/facilities operated outside the United States and within the CCMD's area of responsibility.

(7) C/S/As must connect all sustaining base and deployable segments to the DISN IAW reference (k) and the supporting C/S/A procedures.

(8) All C/S/As shall adhere to decisions from the IS's Principal Authorizing Official (PAO) and DoW Information Security Risk Management Committee (ISRMC) regarding the enterprise deployment, operation, and connection of ISs IAW references (c) and (p).

(9) Mission partners are encouraged to connect using information domains with Data Centric Security (DCS) and Zero Trust (ZT) networks. These architectures enhance the security of classified and controlled unclassified information by enabling access decisions based on data tagging and user attributes rather than network location. Components will ensure systems are capable of data tagging IAW references (hh)–(jj), and North Atlantic Treaty Organization (NATO) Standardization Agreements (STANAGs) (references (dddd)–(ffff)), as applicable, when required for interoperability in the MPE.

(10) The DoW CIO may delegate connection approval authority to the DISA Authorizing Official (AO) for mission partner connections that are established through a DoW CIO-approved Mission Partner Gateway and architecture.

(11) The DoW CIO may delegate approval to DISA for mission partner or defense contractor connections to DISN-provided transport and information services when there has been no change in sponsor, mission, location, contract, architecture/topology, or DoW CIO original approval conditions. DISA will forward all renewal/approval packages to the appropriate C/S/A.

(12) The responsible C/S/A will coordinate with DISA customer provisioning for web services such as data interfaces for alarm, configuration, and trouble ticketing.

(13) All wide-area network transport—including DISN provided and commercially provided services—shall be treated as untrusted infrastructure in alignment with ZT principles. Security of DoW information will be enforced through cryptographic encapsulation, strong identity, continuous monitoring, and data centric access controls IAW references (kk)–(mm), rather than any assumption that an underlying transport is inherently trusted.

b. Foundational Security and Compliance. The responsible C/S/A will:

(1) Ensure ISs connected to the DISN subscribe to a certified and accredited CSSP. Cybersecurity services must be established prior to connection IAW reference (q).

(2) Ensure IT products that connect to the DISN meet all applicable cybersecurity requirements, including compliance with the STIG program and interoperability requirements as guided by reference (k) and current UCRs (Note: The DoW initiated a phased sunset of the DoWIN Approved Products List, with the program officially ending on 30 September 2025, IAW reference (oo)).

(3) Acquire all cybersecurity and cybersecurity-enabled IT products obtained for NSS IAW reference (nn).

(4) To ensure security and control, the responsible C/S/A must centrally catalog, govern, and manage all ports, protocols, and services IAW reference (z).

(5) Implement cyber network defense capabilities to continuously protect, monitor, detect, analyze, and respond to suspected unauthorized activity within the IS and networks IAW reference (q).

(6) Ensure cyber defense capabilities are available to always support the IS when connected to the DISN (e.g., 24 hours/7 days a week for an IS that is continuously connected).

(7) When aligning with an accredited CSSP, ensure any agreements and/or component policy are completed detailing the defensive cyber operations (DCO) services that will be provided by the CSSP and which services will be accomplished by the organization operating the IS.

(8) For mission partner and defense contractor ISs, ensure a signed agreement (e.g., a memorandum of agreement (MOA)) or contract defining the cybersecurity service provider requirements is implemented and programed for funding prior to connection.

(9) Ensure new and modernized DISN-connected ISs and services support IPv6 IAW reference (bb). Legacy systems that cannot immediately meet IPv6 requirements will be documented IAW reference (bb), including risk acceptance and transition planning.

c. System and Service Registration. Prior to connection, the responsible C/S/A will register all DoW ISs owned and operated on behalf of the DoW[1] in the applicable DoW IT repository (either the DoW IT Portfolio Repository (DITPR) or the SIPRNET IT Registry). C/S/As will register IS connection information IAW applicable STIGs and reference (c).

(1) Network Information Center for all unclassified information at <https://www.nic.mil>.

(2) SIPRNET Support Center for all classified information at <https://www.ssc.smil.mil>.

(3) Systems/Network Approval Process (SNAP) for unclassified voice, video, and data circuit registrations; unclassified voice switches; and DoW CIO exceptions to policy for internet service provider (ISP) registration at <https://snap.dod.mil>.

(4) SIPRNET Global Information Grid Interconnection Approval Process System (SGS) for classified voice, video, and data circuit registrations; and cross-domain solution (CDS) deployments at <https://giap.disa.smil.mil>.

(5) Ports, Protocols, and Services Management (PPSM) for all ports, protocols, and services that traverse the DISN, including voice over IP (VoIP) and voice over secure IP (VoSIP) IAW references (jj) and (pp).

(6) NIPRNET <https://pnp.cert.mil>.

---

[1] This applies to ISs under contract, with an MOA, Service-level agreement (SLA), or memorandum of understanding (MOU), and includes all systems that receive, process, store, display, or transmit DoW information, regardless of classification, to include all cloud services.

(7) SIPRNET <https://pnp.cert.smil.mil>.

(8) Register virtual private network (VPN)/IP tunnel traffic traversing the DoW Internet Access Point in the NIPRNET demilitarized zone (DMZ) Whitelist repository located on the SIPRNET at <https://niprdmzwhitelist.csd.disa.smil.mil/>.

4. Defense Contractor and Mission Partner Connections. This section provides specific policy requirements for defense contractors and mission partners connecting to the DISN. These requirements supplement the general policies outlined in paragraph 3. C/S/As are encouraged to include DISA in the early planning stages for all defense contractor and mission partner connections.

a. The C/S/A shall identify and provide validated requirements to DISA for each connection between a C/S/A installation and a defense contractor or mission partner IS. Connection requests must include an identified funding source.

b. Non-U.S. mission partner and defense contractor (when applicable) access to DoW information must comply with references (pp)–(rr). For all defense contractors, access to DoW information must comply with references (ee) and (uu), as well as any additional Defense Federal Acquisition Regulation (DFAR) clauses related to contracted IT and services. For more information on regulations of foreign and domestic commerce in communications, see reference (ss).

c. Defense contractor and mission partners ISs may not provide a backside connection to any other facility or IS without endorsement from the sponsoring C/S/A and explicit approval from the DoW CIO via the Defense Security/ Cybersecurity Authorization Working Group (DSAWG) and ISRMC review process.

d. A separate connection request is required for each mission partner or defense contractor connection. Access will be filtered and limited to only those data and services required to support the C/S/A-approved mission.

e. All connections require a DISA-engineered and -approved DISN or leased solution. The circuit requirement must be ordered by C/S/A through DISA's fulfillment tool (e.g., Marketplace) to generate a Telecommunications Service Request.

f. Notify the DoW CIO and DISA of all renewals and modifications to approved DISN connections. The C/S/A must validate any renewal request

with changes to the sponsor, mission, location, contract, architecture, or original approval conditions and submit for DoW CIO review and reapproval.

g. Connections that do not comply with the guidance contained herein are required to register and gain approval IAW Appendix A of reference (k).

h. The C/S/A is responsible for initiating and ensuring the termination of a connection when a system's ATO expires or a Denial of Authorization to Operate is issued.

5. Defense Contractor Connections. All defense contractor connections to DISN-provided services require a sponsoring government activity (SGA). The SGA is the organization or program office that owns the data, awarded the contract, and is responsible for limiting contractor system access to only the information and services required to execute the DoW-approved mission. Defense contractor systems operating under the National Industrial Security Program (NISP) will adhere to the policies, procedures, and standards established in references (ee) and (ss) and in alignment with reference (tt).

a. Unclassified Systems. The SGA AO is the designated risk owner for contractor's unclassified ISs (handling up to Controlled Unclassified Information (CUI)) and responsible for determining system authorization status IAW references (uu)–(ww). The SGA AO—in coordination with the program office, SO, and applicable contract oversight functions (e.g., Contracting Officer's Representative)—ensures that the contractor's cybersecurity compliance is assessed and maintained throughout the period of performance.

(1) The SGA AO ensures that the contractor maintains a valid certification IAW the Cybersecurity Maturity Model Certification Program and governing policy IAW references (o), (p), (ee), (uu), (vv), and (ww).

(2) Defense contractor ISs connected to the DISN shall report cyber incidents IAW reference (uu).

(3) All defense contractor ISs must be registered in the applicable DITPR prior to connection IAW paragraph 3.c. of this enclosure.

(4) For systems directly connected to DISN provided services, include for new or renewed contracts a provision that defense contractor ISs are subject to cyber security assessments.

(5) Undergo periodic cyber security inspections by sponsoring DoW C/S/A for ISs that process unclassified information to ensure compliance with contract security provisions.

b. Classified Systems. The Defense Counterintelligence and Security Agency (DCSA) is the designated NISP AO for classified contractor ISs IAW references (ee) and (xx).

(1) The NISP AO ensures sponsored defense contractors implement and maintain cybersecurity services from a certified and accredited CSSP prior to connection IAW reference (q). Information on CSSP requirements and authorized CSSPs may be found on the DoW Cybersecurity Knowledge Service site (reference (gggg)).

(2) The NISP AO ensures contractor ISs processing classified information comply with reference (ee) and all applicable contract security provisions within the Defense Federal Acquisition Regulation Supplement (reference (hhhh)) and SGA supplemental contract(s) (see reference (iiii) for specific guidance).

(3) When requested, the SGA will coordinate support for DCSA cybersecurity inspections of defense contractors IS processing classified information.

(4) Classified contractor ISs connected to the DISN shall provide results of inspections upon request to USCYBERCOM and DoW Cyber Defense Command (DCDC).

(5) Inspection results, including any findings of non-compliance and remediation plans, shall be formally documented and reported IAW reference (p) to the sponsoring C/S/A's CIO and DCSA as follows:

(a) High Risk – report within 30 days.

(b) Moderate Risk – report within 90 days.

(c) Low Risk – report within 365 days.

(6) Defense contractors must implement Federated Gateway connectivity solutions (e.g., NIPRNET Federated Gateway (NFG)) IAW reference (k).

(7) Register contractor IS in the applicable DITPR prior to connection IAW paragraph 3.c.

(8) For defense contractor systems directly connected to DISN-provided services, the C/S/A is responsible for submitting defense contractor connection requests to the DSAWG and ISRMC review process IAW references (k) and (yy). The C/S/A, in coordination with the cognizant AO, will:

(9) Ensure the sponsored system is authorized to operate.

(10) Ensure the defense contractor monitors and implements all applicable USCYBERCOM orders and directives under the provisions of the contract and reference (ee).

(11) Register contractor IS in the applicable repository prior to connection IAW paragraph 3.c. (i.e., DITPR or SIPRNET IT Registry).

6. Mission Partner Connections. Mission partner ISs shall adhere to the MPE operational framework IAW reference (e).

a. All mission partner connections to DISN-provided services require a sponsoring C/S/A, which is responsible for limiting the mission partner system access to only the information and services required to execute the DoW-approved mission.

b. Connection requests must be validated and endorsed by the C/S/As cognizant AO, and submitted to the DSAWG and ISRMC review process IAW reference (k).

c. C/S/A sponsors shall coordinate mission partner connection requirements with the MPE DoW Executive Agent (EA) to ensure solutions align with the MPE operational framework and implement Federated Mission Networking standards IAW references (k), (e), and (j).

d. For a direct connection request to DISN-provided transport and services, the C/S/A sponsor shall ensure a formal agreement (e.g., MOA) is in place IAW references (e), (zz), and (aaa), as applicable. This agreement must include provisions for security compliance, cybersecurity inspections, and information sharing.

(1) The agreement must be established in conjunction with, and not supersede, the policies and designated disclosure authorities outlined in reference (ss) for sharing of Classified Military Information.

(2) Ensure mission partners provide documentation of required security measures IAW reference (aaa) and (bbb).

(3) Ensure the mission partner conducts site inspections and remote scanning, maintains an acceptable authorized security posture, and provides cybersecurity services IAW federally mandated guidelines and/or as outlined by the MOA/MOU.

7. Non-U.S. mission partner access to DoW information shall comply with references (qq)–(ss).

8. Non-U.S. mission partners must be authorized to operate IAW IC or DoW guidance and processes. Refer to reference (xx) for additional guidance on partner nation connection requirements for SECRET and below ISs. C/S/As must register the mission partner IS in the applicable repository (DITPR or SIPRNET IT Registry) prior to connection IAW Section 3.c.

9. Mission partners connecting to DCS- and ZT-enabled MPE are required to implement alternative security measures IAW applicable STANAGs and references (v), (e), (j), (bbb), (gg), and (pp). These measures are required to protect classified information residing on the same information domain with data possessing different SECRET and CUI classification releasability caveats with mission partners. DCS-enabled MPEs restrict users' ability to access data based on Attribute Based Access Control to make data access determination decisions.

10. Joint Worldwide Intelligence Communications Connection Process Requests. C/S/As shall request connection to Joint Worldwide Intelligence Communications System (JWICS) IAW reference (ccc).

11. Defense Contractors and Mission Partner Connections Support During Civil-Military Operations

a. DoW policy provides provisions for the resourcing and extension of information services and capabilities to mission partners (civil-military partners) during civil-military operations IAW references (e) and (ddd).

b. C/S/As may provision and provide information services and capabilities for U.S. task forces to support mission partners in stability operations, when it is determined to be in the best interest of the DoW mission, and when the access is not in conflict with host-nation postal or telecommunications ordinances IAW references (e) and (ddd).

(1) These information services and capabilities may include:

(a) Unclassified voice and data services.

(b) Extension of bandwidth to or sharing of existing available bandwidth with mission partners to enable connection to or provision of Internet service and voice capability.

(c) Temporary cellular network services installed by DoW elements, where circumstances require, until local services are re-established.

(2) Ensure wireless equipment complies with existing domestic, regional, and international frequency spectrum allocations and regulations.

c. Provide information services and capabilities to the Department of State (DOS), when requested, to facilitate reconstruction, security, or stabilization assistance to a foreign country. Any services, defense articles, or funds provided or transferred to DOS to provide reconstruction, security, or stabilization assistance to a foreign country shall be subject to the authorities and limitations of those laws authorizing the appropriation of specific funds used to assist, and subject to applicable statutory and regulatory restrictions and limitations.

d. Mission partner access to DISN-provided transport and information services will be IAW reference (k).

12. Alternative Connections. This section addresses connection requests that do not comply with policy and/or requests for use of an alternative to available DISN provided transport.

a. DoW CIO approval is required for alternative connection requests. Such requests will be reviewed via the DSAWG and the ISRMC to ensure they maintain alignment with ZT principles, enterprise architecture, and DoW cybersecurity risk tolerance, and that they implement protections and monitoring equivalent to or greater than DISN-based solutions.

b. Commercially Provided Transport. The use of commercially provided transport as an alternative to available DISN-provided transport requires a commercial ISP E2P IAW references (d) and (k). Upon approval, C/S/As must:

(1) Utilize the DISA Direct Order Entry (DDOE) process (DISA Storefront/ Marketplace) or authorized acquisition to provision commercial ISP upon

approval of Commercial ISP Connection E2P.[2]

(2) Register the Commercial ISP Connection E2P in the SNAP database.

(3) Specific questions on whether a Commercial ISP Connection E2P is required for commercially provided transport should be directed to the DoW CIO through the C/S/A designated office/representative. For assistance in identifying your C/S/A representative, contact the Connection Approval Office (CAO) via <cao@disa.mil>.

c. Urgent Operational Requirements for Temporary Commercial ISP Connection Exception to Policy

(1) C/S/As shall register operational requirements for a temporary Commercial ISP Connection E2P for military operations (e.g., disaster relief or short-notice exercise) in SNAP database as urgent, and the DISA CAO will be notified.

(2) Service EAs shall register CCMD-validated requests for Commercial ISP Connection E2Ps in support of urgent operational requirements. Defense agency SNAP points of contact (POCs) shall register their agency urgent operational requirements.

(3) DISA will provide DISN transport or a commercial ISP connection within 24–48 hours or notify the C/S/A to use a commercially procured connection.

(4) The DSAWG Chair and DoW CIO will be notified to ensure connection is properly documented and managed until commercial ISP connection requirement is no longer required.

(5) C/S/A sponsor will provide verification of connection termination when no longer required.

---

[2] C/S/As are encouraged to synchronize the accreditation of IS(s) using a commercial transport and services connection with the DoW CIO E2P approval date/timeframe to avoid possible delays.

d. Improper Commercial Internet Service Provider Connection Implementation

(1) A commercial ISP connection found to be operating without approval or current authorization to operate must be immediately terminated until rendered compliant, if the connection is physically and/or logically connected to the local infrastructure enclave that is connected to the DISN NIPRNET infrastructure.

(2) Bring into compliance within 45 days, if the organization can demonstrate that the enclave is physically and logically separated from the local infrastructure enclave that is connected to the DISN NIPRNET infrastructure.

13. MINIMIZE Procedures. Only the Joint Staff Director for Operations, J-3 has authority to impose MINIMIZE worldwide or within the continental United States. The directive to implement communications traffic control condition MINIMIZE shall indicate the type of communications traffic to be reduced and/or removed. The DoW will utilize available means (user or technical) to reduce and/or remove nonessential data, voice, and video communications traffic during times of surge or crisis as required to ensure communications availability to meet DoW mission requirements. Controls on users or communications can include—but are not limited to—blocking, routing, usage, preemption or availability controls to ensure prompt transmission of communications traffic in support of mission requirements.

14. Defense Information Systems Network Voice Precedence (SIPRNET Only). The Multi-Level Precedence and Pre-emption capability for unclassified voice services is phased out IAW reference (k). Voice precedence for classified networks remains. Any requirements for classified voice precedence shall be coordinated through the appropriate C/S/A channels.

a. The precedence value assigned to a session by the originator specifies the order of handling to telecommunications systems, IS, and personnel. The value also indicates, to the addressee, the order in which the session is to be noted.

b. In the DoW, the highest to lowest priorities are FLASH OVERRIDE, FLASH, IMMEDIATE, PRIORITY, and ROUTINE. All DISN service requests for voice precedence requirements must be forwarded through the requestor's chain of command to the appropriate approval authority IAW Appendix A of Enclosure A.

c. The use of IMMEDIATE and PRIORITY precedence by DoW personnel assigned to non-U.S. (e.g., foreign government adviser, United Nations, NATO) organizations must be approved by the appropriate C/S/A. Requests for

FLASH or FLASH OVERRIDE must be validated by the C/S/A and approved by the Joint Staff J-6.

d. Temporary upgrading of voice precedence to support C/S/As or other equivalent personnel during travel is authorized for all precedence levels for up to 30 days. Temporary upgrading is also authorized for emergencies and exercises. Requests must be coordinated with DISA and approved by the CCMD.

e. Approval of FLASH and FLASH OVERRIDE access must be provided to DISA and the Joint Staff J-6.

15. Cybersecurity Inspection Program and Monitoring. The responsible C/S/A shall ensure systems connected to DISN-provided transport and information services will adhere to a tiered program of vulnerability assessments and inspections; intended to provide a systemic view of enclave and IS technical and traditional security posture. Inspection risk findings may lead to organizational or individual sanctions; to include potential disconnection of ISs from DISN-provided transport and information services.

a. ISs connected to DISN-provided transport and information services are subject to electronic monitoring for communications management, configuration management, situational awareness, and network security. This includes on-site and remote vulnerability inspections to check configuration for compliance with STIGs and other cybersecurity standards and guidelines.

b. All systems connected or operating on the DISN shall be subject to internal vulnerability assessments (including Blue Team Vulnerability Evaluation and Intrusion Assessments) and cyber security inspections with subject matter experts familiar with security control implementation and security requirements for the organizations and system specific technologies. Examples of organizations conducting external inspections include a Cyber Operational Readiness Assessment (CORA) conducted by DCDC under the direction of USCYBERCOM, DoW and C/S/A component inspectors general, the Government Accountability Office, and other authorized entities.

c. CDS, CD connections, and CDS subject matter experts (SMEs) proficient in security control implementation and technical requirements shall be integrated into all cybersecurity inspection program assessments, evaluations, and formal inspections.

d. When scanning for network compliance is conducted by DoW organizations external to another C/S/A, notification must be provided at least 24 hours prior to

the event or within an identified period (e.g., 1 week) of the organization being scanned for compliance in coordination with DCDC.

e. All systems connected or operating on the DISN will monitor scanning and notices issued or posted to the USCYBERCOM web site (<https://www.cybercom.smil.mil/>) and ensure that current, accurate, and complete contact information is provided to applicable DISN network/service databases.

f. Cyber Operational Readiness Assessment Program. DoW ISs connected to DISN-provided transport and information services are subject to the CORA process IAW reference (u). DCDC J10 oversees and executes Cyber Assessment Programs, to include the CORA program. CORA provides visibility into the key deficiencies of a system or cyber environment. The CORA methodology relies on risk-based metrics as its foundation for assessment. Key Risk Indicators are derived from these metrics and are associated with various technology areas. SOs will support and comply with USCYBERCOM-directed CORAs by:

(1) Employing published CORA criteria and tools for the CORAs' baseline for cyber security inspections.

(2) Adhering to post-inspection requirements, including development of POA&Ms, providing after-action plans, and implementing other mitigation efforts directed by DCDC.

(3) Utilizing additional information and resources available at:

(a) CORA < https://intelshare.intelink.gov/sites/jfhq-dodin/JD/SitePages/CCRI%20Program.aspx>.

(b) DoWIN Inspections Analysis Tool <https://integrate.diat.mil/public>.

16. Official and Authorized Use of the Defense Information Systems Network. The DISN and connected DoW ISs will be used for official and authorized purposes IAW references (eee) and (fff). See Appendix C of Enclosure A for further guidance.

17. Policies for Specialized Technologies and Architectures. This section outlines the requirements for connecting specific technologies and architectures, such as cloud services, wireless systems, and cross-domain solutions, to DISN.

a. Cloud Connections (Infrastructure as a Service, Platform as a Service, and Software as a Service). Ensure all DoW and mission partner use of cloud

computing services complies with the DoW Cloud Computing SRG (references (c) and (ggg)). The cloud SRGs can be found at reference (mmmm).

b. Wireless and Mobile Connections

(1) All DoW ISs use of DoW and non-DoW mobile platforms and applications must be IAW references (q), (ff), (hhh), and (iii).

(2) Wireless Local-Area Network Compliance. All commercial wireless local-area network (WLAN) systems connecting to or providing access to the DISN must comply with the security, certification, and validation requirements of references (k) and (jjj).

(3) Encryption Standards. All DoW-owned and operated WLANs must employ Wi-Fi Protected Access 3 (WPA3)-Enterprise only mode as an interim standard. Systems must transition to WPA3-Enterprise 192-bit mode immediately upon the availability of supporting Public Key Infrastructure (PKI) certificates. As technology evolves and WPA3 is eventually superseded, systems will be required to transition to the next authorized encryption standard to ensure continued security per references (kkk) and (lll).

(4) Configuration. All Component WLANs must be implemented, configured, operated, and secured IAW reference (ggg) and the applicable STIGs IAW reference (bb).

(5) Mobile Platforms. The use of all DoW and non-DoW mobile platforms and applications must comply with current DoW CIO guidance on mobile devices in references (jjj) and (dd).

c. Cross Domain Connections

(1) A CDS is used to interconnect ISs of different security domains IAW reference (mmm).

(2) All data transfers between security domains must be accomplished through a CDS listed on the National Cross Domain Strategy & Management Office (NCDSMO) Baseline list IAW reference (mmm).

(3) Enterprise CD services or centralized CDSs will be used for automated DoW CD information transfer requirements.

(4) Point-to-point CDSs will only be used when an enterprise service or centralized CDS does not meet C/S/A operational mission requirements.

(5) CDS and ZT architecture function as complementary security technologies. Between different designated information domains, the implementation of a ZT framework and a DCS architecture may be authorized as an alternative to a traditional CDS. The ISRMC shall validate and ensure all security requirements are satisfied prior to the approval of any alternative security mechanisms.

(6) All CDS will be deployed and managed on the controlling domain of the CD interconnection. CDS will be separately authorized for operation as an IS or as a CDS component within the IS in which it is deployed IAW reference (mmm).

(7) Information transferred between different security domains must be correctly marked, protected, and disseminated IAW references (gg), (hh), (jj), and (pp).

(8) Any environment operating under IC governance with connections to a collateral DISN system will be documented in the collateral DoW IS's security authorization package and require approval from both DoW and IC connection governance processes.

(9) All CDS architectures must be developed in coordination with the designated Cross Domain Support Element (CDSE). For connections to the DISN or use of DISA enterprise services, coordination must also occur IAW reference (k) and be fully integrated into the DoW enterprise security architecture consistent with DoWIN operations and defense procedures.

d. CDS Approval. All CDS implementations are managed by the DoW cybersecurity risk governance structure IAW reference (yy). The final risk acceptance for information flow between security domains is the responsibility of the DoW risk executive function, performed by the ISRMC, with support from the DSAWG. A Cross Domain Solution Authorization must be obtained prior to operation.

e. Cross Domain Support Element. IAW reference (mmm), the CDSE will manage the component's CD-related activities. For the Joint Force, this specifically includes obtaining CCMD validation, endorsement, and prioritization of information transfer requirements submitted by subordinate joint activities in support of CCMD operations. A full list of CDSE responsibilities may be found in reference (mmm).

f. Cross-Domain Information Transfer Requirements and Prioritization

(1) CD information transfer requirements are assessed and prioritized by the C/S/A based on their impact to the C/S/A's readiness and ability to execute a specific assigned mission. A CD information transfer requirement shall include:

(2) Impact Description. Identifies the information to be transferred and its relevance to organizational readiness and mission execution, and describes the adverse effect to both if the CD capability is not provided.

(3) Readiness Assessment Level. Identifies the impact and correlating Readiness Assessment (RA) level using the RA definitions in reference (ooo).

(4) Impact Rating. Informs CD capability requirements prioritization. Impact Ratings capture the detrimental impact to an organization's readiness and ability to execute the specified mission if a CD capability is not provided to support the information transfer requirement.

(a) CRITICAL. Failure to provide CD information transfer capability will preclude accomplishment of assigned mission(s).

(b) HIGH. Failure to provide CD information transfer capability will have significant impact on readiness and ability to execute assigned mission(s).

(c) MEDIUM. Failure to provide CD information transfer capability will have limited impact on readiness and ability to execute assigned mission(s).

(d) LOW. Failure to provide CD information transfer capability will have negligible impact on readiness and ability to execute assigned mission(s).

(5) Recommendation for new solutions or products in consultation with NC when existing CDSs and products on the CD baseline list cannot meet operational requirements IAW this instruction.

g. CD Capability Requirements Requests. C/S/As and CDSEs will provide coordinated CD capability requirements and associated prioritization information to NCDSMO and USCYBERCOM. The request must, at a minimum, include the information identified in Appendix B of Enclosure A.

18. Use of IP Tunneling and Virtual Private Network. IP tunnels enable hosts to send data securely over another network's connections by encapsulating the

packets, thus securing the information. The following guidance will be followed when the use of an IP tunnel is required to transport classified or CUI data.

a. Non-DoW Federal agencies, mission partners, and defense contractors requiring a connection to the NIPRNET must connect through the NFG. The NFG provides the required secure interface for both logical and physical connections.

b. The minimum cryptographic key required for all VPNs must be compliant with the DISA VPN Security Requirements Guide, National Security Agency (NSA) guidance, or DCDC requirements, as appropriate.

c. Connections using weak Internet Key Encryption with insufficient key length will be blocked from establishing a connection across the boundary into the DoWIN.

d. Requirements for all DoW VPN/IP tunnels must be validated at least annually. This validation shall be documented in the system's authorization package, and all applicable registries updated, IAW reference (k). VPN tunnel use will adhere to the appropriate STIG/SRG and must be documented in the system security authorization.

e. Split tunneling refers to the bandwidth conservation practice of routing only traffic destined for internal resources over the VPN, while letting other traffic (e.g., web, e-mail) directly access the Internet. VPN hardware or software client with split tunneling enabled provides an unsecured backdoor to the enclave from the Internet. Split tunneling is prohibited for traditional remote access VPNs. However, this prohibition does not apply to client traffic management implemented as part of a DoW CIO-approved ZT Architecture that securely routes traffic to different destinations based on data sensitivity and user authorization IAW references (ll) and (mm).

f. These requirements apply to IP tunnels and VPNs regardless of whether the underlying transport is DISN-provided or commercially provided; all such transports are treated as untrusted and must meet the same minimum cryptographic, encapsulation, monitoring, and documentation standards.

g. Physical security protection is implemented over VPN gateway devices used for tunneling classified traffic across the unclassified IP network.

h. IP tunnels/VPNs shall terminate at a policy enforcement point located in or adjacent to the DMZ, where traffic can be authenticated, authorized,

inspected, logged, and restricted before reaching enclave resources IAW reference (ll).

i. Protocols. IP Security (IPSec), Layer 2 Tunneling Protocol (L2TP/L2TP version 3), and Transport Layer Security, OpenVPN with Federal Information Processing Standard (FIPS)-compliant libraries, and Secure Hash Algorithm can be utilized. VPN tunnel use must adhere to relevant STIG/SRG and be documented in the system's security authorization package.

j. Mission Partner VPN Connections to the Defense Information Systems Network

(1) VPN connections to the DISN can be accomplished by provisioning logical tunnels using Multiprotocol Label Switching (MPLS) VPN or IPSec VPN.

(2) Existing mission partner connections to NIPRNET may be extended to NFG without installing new physical circuits. This can be accomplished by provisioning logical tunnels using MPLS VPN or IPSec VPN over the DISN. These tunnels extend existing mission partner connection(s) to the NFG, and the traffic will flow to the NFG on a slightly different path than originating from physical connections. Mission partners are required to maintain a direct physical connection to a DISN node to be eligible for a logical connection. Logical connections are physically homed to a NIPRNET router but are connected to the NFG via an encapsulated tunnel.

(3) Logical connection use cases are as follows:

(a) A commercial circuit extends from the customer to the DISN node. At the DISN router the customer connects to the NFG community of interest (COI) (MPLS VPN) for logical transport to the NFG site.

(b) Mission partners currently connected to the DISN router for NIPRNET access will connect to the NFG COI (MPLS VPN), eliminating NIPRNET access without passing through the NFG first.

(c) Logical connections through sponsors or other DoW agencies are not supported.

k. IP Tunnels/VPNs for Controlled Unclassified Data

(1) The DoW component AO is the approval authority for IP tunnels within the NIPRNET.

(2) IAW reference (k), a CISP may be used under the following conditions and requires DoW CIO approval:

(a) Connections to temporary facilities. Infrastructure non-availability.

(b) Urgent and ad hoc mission (up to 90 days).

(c) Temporary training (less than 90 days).

(d) Non-DoW locations.

(3) ISs must comply with VPN SRG.

(4) Use FIPS 140-3 encryption (reference (jjjj)) for tunneling sensitive data over unclassified networks.

(5) Comply with the NSA/Central Security Service (CSS) protection profile for tunneling sensitive information over unclassified networks.

(6) Document the tunneling solution in the applicable security authorization package prior to installation.

(7) Coordinate the use of IP Tunnels within hosting environments via an ISA, MOU, SLA, or other documentation.

l. IP Tunnels/VPNs for Classified Data

(1) Minimize tunneling of classified data over transport other than DISN-provided transport.

(2) The IS's AO must validate requirements for tunneling classified information across unclassified IP infrastructure.

(3) An IP tunnel securing classified data within the NIPRNET requires an authorization decision, and the connection must be documented in the authorization package. The connection shall be properly registered as outlined in reference (k) and receive a DISA Approval to Connect (ATC)/Interim Approval to Connect (IATC) prior to implementation. DSAWG approval is required for any IP tunnel used to secure DoW communications over the NIPRNET, the Internet, or a CISP, IAW references (k) and (nnn). The responsible C/S/A must ensure the request is submitted through the PPSM registry for DSAWG review and authorization.

(4) Document IP tunnels transporting classified communication traffic in the enclave's security authorization package prior to implementation. An ATC or IATC amending the current connection approval must be in place prior to implementation.

(5) DoW ISRMC approval of the CDS is required before classified data may be tunneled across unclassified IP infrastructure.

(6) IP tunnels shall be registered and updated in SNAP/SGS, and the PPSM registry, IAW reference (k).

(7) Transmissions shall be secured with authorized cryptographic equipment and algorithms and/or protected distribution systems (PDSs).

(8) IP tunnel endpoints shall be located within facilities authorized to process the information at the proper classification level.

(9) IP tunnels may only use cybersecurity and cybersecurity-enabled IT products evaluated IAW references (c), (nn), and (ppp).

m. Cryptography

(1) Products utilizing Commercial National Security Algorithm (CNSA)/ Commercial Solution for Classified cryptography may be used IAW references (nn) and (qqq) and successor policies that require products to have met NSA/CSS approved standards.

(2) ISs must request NSA/CSS review and approval prior to any specific implementation of CNSA Suite cryptography for classified or CUI. At a minimum, requesting organizations shall:

(a) Identify interoperability requirements specific to mission partner organizations and entities.

(b) Identify the releasability of the information to be protected (e.g., command and control (C2), intelligence, releasable or U.S.-only data).

(c) Provide recommended implementation of architecture (i.e., software, firmware, or hardware) to exchange and share information.

(d) Provide implementation plans associated with the approved key and key management activities.

(e) Ensure required formal agreements (e.g., MOA or international agreements) are completed with mission partner organizations and entities for connection and information sharing.

19. Backside Connections. Backside connections join two enclaves (e.g., a C/S/A and a defense contractor) and do not traverse the DISN, but can provide a connection to the DISN through the C/S/A enclave.

a. C/S/A Connections Between DoW Entities

(1) A C/S/A AO may authorize connections between DoW facilities operated by another C/S/A to provide access to DISN-provided transport and information services (e.g., DoW tenant connecting to the DISN through the base/post/camp or station local infrastructure). Connections made between two connecting sites must be established consistent with the requirements in the network STIGs/SRGs.

(2) The DoW facilities are expected to be geographically adjacent (e.g., base/camp/station or metropolitan area). Exceptions may be authorized related to mission needs. Requests for connection exceptions will be processed through DISA to the DSAWG.

b. C/S/A Connections to Mission Partner or Defense Contractor Facilities and Information Systems

(1) Examples of a backside connection between DoW facilities and defense contractor facilities can include connecting using CISP transport and services and physically connecting with fiber or another transmission medium.

(2) C/S/As must obtain DoW CIO approval to connect mission partner or defense contractor facilities or ISs to the C/S/A infrastructure (e.g., base/ post/camp or station enclave), which is connected to the DISN.

(3) Once approved by the DoW CIO, mission partner and DoW contractor connections must be ordered through the DDOE process IAW reference (l).

(4) If SIPRNET e-mail is required in support of a contract, the contractors must obtain their SIPRNET e-mail via their sponsor's enclave (e-mail clients).

(5) Implement the connection behind appropriately protected enclaves and ensure an MOA is established for cybersecurity services with protections equivalent to STIGs/SRGs or federal security requirements.

20. C/S/A Connection Responsibilities. The C/S/A providing a backside connection through its infrastructure to the DISN for another DoW entity, DoW CIO-approved mission partner, or defense contractor will:

a. Implement the connection behind appropriately protected enclaves and ensure an MOA is established for DCO services with protections equivalent to DISA STIGs or federal security requirements.

b. Accept responsibility for the connection in the security authorization documentation reference (p) and update the DISN connection package with DISA, to include a copy of any interconnection agreements and detailed topology diagrams including all connections.

c. Provide details on all current and proposed connections (including, but not limited to, interconnection agreements and topology diagrams) to the DISN connection approval office as part of the connection request package.

d. Notify C/S/A CDSE if a CDS is required for connection. The CDS must be employed, configured, and maintained IAW CDS implementation guidance.

e. Provide supporting encryption equipment, keying material, or a channel servicing unit/data servicing unit (CSU/DSU) except for what may be ordered with vendor leasing action.

f. Ensure customers contact their support activity (C/S/A service provider) rather than DISA in the event of a circuit problem associated with a C/S/A provided connection.

g. Ensure connected mission partners and defense contractors do not provide a backside connection to another organization without prior approval.

h. Records Management. See references (rrr)–(ttt).

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE A

DEFENSE INFORMATION SYSTEMS NETWORK
VOICE PRECEDENCE REQUESTS

1. General. For all DISN voice precedence requests, C/S/As will:

a. Review and approve or disapprove all requests for IMMEDIATE and PRIORITY precedence capability.

b. Validate and forward requirements for FLASH and FLASH OVERRIDE to the Joint Staff J-6 for approval.

c. Ensure:

(1) Precedence requirements are justified in terms of explicit mission need, to include an explanation of negative mission impact if the request is not approved.

(2) Requirements affecting other CCMDs, Services, or Defense agencies have been coordinated with those affected organizations.

(3) Requests for FLASH and FLASH OVERRIDE require a trade-off of equal precedence.

(4) Appropriate communication service priorities are identified.

(5) All DISN voice service (e.g., Defense Red Switch Network (DRSN)) requests for voice connections and precedence requirements must be forwarded through the requestor's C/S/A chain of command to the appropriate approval authority IAW Table 1. Requests for new DRSN connections and/or changes to existing connections must be submitted IAW DISA DRSN Connection Request Form process and reviewed and approved by Joint Staff J-6.

APPROVAL	REQUEST ORIGINATOR				
	Military Service	U.S. Command	DoW Agency	NMCS Joint Staff	Mission Partner Agency/ Organization
FLASH OVERRIDE	Joint Staff/J-6	Joint Staff/J-6	Joint Staff/J-6	Joint Staff/J-6	DoW CIO
FLASH	Joint Staff/J-6	Joint Staff/J-6	Joint Staff/J-6	Joint Staff/J-6	DoW CIO
IMMEDIATE	Service Chief*	Combatant Commander	Agency Director*	Joint Staff/J-6	DoW CIO
PRIORITY	Service Chief*	Combatant Commander	Agency Director*	Joint Staff/J-6	DoW CIO
** For OCONUS requests, the Combatant Commander approves requests within their AOR.*					

Table 1. Voice Precedence Request Approval

d. FLASH and FLASH OVERRIDE requests from mission partners outside the DoW must be sponsored by a C/S/A and must be forwarded through the Joint Staff J-6 to the DoW CIO for approval.

e. CCMDs and Services may tailor the information requests for which they have approval authority. Requests for DISN voice services requiring precedence will be in advance of the date needed and provide the following information:

(1) Description of required operational capability (concise narrative description).

(2) Present capabilities for DISN and why they are inadequate.

(3) Detailed description of the mission directly supported by the requirement or the mission change that generated the requirement and mission impact if disapproved.

(4) Complete identification of the requirement (e.g., type of change, deletion, or addition), including circuit or equipment quantities, configurations, sequence numbers.

(5) Unit, title, and geographic location of requesting agency.

(6) Precedence requested.

(7) Start date (if short notice, give justification and mission impact of delay).

(8) Restoration priority or telecommunications service priority.

(9) Servicing switch (End Office, Small End Office, Private Branch Exchange, Remote Switching Unit, Multi-Function Switch, and Multi-Function SoftSwitch).

(10) Customer Provider Edge or terminating type equipment used behind the voice switch (e.g., analog, digital, VoIP, VoSIP, video teleconference, mobility device)

(11) Number of extensions required. Indicate if extensions are in geographically separate locations requiring extension of connectivity to servicing switch.

(12) Location of the user-requested DISN service (geographic and physical location of the end instrument).

(13) DISA, DoW CIO, ISRMC, or Joint Staff E2Ps in effect.

(14) Identification of the destination and expected frequency and duration of calls, data transmissions, or facsimile transmission. Information may also be expressed in terms of Erlangs (E) of traffic.

(15) Operational mission security requirement (applicable classification of service (e.g., Collateral SECRET/TOP SECRET or TOP SECRET/SCI)).

(16) C/S/A POC (name, office symbol, DSN, and commercial telephone number).

(INTENTIONALLY BLANK)

APPENDIX B TO ENCLOSURE A

CROSS DOMAIN CAPABILITY REQUIREMENT REQUEST

[Name of Reporting Organization]

DD MMM YYYY

SUBJECT: Title of the CD Capability Deficiency

1. CD Information Transfer Requirement. Brief description of information transfer requirement.

2. Capability Deficiency/Gap. Brief description of deficiency and how the requirement is not being met.

3. Requirement Source/Authority. List of the source documents from which the requirement is derived (e.g., *Guidance for the Employment of the Force*, *Joint Strategic Capabilities Plan*, concept plan XXXX, operations plan XXXX, Theater Security Cooperation plan).

4. Impact Description. Provide objective information to quantify the deficiency's impact on the organization's ability to conduct its mission(s). Identify the impacted joint/agency mission essential task list (e.g., OP 3.1.5., Publish Air Tasking Order[s]) and the correlating RA level IAW reference (ooo).

5. CD Capability Impact Rating. CRITICAL/HIGH/MEDIUM/LOW.

6. Actions Taken. Actions taken to date to meet CD information transfer requirement to execute mission(s).

7. Action Necessary to Fix Deficiency. Recommendation or solution to address current CD capability deficiency.

8. Risk and Planned/Potential Mitigation Action. Identify and assess current risk that the CD deficiency poses to mission execution and the planned/ potential mitigation steps necessary to manage this risk until CD capability is implemented.

9. Point of Contact Information. Name, rank, organization, e-mail, and phone number.

(INTENTIONALLY BLANK)

APPENDIX C TO ENCLOSURE A

AUTHORIZED USE OF THE DEFENSE INFORMATION SYSTEMS NETWORK

1. Personal Use of Defense Information Systems Network. All C/S/As shall authorize categories of personal use of DISN communication and ensure that such communications:

a. Do not adversely affect the performance of official duties by the DoW employee or C/S/A.

b. Are of reasonable duration and frequency as determined by leadership and, whenever possible, are made during the DoW employee's or military member's personal time (such as before/after normal duty hours or during lunch periods).

c. Serve a legitimate public interest such as enabling DoW employees or military members to stay at their desks rather than leave the work area to use commercial communication systems.

d. Do not overburden the communications system and create no significant cost to the DoW or C/S/A.

e. Ensure DoW ISs used to access the Internet are used for official and authorized purposes IAW references (eee) and (fff).

2. Limiting Use of Defense Information Systems Network. C/S/A directors or military commanders may prohibit use of government communications systems and equipment, or filter access to commercial web sites or web services, to defend DoW's IT resources, safeguard missions by preserving operational security, and ensure sufficient bandwidth is available for DoW operations IAW reference (eee).

a. Examples of situations where access may be prohibited or filtered include the following:

(1) Accessing streaming video or radio web sites.

(2) Accessing personal commercial e-mail accounts (e.g., Hotmail, Yahoo, Gmail, AOL) from government computers.

(3) Accessing web sites with identified threat of malware infection (e.g., computer viruses, worms, trojan horses, root kits, spyware, adware, ransomware, and other malicious and unwanted software/code).

b. IAW reference (eee), commanders and directors have the authority to limit or prohibit personal use of government communications systems to preserve network security, ensure mission-critical bandwidth, and maintain operational security.

c. All such limitations must be applied uniformly to all personnel and must not interfere with authorized Morale, Welfare, and Recreation activities as permitted by reference (uuu).

3. Prohibited use of DISN includes, but is not limited to:

a. Use, loading, or importing unauthorized software (e.g., applications, games, peer-to-peer software, movies, music videos or files).

b. Accessing pornography.

c. Unofficial advertising, selling, or soliciting (e.g., gambling, auctions, stock trading).

d. Improperly handling classified information.

e. Using the DISN to gain unauthorized access to other ISs.

f. Endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

g. Posting DoW information to external newsgroups, bulletin boards, or other public forums without authorization.

h. Other uses incompatible with public service.

4. Individual and Organizational Accountability. The provisions concerning the official and authorized use of the DISN (federal communications) in reference (eee) constitute lawful general orders or regulations within the meaning of reference (vvv), are punitive, and apply without further implementation. In addition to prosecution by court-martial under the Uniform Code of Military Justice (UCMJ), a violation may serve as a basis for adverse administrative action and other adverse action authorized by U.S. Code or federal regulations. In addition, violation of any provision in reference (eee) may constitute the

UCMJ offense of dereliction of duty or other applicable punitive articles. C/S/As shall:

a. Ensure users complete initial IA orientation and annual refresher training IAW references (w).

b. Use a DoW CIO-approved consent banner and user agreement on all DoW ISs IAW reference (x).

c. Ensure privileged users sign an IS privileged access agreement and acknowledgement of responsibilities IAW reference (x).

d. Ensure military, civilian, and contractor personnel are subject to administrative and/or judicial sanctions, as appropriate, if they knowingly, willfully, or negligently compromise, damage, or place at risk ISs, classified information, or controlled unclassified information by not ensuring implementation of DoW security requirements IAW this instruction, references (hh), (pp), and (eee),and supplemental C/S/A policies and procedures.

(1) Reference (eee) states penalties for violation of the standards of conduct prescribed that include statutory and regulatory sanctions such as judicial (criminal and civil) and administrative actions for DoW civilian employees and members of the Military Departments.

(2) Sanctions for military personnel may include administrative actions, such as warnings, reprimands, adverse evaluations, and suspension of access to classified materials, as well as measures authorized by Service directives and the UCMJ.

(3) Sanctions for civilian personnel may include administrative action, such as warnings, reprimands, adverse performance evaluation, suspension, loss or suspension of access to classified materials as well as other administrative sanctions authorized by contract or agreement; and/or dismissal from employment. Sanctions for civilians may also include prosecution in U.S. District Court or other courts and any sentences awarded pursuant to such prosecution. Sanctions may also be awarded only by civilian managers or military officials who have authority to impose the specific sanctions proposed.

(4) Defense contractors are responsible for ensuring employees perform under the terms of the contract and applicable directives, laws, and regulations, and they must maintain employee discipline. The contracting officer, or designee, is the liaison with the defense contractor for directing or

controlling contractor performance. Outside the assertion of criminal jurisdiction for misconduct, the contractor is responsible for disciplining contractor personnel. Criminal jurisdiction within the United States could be asserted by federal, state, or local authorities. For defense contractors accompanying the U.S. Armed Forces abroad, jurisdiction may be asserted by the foreign state or, for certain offenses, by the federal government, including under reference (www). For additional information on defense contractor personnel authorized to accompany U.S. Armed Forces, see reference (xxx).

ENCLOSURE B

RESPONSIBILITIES

1. Joint Staff. The CJCS is responsible for developing DISN joint policy IAW references (c), (l), (p), and (s), and facilitating communications with Combatant Commanders (CCDRs) to improve the adequacy and effectiveness of communications, C2, cybersecurity, computing services, interoperability and standardization, DoW enterprise services, engineering, and acquisition functions IAW reference (a).

a. Joint Staff Director for Operations, J-3

(1) Advise the CJCS on the responsiveness and readiness of the DISN to support C2 of operating forces in the event of crisis and conflict to national security, in coordination with Joint Staff J-6 and USCYBERCOM.

(2) Advise and recommend, when appropriate, implementation of communications traffic controls to ensure National Military Command System communications availability for mission requirements.

b. Joint Staff Director for Command, Control, Communication, and Computers/Cyber, J-6

(1) Advise the CJCS on C2, communications, computer, and ISs requirements and priorities in coordination with DoW CIO.

(2) Provide guidance to the Joint Staff Directorates and CCMDs on DISN policy and responsibilities, to include obtaining approval to connect to DISN (e.g., mission partners or defense contractors), CD transfer requirements, and DoWIN.

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

(4) Serve as the Warfighting Mission Area (WMA) PAO for the CJCS IAW reference (c).

(5) Appoint a senior executive or flag-level WMA PAO[3] representative to the DoW ISRMC.

(6) Appoint a representative in the military grade of O-6 or equivalent GS-15 civilian as primary representative to the DSAWG.

(7) As the Joint Staff CIO, implement applicable policy for Joint Staff networks.

2. Combatant Commanders. The CCDRs, or their designated representative, shall:

a. Approve the connection and subsequent operation of deployed ISs within CCMD information networks and the connection to DISN sites providing DISN transport and information services to local infrastructure. This ATO by the CCDR must be included in the DISN connection approval request package submitted to DISA.

b. Endorse and validate CCMD CD, mission partner, and defense contractor DISN connection requests in support of mission requirements.

c. Review and submit service restoration priority requests IAW reference (*zzz*).

d. Submit DISN-provided transport and information services requirements through designated Combatant Command Support Agent (CCSA) channels to DISA IAW reference (a).

e. Provide USCYBERCOM, DCDC, and DISA read access to CCMD-level vulnerability management ISs.

f. Approve or disapprove outside the United States local commander requests for DSN voice service (personal or unofficial use). Notify DISA DSN Program Management Office of approvals. Review and revalidate secure voice conference requirements annually.

---

[3] DoW PAOs are appointed for the four DoWIN mission areas (MAs), consisting of the Warfighter MA, the Enterprise Information Environment MA, the Defense Intelligence MA, and the Business Mission Area.

g. Plan for the implementation of communications traffic controls (procedural or technical) for their commands or area of command responsibility during surges or crisis (actual or simulated).

h. Direct implementation of communications traffic controls during surges or crisis (actual or simulated) for their commands, area of command responsibility, or functional area with notification to National Military Command Center (NMCC), USCYBERCOM, C/S/As, other USG agencies, and foreign mission partners as deemed appropriate.

i. Cross Domain Responsibilities

(1) Designate a CDSE or an existing office under the CCMD's authority to carry out CD responsibilities as outlined in reference (mmm).

(2) Designate a CDSE, or an office under authority of a C/S/A or the Joint Staff CIO, to carry out CDSE functions, to include providing oversight and management of CD activities throughout the CD System Development Life Cycle (SDLC).

(3) If the CCMD does not designate a CDSE, it will request CD support from the CCMD's Service Executive Agent, IAW reference (aaaa), or another C/S/A CDSE and develop an MOA outlining CCMD and supporting CDSE responsibilities, including the life-cycle costs, sustainment, and management of any CCMD-directed CDS implementation support.

(4) Ensure the CDSE develops and implements transition plans for CDSs identified on the NCDSMO CD sunset list.

(5) Provide their CDSE with a POA&M or evidence of a funded security strategy that describes the plan for reducing risks associated with CD connections having risk ratings beyond which the DSAWG can accept.

(6) Ensure all procured CDSs are on the NCDSMO CD capabilities portfolio baseline list, unless a waiver is granted IAW reference (mmm).

3. Commander, U.S. Special Operations Command. In addition to the responsibilities outlined in paragraph 11, Commander, U.S. Special Operations Command shall:

a. Coordinate with theater CCMDs and their supporting Service Components for required IS support at theater installation(s).

b. Submit DISN-provided transport and information services requirements directly to DISA, as required.

4. Commander, U.S. Cyber Command. In addition to the responsibilities outlined in paragraph 11, CDRUSCYBERCOM shall:

a. Direct DoWIN secure, operate, and defend requirements for the DoWIN, including the DISN and synchronize cyberspace operations planning in coordination with C/S/As IAW reference (ff).

b. Delineate USCYBERCOM roles and responsibilities to plan, coordinate, and direct DoWIN operations and DCO internal defensive measures.

c. Issue USCYBERCOM orders and directives to provide instructions on the operation and defense of DISN and connected ISs IAW reference (ff).

d. Prioritize Service and CCMD CD information transfer requirements based on impact description provided by the CCMD or Service's ability to execute assigned mission(s) in support of the UCRs and reference (bb).

e. Appoint a flag-level or senior executive representative to the DoW ISRMC IAW reference (yy).

f. Appoint a primary representative in the military grade of O-6 or civilian equivalent of GS-15 to the DSAWG IAW reference (nnn).

g. Provide personnel to participate in cybersecurity inspection teams in support of DCSA-led compliance inspections and USCYBERCOM-directed CORAs of defense contractor classified ISs connected to DISN-provided transport and information services IAW reference (ee) and contract IS security provisions.

5. Director, Defense Information Systems Agency. In addition to the responsibilities outlined in paragraph 11, the Director, DISA shall:

a. Extend the DISN, data centers, and enterprise services to support requests from CCDRs and their DoW contingency operations around the world IAW reference (a).

b. Operate, maintain, and secure the DISN IAW reference (a). Provide and maintain Internet exchange points and cloud service provider interconnections.

c. Plan for the implementation of communications traffic controls worldwide during surges or crisis (actual or simulated) in coordination with Joint Staff J-3/J-36 NMCC (reference (zzz)).

d. Direct worldwide implementation of communications traffic controls during surges or crisis (actual or simulated) as authorized or directed with notification to NMCC, C/S/As, other USG agencies, and foreign mission partners as deemed appropriate.

e. Appoint a flag-level or senior executive representative to the DoW ISRMC IAW reference (yy).

f. Appoint a primary representative in the military grade of O-6 or civilian equivalent of GS-15 to the DSAWG IAW reference (nnn).

g. Ensure an MOA is signed outlining roles and responsibilities for DISA and DCSA as part of the connection approval process and for the oversight of cleared defense contractor connections to the DISN.

h. As Commander, DCDC, provide continuous monitoring of all connections to DISN.

(1) Coordinate with C/S/As to ensure monitoring of connected enclaves.

(2) Direct CORAs for DoW DISN-provided transport, information services and connected ISs IAW the USCYBERCOM Cybersecurity Inspection Program (CSIP).

(3) Issue procedures for coordination and notification of remote compliance monitoring and scanning of C/S/A ISs. Scanning pre-notifications may be in the form of notices posted to a designated DCDC SIPRNET web site or direct DCDC communications to the AO.

(4) Provide personnel to participate in cybersecurity inspection teams in support of DCSA-led compliance inspections and CORAs of defense contractor classified ISs connected to DISN-provided transport and information services IAW reference (ee) and contract is security provisions.

(5) Participate in DISN-related panels, boards, and working groups.

6. Director, Defense Intelligence Agency. In addition to responsibilities outlined in paragraph 11, the Director, Defense Intelligence Agency (DIA) shall:

a. Implement, operate, manage, and secure JWICS components and facilities on the DISN-provided transport IAW established agreements with DISA and the DCDC.

b. Provide threat assessments to support C/S/A ISs and IS risk assessments and decisions.

c. In support of IC CD information transfer connection requirements, perform the following in addition to the responsibilities outlined in Enclosure A.

(1) Designate a CDSE to coordinate, manage, and maintain the DIA-provided DoW information networks enterprise CD services, centralized and point-to-point CDSs IAW reference (mmm). Ensure there is feedback among DIA and supported C/S/As and the NCDSMO about CD services and CDSs.

(2) Conduct security control assessment and authorization to operate requirements of CD solutions IAW applicable CNSS, DoW, IC, and NCDSMO guidance.

(3) Participate in DISN-related panels, boards, and working groups, to include:

(a) Appointing a flag-level representative to the DoW ISRMC.

(b) Appointing a primary representative in the military grade of O-6 or GS-15 civilian equivalent to the DSAWG.

7. Director, National Security Agency/Central Security Service. In addition to responsibilities outlined in paragraph 11, the Director, NSA/CSS shall:

a. In support of DoW CIO and IC CD information transfer requirements, and in addition to responsibilities outlined above, designate a CDSE to work CD activities and issues with NCDSMO.

b. Participate in DISN-related panels, boards, and working groups, to include:

(1) Appointing a flag-level representative to the DoW ISRMC.

(2) Appointing a primary representative in the military grade of O-6 or GS-15 equivalent civilian to the DSAWG.

8. Director, Defense Counterintelligence and Security Agency. In addition to the responsibilities outlined in paragraph 11, the Director, DCSA will direct the DCSA CSIP to:

a. Establish security standards as the AO for defense contractor classified ISs under reference (ee) that are equivalent to published STIGs IAW reference (ff).

b. Ensure classified defense contractor ISs connected to the DISN comply with DCSA security standards.

c. Ensure defense contractor ISs that process classified information connected to DISN are aligned to an authorized cybersecurity service provider.

d. Ensure an MOA is signed outlining roles and responsibilities for both DISA and DCSA in the connection approval process and oversight of cleared defense contractor connection to the DISN.

e. Establish cybersecurity inspection teams including team members from DISA or USCYBERCOM, as appropriate, to conduct DCSA compliance inspections and support DCDC-directed CORAs of defense contractor classified ISs connected to DISN-provided transport and information services IAW reference (ee) and contract IS security provisions.

f. Notify defense contractors with classified ISs connected to the DISN of scheduled DCSA compliance inspections or DCDC-directed CORA.

g. Notify DISA or DCDC of unannounced DCSA compliance inspections, as appropriate.

h. Employ published DCDC CORA criteria and tools for inspections of classified defense contractor ISs connected to DISN-provided transport and information services as governed by reference (ee) security requirements and contract IS security provisions.

i. Provide inspection results upon request to USCYBERCOM, DoW CIO, or DISA for defense contractor ISs processing classified information connected to the DISN.

j. Participate at DSAWG as requested by Under Secretary of War for Intelligence and Security to provide information or comments relating to cleared defense contractor issues as the AO for contractor classified ISs under the authority of references (ss) and (ee).

9. Director, National Cross Domain Strategy and Management Office. The Director, NCDSMO performs the duties and responsibilities IAW reference (mmm) and shall:

a. As the CCSA—IAW reference (yyy) and when requested by a CCMD—provide CD support service IAW Enclosure A. The MOA or MOU outlining CCMD and supporting Service CDSE responsibilities is required and shall address the life cycle costs, sustainment, and management of any CCMD-directed CDS.

b. Identify, assess, and document the DISN assets and associated dependencies needed to implement required C/S/A mission-essential tasks and required capabilities in coordination with DISA.

c. Provide headquarters (HQ) of CCMDs and subordinate unified commands administrative and logistical support (i.e., base operating support, including engineering documentation for transport and services, submissions for DISN-provided transport and services, and necessary infrastructure), IAW reference (yyy).

d. Participate in DISN-related panels, boards, and working groups IAW references (yy) and (nnn).

e. Provide cyber defense services IAW reference (q).

10. Service Executive Agents

a. Provide CDSE support to hosted CCMDs when requested IAW established MOAs.

b. Register CCMD-validated requests for a CISP connection E2P in support of urgent operational requirements.

11. All C/S/As Connected to Defense Information Systems Network Transport or Information Services

a. Submit requirements for DoW ISs and network connections via their chain of command to DISA IAW reference (k). Ensure transmission of classified information is secured through use of an authorized cryptographic equipment and algorithms and/or PDSs.

b. Ensure that SIPRNET enclaves with the requirement to process NATO classified information meet NATO and U.S. security requirements to handle

NATO classified information IAW reference (bbbb). Reference (kkkk) lists registered enclaves.

c. Ensure C/S/A organizations provide for or align with an authorized CSSP to acquire cybersecurity support for each IS.

d. Endorse and maintain oversight of subordinate organizations' connection requirements and requests by:

(1) Validating operational requirements and prioritizing mission partner and defense contractor connection requests.

(2) Ensuring that foreign entity connection requests are endorsed by the CCMD headquarters.

(3) Assigning a primary (in military grade of O-6 or GS-15 civilian equivalent) and an alternate representative to validate and endorse mission partner and defense contractor DISN connection requirements for their C/S/A HQ.

e. Program, budget, fund, and provide support for assigned portions of the DISN, including procurement (e.g., SCRM), training, operations, maintenance, usage fees, CD service, CDS development, physical security, electronic security, and survivability measures.

f. Perform the following tasks in support of Service CD information transfer requirements:

(1) IAW reference (mmm), designate a CDSE or a C/S/A office under authority of C/S/A CIO to carry out CDSE functions to provide oversight and management of CD activities throughout the CD SDLC.

(2) Advocate compliance with current NCDSMO requirements.

(3) Support funding strategy for risk mitigation strategies for CD connections assessed risk ratings above the level the DSAWG can accept (approve a POA&M or a documented and funded strategy describing their risk mitigation approved IAW reference (mmm)).

(4) Support security test and assessment of CDS implementation IAW DoW and IC guidance to implement security controls as required.

(5) As the CCSA—IAW reference (aaaa) and when requested by CCMD—provide CD support service IAW Enclosure A. The MOA or MOU outlining CCMD and supporting Service CDSE responsibilities is required and shall address the life cycle costs, sustainment, and management of any CCMD-directed CDS.

g. Provide requisite site support for DISN equipment located on bases, posts, camps, and stations. This includes providing power, physical security, floor space, and onsite coordination for the DISN network points of presence on these bases, posts, camps, and stations. Site support must be specified in procedural documentation and coordinated between the Service HQ and DISA HQ.

h. Identify, assess, and document the DISN assets and associated dependencies needed to implement required C/S/A mission-essential tasks and required capabilities in coordination with DISA.

i. Provide HQ of CCMD and subordinate unified commands administrative and logistical support (i.e., base operating support, including engineering documentation for transport and services, submissions for DISN-provided transport and services, and necessary infrastructure) IAW reference (aaaa).

j. Ensure their DoW ISs are compliant with DoW cybersecurity requirements IAW references (c) and (k).

k. Ensure that defense contractors' classified ISs are compliant with cybersecurity requirements IAW reference (ee).

l. Ensure that foreign mission partner ISs are compliant with cybersecurity requirements IAW reference (bbb).

m. At a minimum, annually review their connected ISs to ensure compliance with applicable cybersecurity requirements, including mission partner and defense contractor ISs sponsored by the C/S/A.

n. Provide information, as requested, to DISA for DISN-provided transport and information services billing, management, and inventory purposes.

o. Support MINIMIZE operations.

(1) Conduct planning for implementation of communications traffic controls for C/S/A communications during surges or crises (actual or simulated).

(2) Notify NMCC, USCYBERCOM, and DoW CIO when communications traffic controls are implemented for C/S/A communications.

p. For owned/leased telecommunications equipment and services, all C/S/As shall:

(1) Acquire effective, efficient, and economical base telecommunications equipment and services.

(2) Maintain an inventory of all base telecommunications equipment and services.

(3) Review and revalidate all requirements for C/S/A telecommunications equipment and services.

(4) Terminate services that are not economical or no longer needed.

(INTENTIONALLY BLANK)

ENCLOSURE C

REFERENCES

a. DoDD 5105.19, 15 February 2022, “Defense Information Systems Agency (DISA)”

b. DoDD 8000.01 CH 1, 27 July 2017, “Management of the Department of Defense Information Enterprise (DoD IE)”

c. DoDI 8500.01 CH 1, 7 October 2019, “Cybersecurity”

d. DoDI 8010.01, 10 September 2018, “Department of Defense Information Network (DODIN) Transport”

e. DoDI 8110.01, 30 June 2021, “Mission Partner Environment Information Sharing Capability Implementation for the DoD”

f. *Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations*, 19 January 2017

g. Pub. L. 113–291, 19 December 2014, “Federal Information Technology Acquisition Reform Act (FITARA)”

h. Title 48, CFR, chapter 30 (parts 3001–3052), October 2023, “Homeland Security Acquisition Regulation”

i. DoW CIO memo, 3 December 2025, “Mission Partner Environment Modernization”

j. CJCSI 6290.01, 26 July 2024, “Mission Partner Environment Support Request Management Process for Coalition Interoperability Assurance and Validation”

k. Defense Information Service Agency, 2023, Version 6.1, “DISN Connection Process Guide (CPG)”

l. DoDI 8100.04, 9 December 2010, “DoD Unified Capabilities (UC)”

m. DoDI 8420.02, August 3, 2023, “DoD Satellite Communications”

n. CJCSI 6250.01G, July 26, 2022, “Department of Defense Satellite Communications”

o. ICD 503, 25 October 2024, “Intelligence Community Information Environment Risk Management”

p. DoDI 8510.01 CH 1, 19 July 2022, “Risk Management Framework (RMF) for DoD Information Technology (IT)”

q. DoDI 8530.01 CH 3, 25 July 2017, “Cybersecurity Activities Support to DoD Information Network Operations”

r. DoD CIO, 6 June 2024, “Fulcrum: The Department of Defense (DoD) Information Technology (IT) Advancement Strategy ”

s. DoDD 8115.01, 10 October 2005, “Information Technology Portfolio Management”

t. DoDI 8410.02, 28 December 2021, “Support to DoD Information Network Operations”

u. DCDC Campaign OPORD 26-00## (8600-26), “Directing DODIN Operations and DCO-IDM”

v. *Joint Concept for Operating in the Information Environment (JCOIE)*, 25 July 2018

w. DoDD 8140.01, 5 October 2020, “Cyberspace Workforce Management”

x. DoDI 8140.02, 28 December 2021, “Identification, Tracking and Reporting of Cyberspace, Workforce Requirements”

y. DODM 8140.03, 15 February 2023, “Cyberspace Workforce Qualification and Management Program”

z. DoDI 8551.01, 31 May 2023, “Ports, Protocols, and Services Management (PPSM)”

aa. CJCSM 5123.01J, 15 January 2026, “Manual for The Joint Requirements Oversight Council and The Joint Force Requirements Process”

bb. DoDI 8440.02, 17 December 2024, “DoD Implementation of Internet Protocol Version 6 (IPv6)”

cc. DoDI 8330.01, 27 December 2022, “Interoperability of IT, Including National Security Systems (NSS)”

dd. DoDI 5200.44, 16 February 2024, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)”

ee. Title 32, CFR, 20 October 2021, Chapter 1, Subchapter D, Part 117, “National Industrial Security Program Operating Manual (NISPOM)”

ff. DoDM 8530.01, 31 May 2023, “Cybersecurity Activities Support Procedures”

gg. DoDM 5200.01 Volume 1 CH 3, 17 January 2025, “DoD Information Security Program: Overview, Classification, and Declassification”

hh. DoDI 5200.48, 6 March 2020, “Controlled Unclassified Information (CUI)”

ii. DoDI 8320.02 CH 5, 25 June 2020, “Sharing Data, Information, and IT Services”

jj. DoDM 5200.01, Volume 2 CH 4, 28 July 2020, “DoD Information Security Program: Marking of Information”

kk. DTM 25-003, July 2025, “Implementing the DoD Zero Trust Strategy”

ll. DoD CIO, July 2022, ”DoD Zero Trust Reference Architecture, Version 2.0”

mm. DoW CIO memo, 13 November 2025, “Implementing Target Level Zero Trust Across the DoW Enterprise”

nn CNSSP No. 11, 1 June 2013, “Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products”

oo. DoW CIO memo, 18 July 2025, “DoD Information Network Approved Products List.”

pp. DoDM 5200.01 Volume 3 CH 3, 28 July 2020, “DoD Information Security Program: Protection of Classified Information”

qq. Title 22, CFR , 14 October 2021, chapter 1, subchapter M, “International Traffic in Arms Regulations (ITAR)”

rr. Title 15, CFR, 21 October 2021, Chapter VII, Subchapter C, "Export Administration Regulations (EAR)"

ss. DoDD 5230.11, 7 November 2023, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"

tt. DoD CIO, 2024, *Defense Industrial Base Cybersecurity Strategy 2024*

uu. Defense Federal Acquisition Regulation Supplement (DFARS), 25 November 25, Part 252.204, "Safeguarding Covered Defense Information and Cyber Incident Reporting"

vv. NIST SP 800-171, Revision 3, 14 May 2024, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"

ww. NIST SP 800-172, 28 February 2021, "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171"

xx. DoDI 5220.31, 9 May 2023, "National Industrial Security Program (NISP)"

yy. DoD Information Security Risk Management Committee (DoD ISRMC) Charter, October 2024.

zz. DoDI 4000.19, 16 December 2020, "Support Agreements"

aaa. DODI 5530.03, 21 November 2005, "International Agreements"

bbb. Joint Staff J-6, 4 November 25, *Partner Nation Cybersecurity Connection Guide (PNCCG) 2.0*

ccc. DIA Directive 8550.500, 16 November 2023, "JWICS Connection Approval"

ddd. DoDD 3000.05, 13 December 2018, "Stabilization"

eee. DoD Regulation 5500.07-R, May 15, 2024, "Joint Ethics Regulation (JER)"

fff. DoDI 8170.01 CH 2, 12 March 2025, "Online Information Management and Electronic Messaging"

ggg. DISA, December 2025, Revision 3, "Department of Defense (DoD) Cloud Connection Process Guide."

hhh. National Security Memorandum 10, 4 May 2022, "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems"

iii. National Security Agency, September 2022, "Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)," <https://www.nsa.gov/cybersecurity-guidance/>

jjj. DoDI 8420.01, 9 December 2025, "Commercial Wireless Local-Area Network Devices, Systems, and Technologies"

kkk. DoDI 8520.02, 24 May 2011, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling"

lll. DoD CIO memo, 20 December 2019, "DoW Mobile Public Key Infrastructure (PKI) Credentials"

mmm. DoDI 8540.01 CH 1, 28 August 2017, "Cross Domain (CD) Policy"

nnn. DoD Defense Security/Cybersecurity Authorization Working Group, Charter Version 3, 16 August 2021

ooo. CJCSI 3401.01E, 19 May 2014, "Joint Combat Capability Assessment"

ppp. CNSSP No. 15, 20 October 2016, "Use of Public Standards for Secure Information Sharing"

qqq. CNSSP No. 7, 9 December 2015, "Policy on the Use of Commercial Solutions to Protect National Security Systems"

rrr. DoDI 5015.02 CH 1, 17 August 2017, "DoD Records Management Program"

sss. DODM 8180.01, 4 August 2023, "Information Technology Planning for Electronic Records Management

ttt. CJCSI 5760.01B, 26 April 2023, "Records Management Policy for the Joint Staff and Combatant Commands"

uuu. DoDI 1015.10, 6 July 2011, “Military Morale, Welfare, and Recreation (MWR) Programs”

vvv. Title 10, U.S. Code, section 892 - UCMJ Article 92, “Failure to obey order or regulation”

www. Title 18, U.S. Code, Part II, Chapter 212, “Military Extraterritorial Jurisdiction Act of 2000,” Section 3261

xxx. DoDI 3020.41, 27 November 2024, “Operational Contract Support (OCS)”

yyy. CJCSI 3280.01E, 4 February 2022, “National Military Command System”

zzz. DISA Circular 310-130-4, 5 May 2006, “Defense User's Guide to the Telecommunications Service Priority (TSP) System”

aaaa. DoDD 5100.03 CH 1, 7 September 2017, “Support of the Headquarters of Combatant and Subordinate Unified Commands”

bbbb. USSAN 1-07, 5 April 2007, “Implementation of NATO Security Requirements”

cccc. National Information Assurance Partnership, “Protection Profiles,” <https://www.niap-ccevs.org/protectionprofiles>, last accessed 2 July 2026

dddd. NSO STANAG 4774, Ed. 1, 20 December 2017, “Confidentiality Metadata Label Syntax”

eeee. NSO STANAG 4778, Ed. 1, 26 October 2018, “Metadata Binding Mechanism- ADatP”

ffff. NSO STANAG 5636, Ed. 1, 18 November 2022, “NATO Core Metadata Specification (NCMS)”

gggg. DoW Cybersecurity Knowledge Service, <https://cybersecurityks.osd.mil/dodcs/CSProgram/CSProgramsAndActivities/CSSP/Pages/default.aspx>, last accessed 2 July 2026

hhhh. Defense Federal Acquisition Regulation Supplement, <https://www.acquisition.gov/dfars>, last accessed 2 July 2026

iiii. Defense Federal Acquisition Regulation Supplement (DFARS) and Procedures, Guidance, and Information (PGI), <https://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html>, last accessed 2 July 2026

jjjj. FIPS 140-3, 22 September 2019, "Security Requirements for Cryptographic Modules"

kkkk. Central United States Registry, <https://www.cusrac.army.mil>, last accessed 2 July 2026

llll. DoW Cyber Exchange, "8140 Qualification Matrices," <https://www.cyber.mil/dod-workforce-innovation-directorate/dod8140/qualification-matrices>, last accessed 2 July 2026

mmmm. DoW Cloud Computing Security document library, <https://www.cyber.mil/dccs-documents>, last accessed 2 July 2026

INTENTIONALLY BLANK

GLOSSARY

PART I-ABBREVIATIONS AND ACRONYMS

Items marked with an asterisk (*) *have definitions in PART II*

AO	Authorizing Official
ATC	Approval to Connect
ATO	Authorization to Operate
C/S/A	Combatant Command/Service/Agency
C2	command and control
CAO	Connection Approval Office
CCDR	Combatant Commander
CCMD	Combatant Command
CCSA	Combatant Command Support Agent
CD	cross domain
CDRUSCYBERCOM	Commander, U.S. Cyber Command
CDS	cross domain solution
CDSE	Cross Domain Support Element
CIO	chief information officer
CISP	commercial internet service provider
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CNSA	Commercial National Security Algorithm
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COI	community of interest
CORA	Cyber Operational Readiness Assessment
CPG	connection process guide
CSIP	Cybersecurity Inspection Program
CSS	Central Security Service
CSSP	Cybersecurity Service Provider
CSU	channel servicing unit
CUI	Controlled Unclassified Information
DoW	Department of War
DCDC	Department of War Cyber Defense Command
DCO	Defensive Cyberspace Operations
DCS	Data Centric Security
DCSA	Defence Counterintelligence and Security Agency
DDOE	DISA Direct Order Entry

DFAR	Defense Federal Acquisition Regulation
DFARS	Defense Federal Acquisition Regulation Supplement
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITPR	DoW Information Technology Portfolio Repository
DJ-3	Joint Staff Director for Operations, J-3
DMZ	demilitarized zone
DOS	Department of State
DoWIN	Department of War Information Network
DREN	Defense Research Engineering Network
DRSN	Defense Red Switch Network
DSAWG	Defense Security/Cybersecurity Authorization Working Group
DSU	data servicing unit
E	Erlang
E2P	exception to policy
EA	executive agent
FIPS	Federal Information Processing Standard
IATC	Interim Approval to Connect
IAW	in accordance with
IC	Intelligence Community
ICD	Intelligence Community Directive
IG	Installation Gateway
IP	internet protocol
IPSec	Internet Protocol Security
IPv6	Internet Protocol Version 6
IS	information system
ISP	internet service provider
ISRMC	DoW Information Security Risk Management Committee
IT	information technology
ITAR	International Traffic in Arms Regulations
J-6	Joint Staff Directorate for Command, Control, Communications and Computers/Cyber, J-6
J-8	Joint Staff Directorate for Joint Force Development, J-8
JWICS	Joint Worldwide Intelligence Communication System
L2TP	Layer 2 Tunnelling Protocol

MA	mission area
MPE	Mission Partner Environment
MPLS	Multiprotocol Label Switching
MOA	memorandum of agreement
MOU	memorandum of understanding
NATO	North Atlantic Treaty Organization
NCDSMO	National Cross Domain Strategy and Management Office
NFG	NIPRNET Federated Gateway
NIPRNET	Non-classified Internet Protocol Router Network
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NMCC	National Military Command Center
NSA	National Security Agency
NSS	National Security System
PAO	Principal Authorizing Official
PDS	Protected Distribution Systems
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
POC	points of contact
PPSM	Ports, Protocols, and Service Management
RMF	Risk Management Framework
SCI	Sensitive Compartmented Information
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SDREN	SECRET Defense Research Engineering Network
SGA	sponsoring government activity
SGS	SIPRNET Global Information Grid Interconnection Approval Process System
SIPRNET	SECRET Internet Protocol Router Network
SLA	Service-level agreement
SNAP	System/Network Approval Process
SO	system owner
SRG	Security Requirements Guide
STANAG	NATO Standardization Agreement
STIG	Security Technical Implementation Guide
UCMJ	Uniform Code of Military Justice
UCR	Unified Capabilities Requirements
USCYBERCOM	U.S. Cyber Command

USG	U.S. Government
VoSIP	voice over secure IP
VPN	virtual private network
WLAN	wireless local-area network
WMA	Warfighting Mission Area
WPA3	Wi-Fi Protected Access 3
ZT	Zero Trust

PART II – DEFINITIONS

Unless otherwise stated, the terms and definitions contained in this glossary are for the purpose of this instruction only.

authorization. Authorization is the process by which a senior management official, the authorizing official, reviews security and privacy information describing the current security and privacy posture of information systems or common controls that are inherited by systems. As it relates to a Risk Management Framework (RMF) authorization package, a system authorization or a common control authorization can be an initial authorization, an ongoing authorization, or a reauthorization. (NIST SP 800-37)

Authorizing Official. A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation. Also called AO. (NIST SP 800-37)

Cybersecurity Inspection Program. Information systems connected to Defense Information Systems Network-provided transport and information services are subject to electronic monitoring for communications management, configuration management, situational awareness, and network security. This includes on-site and remote vulnerability inspections to check configuration for compliance with Security Technical Implementation Guides and other cybersecurity standards and guidelines. Also called CSIP.

Commercial National Security Algorithm Suite. Replaced Suite B as a result of NSS using more complex approved cryptographic algorithms. For additional information refer to <https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm.>

commercial solution for classified. A commercial off-the-shelf (COTS) end-to-end strategy and process in which two or more COTS products can be combined into a solution to protect classified information. Also called CSfC. (CNSSI No. 4009)

declaration. A mechanism designed to capture relevant data about Department of War information technology (i.e., applications and their underlying PPS). Includes what was formerly known as the registration process and encompasses obtaining data from other federated sources, whether those sources were

populated by other registration activities or via electronic sensing. (DoDI 8551.01)

Defense Information Systems Network Connection Process Guide. Step-by-step guide to the detailed procedures that customers must follow in order to obtain and retain connections to the Defense Information Systems Network. Also called DISN CPG.

Defense Security/Cybersecurity Authorization Working Group. The Defense Security/Cybersecurity Authorization Working Group (DSAWG) is the first accreditation or accreditation review level for the transport, network management, and network segments of the Defense Information Systems Network (DISN) for the Department of War Information Networks (DoWIN). In addition, as the community jury for evaluating risk to the DISN/DoWIN, the DSAWG reviews specific topic areas assigned by the DISN/DoWIN Principal Accrediting Authorities in their capacity as the DoW Information Security Risk Management Committee. Also called DSAWG. (DoDI 8500.01)

demilitarized zone
a. A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet. (NIST SP 800-45)
b. An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the demilitarized zone and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. (NIST SP 800-41)
c. Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's CS policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. (CNSSI No. 4009)
Also called DMZ.

Department of War Information Network. The Department of War Information Network is the set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether connected, interconnected, or stand-alone, including owned and leased communications and computing systems and services, and National Security System. Also called DoWIN.

Department of War Information Technology Portfolio Repository. The Department of War Information Technology Portfolio Repository (DITPR) is a computer system for tracking DoW information technology systems. DITPR

contains basic identifying information regarding all DoW information technology (IT) systems. This includes system names, acronyms, descriptions, sponsoring component, points of contact, and other basic information required for analysis of DoW inventory, portfolios, or capabilities. DITPR and the associated DoW SIPRNET IT Registry are the DoW's authoritative inventories of IT systems that provides senior DoW decision makers a coherent and contextual view of the capabilities and associated system enablers supporting resource decisions and a common central repository for IT system information to support the Defense Business System certification process. Also called DITPR.

Enclave. A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter (CNSSI No. 4009).

Information Systems Security Manager. Individual responsible for the information assurance of a program, organization, system, or enclave.

information service. The offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, which includes electronic publishing but does not include any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunication service (DoDI 8500.01).

IP Tunneling. The encapsulation of an Internet Protocol packet within another packet within a network or between two or more networks.

MINIMIZE. A condition wherein normal data, voice, and video communications traffic is drastically reduced in order that communications traffic connected with an actual or simulated emergency shall not be delayed.

mission partners. Any entity outside the U.S. military or Department of War that collaborates in operations, including other U.S. government agencies, state/local governments, foreign allies, coalition partners, international organizations, academia, and the private sector.

Mission Partner Environment. A capability framework that improves partner information-sharing, data exchange and integrated execution through common standards governance and agreed-to procedures. Mission Partner Environment supports commanders' execution of critical joint warfighting functions: command and control, information, intelligence, fires, movement and maneuver, protection, and sustainment. To perform these warfighting

functions, commanders require services be common to both the enterprise and expeditionary levels of operation for human-to-human collaboration (e.g., chat, secure voice, video teleconferencing, e-mail (with or without attachments), web browsing). Also called MPE.

National Security System
a. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency
(1) the function, operation, or use of which
(a) involves intelligence activities;
(b) involves cryptologic activities related to national security;
(c) involves command and control of military forces;
(d) involves equipment that is an integral part of a weapon or weapons system;
(e) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions;
(2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
b. Subparagraph a.(1)(e) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).
Note: NIST SP 800-59 features a variety of questions to help determine whether a system may be designated a national security system.
Also called NSS. (CNSSI No. 4009)

Ports, Protocols, and Services Management. Registry for all networks/systems ports, protocols, and services for all IP solutions or applications reference. Also called PPSM. (DoDI 8551.01)

Sensitive Compartmented Information. A subset of Classified National Intelligence concerning or derived from intelligence sources, methods, or analytical processes, that is required to be protected within formal access control systems established by the Director of National Intelligence (CNSSI No. 4009).

SIPRNET Global Information Grid Interconnection Approval Process System. Registry for voice, video, and data circuit registrations/connections to classified networks/services. Also called SGS. (DISN CPG)

Security Technical Implementation Guide. Based on Department of War (DoW) policy and security controls. Implementation guide geared to a specific product

and version. Contains all requirements that have been flagged as applicable for the product which has been selected on a DoW baseline. Also called STIG.

Security Requirement Guide. Compilation of control correlation identifiers grouped in more applicable, specific technology areas at various levels of technology and product specificity. Contains all requirements that have been flagged as applicable from the parent level regardless of whether they are selected on a Department of War baseline or not. Also called SRG.

System/Network Approval Process. Registry for voice, video, data circuit registrations and connections to unclassified networks/services granted by the Department of War Chief Information Officer as a temporary exception to policy registrations (DISN CPG).

Tunneling. Encapsulation of one protocol's packet within the payload of another protocol's packets. Note: Tunneling enables one network to send its data via another network's connections. (CNSSI No. 4009)

virtual private network
a. Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.
b. Restricted-use logical computer network that is constructed from the system resources of a physical network by using encryption and/or by tunneling links of the virtual network across the real network.
(CNSSI No. 4009)

(INTENTIONALLY BLANK)

(INTENTIONALLY BLANK)
Inner Back Cover

INTENTIONALLY BLANK
(BACK COVER)