CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

Directive Current as of 4 August 2015

J-6 CJCSI 6211.02D
DISTRIBUTION: A, B, C, JS-LAN, S 24 January 2012

DEFENSE INFORMATION SYSTEMS NETWORK (DISN) RESPONSIBILITIES

References: See Enclosure E.

1. Purpose. This instruction establishes policy and responsibilities for the connection of information systems (ISs) (e.g., applications, enclaves, or outsourced processes) and unified capabilities (UC) products to the DISN-provided transport (including data, voice, and video) and access to information services transmitted over the DISN (including data, voice, video, and cross-domain (CD)).

a. The policy and responsibilities in this instruction are in accordance with (IAW) the Unified Command Plan (UCP) (reference a), Department of Defense Directive (DODD) 5100.20, "National Security Agency/Central Security Services (NSA/CSS)" (reference b), DODD 5105.19, "Defense Information Systems Agency (DISA)" (reference c), DODD 8000.01, "Management of the Department of Defense Information Enterprise" (reference d), DODD 8500.01E, "Information Assurance (IA)" (reference e), Department of Defense Instruction (DODI) 8100.04, "DOD Unified Capabilities (UC)" (reference f), DODI 8500.2, "Information Assurance (IA) Implementation" (reference g), DODI 8510.01, "DOD Information Assurance Certification and Accreditation Process (DIACAP)" (reference h), DODI 8410.02, "NETOPS for the Global Information Grid (GIG)" (reference i), DODI 8551.1, "Ports, Protocols and Services Management (PPSM)" (reference j), and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01 Series, "Information Assurance (IA) and Support to Computer Network Defense (CND)" (reference k).

b. Additional policies governing satellite communications are covered in the CJCSI 6250.01 Series, "Satellite Communications" (reference l).[1]

c. Policy on sensitive compartmented information (SCI) is covered in Intelligence Community Directive (ICD) 503, "Intelligence Community

[1] https://ca.dtic.mil/cjcs_directives/cdata/limited/6250_01.pdf

Information Technology Systems Security Risk Management, Certification and Accreditation" (reference m).

2. Cancellation. CJCSI 6211.02C Series, "Defense Information Systems Network (DISN): Policy and Responsibilities" (reference n) and CJCSI 6215.01C Series, "Policy for Department of Defense Voice Networks with Real Time Services (RTS)" (reference o), are canceled.

3. Applicability. This instruction applies to:

a. The Joint Staff, combatant commands, Services, Defense agencies, and Department of Defense (DOD) field and joint activities, including DOD and Service Nonappropriated Fund Instrumentalities (hereafter referred to as CC/S/As).

b. Mission partners and defense contractors connecting to or using DISN-provided transport or information services transmitted over DISN.

c. Instruction Scope:

(1) DISN-provided transport and information services including, but not limited to, the Nonsecure Internet Protocol Router Network (NIPRNET), SECRET Internet Protocol Router Network (SIPRNET), DISN voice services (i.e., Defense Switched Network (DSN), Defense Red Switch Network (DRSN), Voice over Internet Protocol (VoIP), and Voice over Secure Internet Protocol (VoSIP)), DISN Video Services (DVS), Enhanced Mobile Satellite Services (EMSS), and DISN-Leading Edge Services (DISN-LES).

(2) UC products (hardware and software) and end-to-end voice, video, data, and application services funded or operated by the CC/S/As, authorized mission partners, or by defense contractor users IAW DODI 8100.04 (reference f).

(3) ISs and networks connected to DISN-provided transport and/or information services IAW the "DISN Connection Process Guide" (reference p).

(4) Outside Instruction Scope. Information technology (IT), security, connection, and DOD Chief Information Officer (CIO) waiver requirements for non-DISN DOD networks such as the Defense Research Engineering Network (DREN), SECRET Defense Research Engineering Network (SDREN), Combined Enterprise Regional Information Exchange System (CENTRIXS), or other DOD networks (e.g., standalone or training enclaves) not connected to the DISN are outside the scope of this instruction. For guidance on these networks, contact the DOD CIO and/or network owners (e.g., Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) for DREN and SDREN). For information on multinational networks, see DODI 8110.1, "Multinational

Information Networks Implementation" (reference q), or CJCSI 6285.01, "Multinational Information Sharing (MNIS) Operational Systems Requirements Management Process" (reference r).

4. Policy. See Enclosure B.

5. Definitions. See Glossary. Major source documents for definitions in this instruction are Joint Publication (JP) 1-02, "DOD Dictionary of Military and Associated Terms" (reference s), and Committee on National Security Systems Instruction (CNSSI) 4009, "National Information Assurance Glossary" (reference t).

6. Responsibilities. See enclosures C and D.

7. Summary of Changes

a. Replaces the policy and responsibilities previously published in CJCSI 6211.02C (reference n) and CJCSI 6215.01C (reference o).

b. Updates Joint Staff responsibilities based on disestablishment of the Command, Control, Communications and Computer Systems Directorate (J-6).

c. Removes specific process steps and procedures for connection to and management of DISN-provided transport and information services; performance measurement standards in terms of management thresholds and performance objectives; and implementation guidance supporting engineering solutions, which will be maintained and updated as required by the Defense Information Systems Agency (DISA) IAW DODD 5105.19 (reference c).

d. Updates Unified Cross Domain Management Office (UCDMO) roles and responsibilities.

e. Adds guidance on prioritization of CD requirements.

f. Adds guidance on Commercial Internet Services Provider (ISP) Connection Waivers.

g. Removes DISN Security Information Assurance Program enclosure. Updates guidance based on the Cyber Security Inspection Program, which can be found in CJCSI 6510.01 Series (reference k).

h. Provides guidance on use of commercially-provided transport and information services (Telecommunications Act of 1996 (reference u)).

i. Updates guidance on use of CC/S/A-provided connections (e.g., backside connections) to other DOD entities, mission partners, and defense contractors.

j. Updates guidance on Internet Protocol (IP) tunnels.

k. Replaces the term "non-DOD" with the terms "mission partner" as defined in DODD 8000.01 (reference d) and "defense contractor" as defined in title 41, United States Code, chapter 1, "defense contractor" (reference v).

l. The Department of Defense is in the process of updating terminology for a number of terms used in the current certification and accreditation process. Both old and updated similarly defined terms are used throughout this instruction. Such similar terms include Designated Accrediting Authority (DAA) with Authorizing Official; certification with security control assessment; and accreditation with authorization to operate. These terms are all defined in CNSSI 4009 (reference t) terminology.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--
http://www.dtic.mil/cjcs_directives.

9. Effective Date. This instruction is effective upon receipt.

CRAIG A. FRANKLIN
Major General, USAF
Vice Director, Joint Staff

Enclosures:

A -- DEFENSE INFORMATION SYSTEMS NETWORK (DISN) BACKGROUND
B -- POLICY
C -- JOINT STAFF, COMBATANT COMMAND, SERVICE, DEFENSE AGENCY, DOD FIELD ACTIVITY, AND JOINT ACTIVITY SPECIFIC RESPONSIBILITIES
D -- JOINT STAFF, COMBATANT COMMAND, SERVICE, DEFENSE AGENCY, DOD FIELD ACTIVITY, AND JOINT ACTIVITY COLLECTIVE RESPONSIBILITIES
E -- REFERENCES

DISTRIBUTION

A, B, C, and JS-LAN plus the following:

	Copies
Chief Information Officer, Department of Defense	2
Under Secretary of Defense for Intelligence	2
Commandant of the Coast Guard	2
Director, Defense Security Service	2

OPR 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 SIPR and NIPR Joint Electronic Library Web sites.

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

ENCLOSURE A

DEFENSE INFORMATION SYSTEMS NETWORK (DISN) BACKGROUND

1. DISN. The DISN is a composite of DOD-owned and leased subsystems and networks. It is DOD's worldwide enterprise-level infrastructure providing end-to-end information transfer in support of DOD operations. The DISN facilitates information resource management and supports national security as well as DOD needs. It also furnishes network services to DOD installations and deployed forces. Those services include data, voice, video, CD, messaging, and other unified capabilities along with ancillary enterprise services such as directories. The DISN is comprised of three segments: sustaining base, DISN transport, and deployed infrastructure.

a. The sustaining base infrastructure (i.e., base, post, camp, station, and enclaves) interfaces with the DISN-provided transport infrastructure to support strategic/fixed environment user requirements within the CC/S/A base infrastructures and deployed warfighter. The sustaining base infrastructure is the responsibility of the CC/S/A.

b. DISN-provided transport infrastructure delivers information transfer services between CC/S/A installations and facilities; connections to external mission partners and defense contractors; and connections to the deployed infrastructure (e.g., warfighter) is the responsibility of DISA.

c. The deployed warfighter and associated Combatant Commander's infrastructure support the Joint Task Force and/or Combined Task Force. The combatant command and subordinate Service components have primary responsibility for the deployed warfighter and associated infrastructure within the theater.

d. The DISN provides the transport infrastructure and makes available a common set of enterprise services necessary to meet operational requirements.

e. DISN information transfer facilities support secure transport requirements and services for sub-networks such as the NIPRNET, SIPRNET, DISN voice transport and information services (e.g., DSN, DRSN, and UC), DVS Network, EMSS, DISN-LES, and other government agency networks.

f. The DSN and DRSN are worldwide private-line voice sub-networks of the DISN that provide non-secure and secure services to authorized users between the CC/S/A sustaining base and deployed warfighter infrastructures via the DISN provided transport infrastructure.

g. DISN is designated as a mission critical and mission assurance category (MAC) I (e.g., High) national security system (NSS). The DISN and its sub-networks (including, but not limited to NIPRNET, SIPRNET, DISN Voice, and video services (i.e., DSN, DRSN, VoIP, and VoSIP), DVS, EMSS, and DISN-LES) must be operated to meet criteria established in DISA Circular 310-130-2, "Communications Requirements" (reference w), and protected IAW DODD 8500.01E (reference e) and other 8500 Series issuances.

2. DISN and the Global Information Grid (GIG). The DISN infrastructure is an integral part of the GIG.

a. GIG 2.0 is the DOD effort to evolve the GIG, including the DISN infrastructure, into a seamless, single information environment optimized for the warfighter to achieve and maintain the information advantage as a critical element of national power (GIG 2.0 Concept of Operations (CONOPS) (reference x)).

b. This single information environment will provide an agile and flexible infrastructure that supports military operations while under duress and is capable of rapid configuration change across the terrestrial, space, and aerial layers.

c. Future DISN-provided transport and information services will be developed to support the seamless integration of GIG 2.0 to satisfy tactical service requirements to the warfighter.

ENCLOSURE B

POLICY

1. DISN Management

a. The Department of Defense shall use DISN-provided transport to satisfy DOD information transfer requirements between DOD installations and facilities, and for external connections to mission partner and defense contractor ISs and networks IAW DODI 8100.04 (reference f).

b. Current warfighter requirements for DISN-provided transport and information services are documented in the GIG 2.0 Initial Capabilities Document (ICD) (reference y).

c. The DISN shall be managed, operated, and defended as part of a unified DOD information enterprise as an integral component of DOD information networks IAW DODD 8000.01 (reference d), DODI 8500.2 (reference g), and consistent with DODI 8410.02 (reference i).

(1) Direction of DOD information networks operations and defense shall be IAW the UCP (reference a).

(2) DISN-provided transport and information services shall employ:

(a) Certified information assurance (IA) personnel IAW DODD 8570.01, "Information Assurance Training, Certification and Workforce Improvement" (reference z).

(b) Strict change management processes and procedures to implement security requirements contained in applicable Security Technical Implementation Guides (STIGs).

(c) Only those IP protocols, data services, and associated ports that have undergone a vulnerability assessment and authorization process IAW DODI 8551.01 (reference j).

(d) IS configuration approved in the Interoperability Certification letter IAW CJCSI 6212.01, "Interoperability and Supportability of Information Technology and National Security Systems" (reference aa) and the DOD Information Assurance Certification and Accreditation Process (DIACAP) package.

(3) UC equipment and software that are leased, procured (whether ISs or services), or operated by the CC/S/As shall be in compliance with Unified Capabilities Requirements (UCR) (reference bb) as specified in DODI 8100.04 (reference f), or have an approved Information Support Plan IAW DODI 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" (reference cc) that includes UC equipment or products.

(4) CC/S/As shall procure or operate UC products listed on the DOD UC Approved Products List (APL),[2] as applicable, unless granted an exception to policy IAW DODI 8100.04 (reference f).

(5) Supply Chain Risk Management (SCRM) will be instituted using the process IAW Directive-Type Memorandum (DTM) 09-016, 25 March 2010, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems" (reference dd).

2. DISN Connection

a. All connections to the DISN shall be IAW the DISN Connection Process Guide (reference p).[3]

b. DOD ISs

(1) DOD ISs connected to the DISN-provided transport and information services or commercial transport must be authorized to operate IAW applicable guidance and processes including, but not limited to, DODI 8510.01 (reference h), DODI 8100.04 (reference f), or ICD 503 (reference m)). This includes DOD-owned ISs and ISs operated on behalf of the Department of Defense (e.g., contract, memorandum of agreement (MOA), or memorandum of understanding (MOU)) that receive, process, store, display, or transmit DOD information, regardless of classification or sensitivity.

(2) DOD ISs must be registered in the DOD Information Technology Portfolio Repository (DITPR) (i.e., DITPR NIPRNET or SIPRNET IT Registry application) by the responsible CC/S/A prior to connection IAW DOD CIO memorandum, "DOD IT Portfolio Repository (DITPR) and DOD SIPRNET IT Registry Guidance" (reference ee).

[2] http://www.disa.mil/ucco/
[3] http://www.disa.mil/connect/

(3) DOD ISs connected to the DISN-provided transport capability shall be discoverable, assessable, operated, and managed securely through continuous compliance, monitoring, and risk management IAW DODI 8500.2 (reference g).

c. Mission Partner and Defense Contractor ISs

(1) Mission partner and defense contractor ISs connected to the DISN shall be authorized to operate IAW applicable federal, Intelligence Community (IC), or DOD guidance and processes. For example, defense contractor unclassified ISs operating on behalf of the Department of Defense would comply with DOD 8510.01 (reference h), federal mission partners not identified as an NSS would comply with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, "Guide for Applying Risk Management Framework to Federal Information Systems" (reference ff), IC entities would comply with ICD 503 (reference m), and defense contractor ISs that process classified information would comply with DODI 5220.22, "National Industrial Security Program (NISP)" (reference gg) for defense contractor ISs.

(2) Non-U.S. mission partner and defense contractor (when applicable) access to DOD information must be in compliance with DODD 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations" (reference hh), the International Traffic in Arms Regulations (ITAR) (reference ii), and the Export Administration Regulations (EAR) (reference jj).

(3) Defense contractor and other mission partner ISs operating on behalf of the Department of Defense (e.g., contract or MOA) must be registered in the DITPR (NIPRNET or SIPRNET instance) by the sponsoring CC/S/A prior to connection.

(4) CC/S/A must include documentation and artifacts equivalent in detail and scope to those provided by DOD entities in the request for a direct or indirect connection to the DISN IAW DISN Connection Process Guide (reference p).

(5) All mission partner and defense contractor connections to DISN-provided transport and information services require a sponsoring CC/S/A and a separate connection request. Mission partner and defense contractor system access must be limited only to the information and services required to execute the DOD-approved mission.

(6) All connection requests for a mission partner or defense contractor IS to the DISN-provided transport and information services must be endorsed, validated, and submitted by the CC/S/A IAW the DISN Connection Process Guide (reference p) and the Defense IA Security Accreditation Working Group (DSAWG), DISN/GIG Flag Panel processes.

(7) Defense contractor ISs connected to the DISN-provided transport and information services must comply with connection guidelines issued by this instruction and DISA as the operating entity. In addition, if the defense contractor ISs are classified, they must comply with DOD 5220.22-M, "National Industrial Security Program Operating Manual" (reference kk).[4]

d. CC/S/As will register[5] IS connection information as required IAW the DISN Connection Process Guide (reference p).

e. Use of non-DISN commercial transport as an alternative to DISN-provided transport requires a GIG Waiver Panel (GWP) approved Commercial ISP Connection Waiver. See paragraphs 10 and 11 of Enclosure D on Commercial ISP Connection Waivers.

f. Site inspection, remote scanning, acceptable authorized security posture (DODI 8510.01 (reference h)), and providing computer network defense (CND) services IAW DODD O-8530.1, "Computer Network Defense (CND)" (reference ll), are conditions for a DOD IS, mission partner IS, or defense contractor IS to obtain and retain an authority to connect (ATC) or interim authority to connect (IATC) IAW the DISN Connection Process Guide (reference p).

g. Mission partner or defense contractor IS connection to DISN-provided transport and information services must be through an established DISN Demilitarized Zone (DMZ) (e.g., FED DMZ) and will follow DISN DMZ security requirements.

---

[4] DSS is the authorizing official (DAA) for contractor classified ISs under the authority of DODI 5220.22 (reference gg) and the DOD 5220.22-M (reference kk). CC/S/As are the authorizing official (DAA) for contractor unclassified ISs under the authority of DODI 8510.01 (reference h).

[5] Network Information Center (www.nic.mil) for all unclassified information; SIPRNET Support Center (www.ssc.smil.mil) for all classified information; Systems/Network Approval Process (SNAP) (https://snap.dod.mil) for unclassified voice, video, data circuit registrations and connections, unclassified voice switches; and DOD CIO GIG Waivers for Internet Service Provider registration; SIPRNET GIG Interconnection Approval Process (GIAP) System (SGS) (https://pnp.cert.smil.mil) for classified voice, video, data circuit registrations and connections; and cross domain solution (CDS) deployments; and Ports, Protocols, and Services Management (PPSM) (https://pnp.cert.smil.mil) on SIPRNET for all networks/systems ports, protocols, and services for all IP solutions or applications, including VoIP and VoSIP.

3. Minimize. The Department of Defense will utilize means available (user or technical) to reduce (i.e., minimize) and/or remove nonessential data, voice, and video communications traffic during times of surge or crisis as required to ensure communications availability to meet DOD mission requirements.[6]

a. Controls on users or communications can include, but are not limited to, blocking, routing, usage, or availability controls to ensure prompt transmission of communications traffic in support of mission requirements.

b. The directive to implement minimize shall indicate the type of communications traffic to be reduced and/or removed.

4. DISN Voice Precedence[7]

a. All DISN service requests for voice precedence requirements must be forwarded through the requestor's chain of command to the appropriate approval authority (see Enclosure D).

b. The use of IMMEDIATE and PRIORITY precedence by DOD personnel assigned to non-U.S. (foreign government adviser, United Nations (UN), North Atlantic Treaty Organization (NATO), etc.) organizations must be approved by the appropriate CC/S/A. Requests for FLASH or FLASH OVERRIDE must be validated by the appropriate CC/S/A and approved by the Joint Staff.

c. Temporary upgrading of voice precedence to support CC/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 combatant command.

d. Approvals of FLASH and FLASH OVERRIDE access must be provided to DISA and the Joint Staff J-8.

5. Computer Network Defense Service Providers (CNDSPs)

a. DOD ISs connected to the DISN-provided transport and information services must be aligned to an accredited CNDSP IAW DODD O-8530.1 (reference ll) prior to connection.

---

[6] MINIMIZE is 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.

[7] In communications, a priority of importance designation is assigned by the originator.

b. For mission partner and defense contractor ISs, the sponsoring CC/S/A must ensure a signed agreement (e.g., MOA) or contract defines the CNDSP requirements, requirements specified in DODD O-8530.1 (reference ll), are included in the agreement, and these CNDSP requirements are implemented prior to connection.

6. Cross Domain (CD) Connections

a. Enterprise CD services or centralized cross domain solutions (CDSs) will be used for automated DOD CD information transfer requirements.

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

c. Enterprise CD services, centralized CDSs, and point-to-point CDSs will employ CDSs from the Cross Domain Baseline, unless an exception letter or a Plan of Action and Milestones (POA&M) is approved through the Cross Domain Resolution Board (CDRB), DSAWG, and DISN/GIG Flag Panel.

d. Life-cycle security management of cross domain security configurations is required. In non-enterprise operating environments, the target Regional or Point-to-Point CDS hosting environment must identify (appoint in writing) individual(s) responsible to oversee the day-to-day security management, configuration, and established information transfer processes. This (or these) individual(s) are responsible for reporting security incidents to the local/site Information Assurance Manager.

e. DISN connections among ISs of different security domains internal to the DOD and external (e.g., mission partner) will be IAW this instruction, DODD 8500.01E (reference e), DODD O-8530.1 (reference ll), and other applicable DOD issuances and instructions. Connections to SCI ISs must be IAW ICD 503 (reference m).

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

7. Cyber Security Inspection Program (CSIP) and Monitoring

a. ISs connected to DISN-provided transport and information services are subject to the CSIP IAW CJCSI 6510.01 (reference k). This includes a tiered program of vulnerability assessments, Blue Team Vulnerability Evaluations and Intrusion Assessments, cyber security inspections, and Red Team operations 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.

b. 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 IA standards and guidelines.

c. Defense contractor systems operating under the NISP will adhere to the policies, procedures, and standards established under the NISP.

8. Official and Authorized Use of the DISN. The DISN and connected DOD ISs will be used for official and authorized purposes IAW DOD Regulation 5500.7-R, "Joint Ethics Regulation (JER)" (reference mm)[8] and DTM 09-026, "Responsible and Effective Use of Internet-Based Capabilities" (reference nn).

9. Records Management. Electronic records stored on or pertaining to the DISN will be managed IAW title 44, United States Code, Chapters 31, 33, and 41 (reference oo); DODD 5015.2, "DOD Records Management" (reference pp); DOD 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard" (reference qq), and CJCSI 5760.01 Series, "Records Management Policy for the Joint Staff and Combatant Commands" (reference rr).

[8]Federal government communication systems and equipment (including government-owned telephones, facsimile machines, electronic mail, Internet systems, and commercial systems when use is paid for by the federal government) shall be for official use and authorized purposes only.

(INTENTIONALLY BLANK)

ENCLOSURE C

JOINT STAFF, COMBATANT COMMAND, SERVICE, DEFENSE AGENCY, DOD FIELD ACTIVITY, AND JOINT ACTIVITY SPECIFIC RESPONSIBILITIES

1. Joint Staff. The Chairman of the Joint Chiefs of Staff is responsible for developing DISN joint policy IAW DODD 8500.01E (reference e), DODI 8100.04 (reference f), DODI 8510.01 (reference h), and DODD 8115.01, "Information Technology Portfolio Management" (reference ss), and facilitating communications with Combatant Commanders to improve the adequacy and effectiveness of communications, command and control, IA, computing services, interoperability and standardization, DOD enterprise services, engineering, and acquisition functions IAW DODD 5105.19 (reference c).

a. The Director for Operations, J-3 shall:

(1) Advise the Chairman on the responsiveness and readiness of the DISN to support command and control of operating forces in the event of war or threats to national security in coordination with J-8 and United States Strategic Command (USSTRATCOM).

(2) Advise and recommend, when appropriate, implementation of communications traffic controls (MINIMIZE) to ensure National Military Command System (NMCS) communications availability for mission requirements IAW CJCSI 3280.01, "National Military Command System (U)" (reference tt).

b. The Director for Force Structure, Resources, and Assessments, J-8 shall:

(1) Advise the Chairman on command, control, communications, and computer and information systems requirements and priorities in coordination with DOD CIO.

(2) Provide advice and assistance to the Joint Staff directorates and combatant commands on DISN policy and responsibilities to include obtaining approval to connect to DISN (e.g., mission partners or defense contractors), CD transfer requirements, and DOD information networks.

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

(4) Review and approve or disapprove all requests for FLASH and FLASH OVERRIDE DSN/DRSN service after validation by a Combatant Commander,

Service Chief, or Director of a Defense Agency.

(5) Serve as the Warfighting Mission Area (WMA) Principal Accrediting Authority (PAA) for the Chairman IAW DODI 8510.01 (reference h).

(6) Appoint a flag-level WMA PAA[9] representative to the DISN/GIG Flag Panel.

(7) Appoint a representative in the military grade of O-5/O-6 or U.S. government (USG) civilian equivalent as primary representative to the GWP and USG alternates with GWP voting authority.

(8) Appoint a representative in the military grade of O-6 (e.g., Colonel) or USG civilian equivalent as primary representative to the DSAWG and USG alternates with Service DSAWG voting authority.

c. The Joint Staff CIO shall implement applicable responsibilities in Enclosure D for Joint Staff networks.

2. Combatant Commanders. In addition to responsibilities outlined in Enclosure D, the Combatant Commanders shall:

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

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

c. Review and submit service restoration priority requests IAW with DISA Circular 310-130-4, "Defense User's Guide to the Telecommunications Service Priority (TSP) System" (reference uu).

d. Submit DISN-provided transport and information services requirements through designated Service Executive Agent channels to DISA IAW DODD 5100.03, "Support of the Headquarters of Combatant and Subordinate Unified Commands" (reference vv).

[9] DOD PAAs are appointed for the four GIG mission areas (MAs) consisting of the WMA, the Enterprise Information Environment MA (EIEMA), the Defense Intelligence MA (DIMA), and the Business Mission Area (BMA).

e. Minimize

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

(2) 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), USSTRATCOM, CC/S/As, other USG agencies, and foreign mission partners as deemed appropriate.[10]

f. Cross Domain Responsibilities. If a combatant command does not designate a Cross Domain Support Element (CDSE) or an existing office to carry out combatant command CD responsibilities outlined in Enclosure D, the combatant command shall:

(1) Request CD support from the combatant command's Service Executive Agent IAW DODD 5100.03 (reference vv) or another CC/S/A CDSE.

(2) Develop an MOA outlining combatant command and supporting CDSE responsibilities (Enclosure D), including the life-cycle costs, sustainment, and management of any combatant command-directed CDS implementation support.

g. Provide USSTRATCOM and DISA read access to combatant command level vulnerability management ISs (e.g., Vulnerability Management System (VMS)), as requested.

h. Approve or disapprove outside the United States local commander requests for DSN voice service (personal or unofficial use). Notify DISA DSN Program Management Office (PMO) of approvals.

i. Review and revalidate secure voice conference requirements annually.

3. Commander, U.S. Special Operations Command (CDRUSSOCOM). In addition to the responsibilities outlined in paragraph 2 (above) and Enclosure D, the CDRUSSOCOM shall:

a. Coordinate with theater combatant commands 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. If service requirement is for a CDS, provide a courtesy copy to the UCDMO.

[10] Emergency Action Procedures -- CJCS Volume IX (CJCS LERTCON Procedures) (U) (reference ww).

4. Commander, U.S. Strategic Command (CDRUSSTRATCOM). In addition to the responsibilities outlined in paragraph 2 (above) and Enclosure D, the CDRUSSTRATCOM shall:

a. Direct DOD information networks operations and defense of DOD information network including the DISN and synchronize cyberspace operations planning in coordination with CC/S/As IAW the UCP (reference a).

b. Delineate U.S. Cyber Command (USCYBERCOM) roles and responsibilities to plan, coordinate, and direct DISN network operations and defense.

c. Issue USSTRATCOM warning and tactical orders and directives[11] through USCYBERCOM to provide instructions on the operation and defense of DISN IAW UCP (reference a).

d. Prioritize Service and combatant command CD information transfer requirements based on impact description provided by the combatant command or Service's ability to execute assigned mission(s) in support of the National Military Strategy (reference xx).

e. Minimize

(1) Plan for the implementation of certain communications traffic controls worldwide during surges or crisis (actual or simulated) in coordination with Joint Staff (NMCC).

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

f. Direct Command Cyber Readiness Inspections (CCRIs) of DOD DISN-provided transport and information services and connected ISs IAW the USSTRATCOM/USCYBERCOM CSIP.

g. Monitoring Connections

[11] Currently USSTRATCOM-issued warning and tactical orders and directives include alert orders (ALERTORDs), deployment orders (DEPORDs), execute orders (EXORDs), fragmentary orders (FRAGOs), IA Vulnerability Notices, operations orders (OPORDs), planning orders (PLANORDs), tasking orders (TASKORDs), and warning orders (WARNORDs). Previous issued orders and directives include Communications Tasking Orders (CTOs), Coordination Alert Messages (CAMs), GIG Vulnerability Bulletins, Network Defense Tasking Messages (NDTMs), and Operational Directive, Message (ODM).

(1) Coordinate with CC/S/As on monitoring of connected enclaves.

(2) Issue procedures for coordination and notification of USSTRATCOM-directed remote compliance monitoring and scanning of CC/S/A ISs.

(3) USSTRATCOM -directed scanning pre-notification may be in the form of notices posted to a designated USSTRATCOM SIPRNET Web site or direct USSTRATCOM communications to the Authorizing Official (DAA).

h. DISN Related Panels, Boards and Working Groups

(1) Appoint a flag-level chair for the DISN/GIG Flag Panel.

(2) Appoint a representative in the military grade of O-5/O-6 or USG civilian equivalent as primary representative to the GWP and USG alternates with GWP voting authority.

(3) Appoint a representative in the military grade of O-6 or USG civilian equivalent as primary representative to the DSAWG and USG alternates with USSTRATCOM DSAWG voting authority.

(4) Appoint a representative in the military grade of O-6 or USG civilian equivalent representative to the CDRB.

5. Service Chiefs. In addition to responsibilities outlined in Enclosure D, the Service Chiefs shall:

a. Provide communications capability to meet combatant command validated connectivity requirements, including combatant command DISN connectivity through DISN collection and distribution sites for both deployed and garrison local infrastructures. ISs must be focused on supporting operational requirements of the combatant command or parent Service and be capable of supporting contingency operations.

b. Approve the connection of tenant ISs to base/post station transport and services and to DISN provided transport and services. This approval to operate by the Service must be included in the DISN connection approval request package submitted to DISA and ensure an MOA is established to provide CND services for these connections.

c. Implement CSIP teams to conduct Service cyber security inspections, Blue Team Vulnerability Evaluations and Intrusion Assessments, and vulnerability assessments of Service ISs connected to DISN-provided transport and information services.

d. In addition to the responsibilities outlined in Enclosure D, Services will perform the following tasks in support of Service CD information transfer requirements:

(1) Designate a CDSE to work on Service CD activities and issues with the UCDMO.

(2) Support Security Test and Evaluation (ST&E) of CDSs IAW DOD and IC guidance to implement security controls as required.

(3) As Service Executive Agent IAW DODD 5100.03 (reference vv), when requested by combatant command, provide CD support service per Enclosure D. An MOA or MOU outlining combatant command and supporting Service CDSE responsibilities is required and shall address the life cycle costs, sustainment, and management of any combatant command-directed CDS.

e. 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 (POPs) on these bases, posts, camps, and stations. Site support must be specified in procedural documentation and coordinated between the Service Headquarters and DISA Headquarters.

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

g. Provide Headquarters of Combatant 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 DODD 5100.03 (reference vv).

h. <u>DISN Related Panels, Boards, and Working Groups</u>

(1) Appoint a representative in the military grade of O-5/O-6 or USG civilian equivalent as primary representative to the GWP and USG alternates with GWP voting authority.

(2) Appoint a representative in the military grade of O-6 or USG civilian equivalent as primary representative to the DSAWG and USG alternates with Service DSAWG voting authority.

(3) Appoint a representative in the military grade of O-6 or USG civilian equivalent representative to the CDRB.

6. Director, Defense Information Systems Agency (DISA). In addition to responsibilities outlined in Enclosure D, the Director, DISA shall:

a. DISN Management and Operation

(1) Provide DISN-provided transport and information services used for data, voice, video, and cross domain through a combination of terrestrial, aerial, satellite assets, and services IAW DODD 5105.19 (reference c). Transport services include information transfer services between CC/S/A installations, facilities, and enclaves, for connections to external mission partner and defense contractor ISs and networks, and wide area network information transfer.

(2) Manage process for connection to all DISN-provided transport and information services.[12]

(3) Direct operation and management of DISN-owned and leased DISN subsystems and networks to meet CC/S/A operational requirements.

(4) Maintain configuration management of the DISN-provided transport and information services.

(5) Implement and coordinate the necessary actions to provide end-to-end responsibility, management, and operations of DISN telecommunications and UC.

(6) Prescribe the threshold and objective performance metrics that will be used for the DISN-provided transport and information services in DISA Circular 310-130-2, (reference w) and based on UCR (reference bb).

(7) Provide dialing and numbering plans for DISN-provided transport and information services.

(8) Specify, coordinate, and document Service support required for DISN equipment located at bases, posts, camps, and stations.

(9) Monitor the effectiveness of the DISN-provided transport and information services in satisfying user requirements and respond to combatant command and Service requests for reports on IS performance.

(10) Perform required system engineering and modeling to achieve the optimal network design and implementation approach.

[12] DISA connection process can be found at http://www.disa.mil/connect/ on (NIPRNET) and http://www.disa.smil.mil/connect/ on (SIPRNET).

(11) Identify and promulgate performance standards, security implementation guidance (i.e., STIG), and supporting engineering solutions for DISN-provided transport and information services (e.g., availability and response time), and mission survivability requirements based on the Joint Staff validated requirements and the UCR (reference bb).

(12) Support the combatant commands in creating a User-Defined Operational Picture for their areas of responsibility (AORs).

(13) Develop process to record the technical and operational characteristics of active connections, in addition to pending and operational CC/S/A CD information transfer requirements.

(14) Assess the technical, programmatic, and operational feasibility of adding new transport and information services capabilities to the DISN as directed by DOD CIO.

(15) Identify technical solutions to close joint capability gaps validated and provided by the Joint Staff with DISN-provided transport and information services.

(16) Establish and operate a contingency response capability to allow for rapid extension of DISN-provided transport and information services into regions around the world to support DOD contingency operations.

(17) Identify existing non DISN-provided transport and information services utilized by CC/S/As and provide recommendations on those services, which could be incorporated into future DISN-provided transport and information services capabilities.

(18) Provide program objective memorandum recommendations with cost data to CC/S/As including UC Master Plan with UC migration strategy, transition engineering solutions, and recommendations for the modernization of DISN-provided transport and information services IAW DODI 8100.4 (reference f).

(19) Publish a catalog of DISN-provided transport and information services and cost-effective and economical rates IAW the Office of the Secretary of Defense cost recovery program based on site subscription fees.[13]

[13] DISA computing services catalogs of service and rates can be found at http://www.disa.mil/computing /index.html and http://www.disa.smil.mil/computing/index.html. The DISN Telecommunications Business Service Catalog can be found at http://disa.mil/ns/customer_service/catalog.html.

b. DISN-Provided Transport and Information Services Connection Process

(1) Maintain a DISN Connection Process Guide (reference p) describing steps and requirements for connection to DISN-provided transport and information services IAW DODI 8100.04 (reference f) and DODI 8500.2 (reference g).

(2) Update DISN Connection Process Guide (reference p) IAW DOD CIO issuances and USSTRATCOM warning and tactical orders and directives issued through USCYBERCOM on the operation and defense of the DISN IAW UCP (reference a), as needed.

(3) Process, review, and approve CC/S/A validated DISN connection requests.

(4) Ensure that the connection meets technical and interoperability requirements IAW DODI 4630.8 (reference cc) and CJCSI 6212.01 (reference aa).

(5) Ensure DOD, mission partner, or defense contractor ISs connected to the DISN have authorizations to operate IAW DODI 8510.01 (reference h), for defense contractor classified ISs (DOD 5220.22-M (reference kk)), or other governing policy and process as described in Enclosure B (Paragraph 2).

(6) Track and approve all primary connections/points of presence (POPs) to the DISN, employing standard equipment configuration and IAW published STIGs.

(7) Defense Contractor Classified ISs

(a) Defense contractor classified ISs are subject to security standards that are equivalent to the published STIGs and DOD 5220.22-M (reference kk).

(b) Ensure MOA is signed outlining roles and responsibilities for both DISA and Defense Security Service (DSS) in the connection approval process and oversight of cleared defense contractor connection to the DISN.

(8) Defense Contractor Unclassified ISs. Defense contractor operating ISs that process unclassified information on behalf of the DOD are subject to security standards to the published STIGs and DODI 8500.2 (reference g).

(9) In coordination with DSAWG, review Commercial ISP Connection Waiver requests to DOD ISs (network and standalone) and make recommendations to the DOD CIO GWP.

(10) Develop a process to allow CC/S/As with DOD CIO Commercial ISP Connection Waiver to order commercial transport and information services through DISA.

c. Security Control Assessment (Certification) and Authorization to Operate (Accreditation) for DISA-Provided DISN Networks

(1) Authorize operation of DISN networks IAW DODI 8510.01 (reference h).

(2) Authorize the DISN SIPRNET to process SECRET NATO information, IAW United States Security Authority for NATO Affairs Instruction 1-07 (reference yy).[14]

d. DISN Monitoring, Assessment and Inspections

(1) Monitor DISN connected enclaves in support of USSTRATCOM/ USCYBERCOM.

(a) Assess enclave compliance with DOD vulnerability management requirements as directed by USSTRATCOM/USCYERBCOM.

(b) Conduct onsite and/or remote compliance scanning and vulnerability assessments to ensure ISs provide adequate security as directed by USSTRATCOM/USCYBERCOM.

(2) Conduct SIPRNET and NIPRNET compliance validation visits as directed by USSTRATCOM/USCYBERCOM. Compliance validation visits will, at a minimum, consist of traditional security checks, scanning of the connected network, and a CDS compliance inspection, if a CDS is operational. This includes the following tasks:

(a) Maintain reports of the visits on the DOD database.

(b) Provide report access to the DOD CIO; the Joint Staff; USSTRATCOM; the Director, Operational Test and Evaluation (DOT&E); and concerned CC/S/As for review.

(c) Establish processes and procedures for the documentation of site response to compliance visit open findings.

(d) Collaborate with the UCDMO and NSA/CSS to develop requirements and standards for CDS compliance inspections, IAW Committee on National Security Systems (CNSS) guidelines.

[14] NATO information must be handled IAW United States Security Authority for NATO Affairs Instruction 1-07 (reference yy).

(e) Assess security implementation on connected environments from the cryptographic device to the workstation for classified connections (i.e., SIPRNET) and from the point of presence of the connection to the workstations for unclassified connections (i.e., NIPRNET).

(f) Conduct scheduled or USSTRATCOM directed CDS compliance inspections.

(g) Conduct internal cyber security inspections of DISA owned and/or managed portion of DISN to determine DISN readiness and compliance with security policy, procedures, and practices.

(h) Serve, if requested by DSS, as a team member on DSS inspections of defense contractor classified ISs connected to the DISN.

e. In addition to responsibilities outlined in Enclosure D, DISA will perform the following tasks in support of DOD and IC CD information transfer connection requirements:

(1) Provide CD enterprise services and integrate new CD information transfer requirements into DOD enterprise CD services.[15]

(2) Designate a CDSE to coordinate and manage the implementation of DISA-provided CD enterprise services, point-to-point CDSs, and products. Ensure there is feedback among DISA and supported CC/S/As and the UCDMO on CDSs and products.

(3) Coordinate with CC/S/A CDSEs and provide quarterly status reports on operational DISN CD services and CDSs to the DSAWG and UCDMO.

(4) Notify the DSAWG, UCDMO, affected CC/S/A Authorizing Officials (DAAs), and CDSEs concerning vulnerabilities, configuration changes, or operational changes that affect individual or classes of CDS authorized to operate.

f. <u>DISN Related Panels, Boards and Working Groups</u>

(1) Appoint a flag-level representative to the DISN/GIG Flag Panel.

(2) Appoint DSAWG chairperson in the military grade of O-6 or USG equivalent as directed by the DOD CIO.

[15] Previous security evaluation and risk assessments for enterprise or centralized services will be reviewed prior to integration of new information transfer requirements.

(3) Appoint a representative in the military grade of O-6 or government USG civilian equivalent as a primary DSAWG representative as well as USG alternates with DISA DSAWG voting authority.

(4) Appoint a representative in the military grade of O-6 or USG civilian equivalent representative to the CDRB.

g. Provide CND services IAW DODD O-8530.1 (reference ll)

7. Director, Defense Intelligence Agency (DIA). In addition to responsibilities outlined in Enclosure D, the Director, DIA, shall:

a. Implement, operate, manage, and secure Joint Worldwide Intelligence Communications System (JWICS) components and facilities on the DISN-provided transport IAW established agreements with DISA.

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

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

(1) Designate a CDSE to coordinate, manage, and maintain the DIA-provided DOD information networks enterprise CD services, centralized and point-to-point CDSs. Ensure there is feedback among DIA and supported CC/S/As and the UCDMO about CD services and CDSs.

(2) Conduct Certification Test & Evaluation (CT&E) and ST&E of CD solutions IAW with UCDMO guidance and IAW applicable DOD and IC security control assessment (certification) and authorization to operate (accreditation) requirements.

d. DISN Related Panels, Boards and Working Groups

(1) Appoint a flag-level representative to the DISN/GIG Flag Panel.

(2) Appoint a representative in the military grade of O-6 or USG civilian equivalent as primary representative to the DSAWG and USG alternates with DIA DSAWG voting authority.

(3) Appoint a representative in the military grade of O-6 or USG civilian equivalent representative to the CDRB.

8. Director, National Security Agency (NSA)/Central Security Service (CSS). In addition to responsibilities outlined in Enclosure D, the Director, NSA/CSS shall:

a. Recommend techniques and procedures to minimize DISN information security vulnerabilities IAW DODD 8500.01E (reference e) and CJCSI 6510.01 series (reference k).

b. Develop and/or certify communications security (COMSEC) solutions and produce keying material for COMSEC IAW DODI 8523.01, "Communications Security (COMSEC)" (reference zz).[16]

c. In support of DOD and IC CD information transfer requirements, and in addition to responsibilities outlined in Enclosure D, NSA/CSS will:

(1) Establish and maintain methods for performing, analyzing, and evaluating security countermeasures and attacks in support of the community evaluation of the global risk for CDSs.

(2) Notify the DSAWG, UCDMO, affected CC/S/A Authorizing Officials (DAAs), and CDSEs concerning vulnerabilities, configuration changes, or operational changes that affect individual or classes of CDSs authorized to operate.

(3) Designate a CDSE to work on CD activities and issues with the UCDMO.

(4) Conduct CT&E of CDSs IAW with UCDMO guidance.

d. DISN Related Panels, Boards and Working Groups

(1) Appoint a flag-level representative to the DISN/GIG Flag Panel.

(2) Appoint a representative in the military grade of O-6 or USG civilian equivalent primary representative to the DSAWG and USG alternates with NSA/CSS DSAWG voting authority.

(3) Appoint a representative in the military grade of O-6 or USG civilian equivalent representative to the CDRB.

9. Director, Defense Security Service (DSS). In addition to the responsibilities outlined in Enclosure D, the Director, DSS will direct DSS Cyber Security Inspection Program:

a. Establish security standards as the Authorizing Official (DAA) for defense contractor classified ISs under DOD 5220.22-M (reference kk) that are equivalent to published STIGs and IAW DTM 09-016, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems" (reference dd).

[16] DODI 8100.04 (reference f) does not apply to DOD cryptologic SCI systems.

b. Ensure defense contractor classified ISs connected to the DISN are in compliance with DSS security standards.

c. Ensure defense contractor ISs that process classified information connected to DISN are aligned to an accredited CNDSP.

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

e. Establish Cyber Security Inspection Teams including team members from DISA or USSTRATCOM, as appropriate, to conduct DSS compliance inspections and support USSTRATCOM-directed CCRIs of defense contractor classified ISs connected to DISN-provided transport and information services IAW DOD 5220.22-M (reference kk) and contract IS security provisions.

(1) Notify defense contractors with classified ISs connected to the DISN of scheduled DSS compliance inspections or USSTRATCOM-directed CCRI.

(2) Notify DISA or USSTRATCOM of unannounced DSS compliance inspections, as appropriate.

(3) Employ published USSTRATCOM CCRI criteria and tools for inspections of defense contractor classified ISs connected to DISN-provided transport and information services as governed by DOD 5220.22-M (reference kk) security requirements and contract IS security provisions.

(4) Provide inspection results upon request to USSTRATCOM, DOD CIO, or DISA for defense contractor ISs processing classified information connected to the DISN.

f. Participate at DSAWG as requested by Under Secretary of Defense for Intelligence (USD(I)) to provide information or comments relating to cleared defense contractor issues as the Authorizing Official (DAA) for contractor classified ISs under the authority of DODI 5220.22 (reference gg) and the DOD 5220.22-M (reference kk).

10. Director, Unified Cross Domain Management Office (UCDMO). The Director, UCDMO shall:

a. Chair the CDRB.

b. Promote the development and use of enterprise cross domain capabilities.

c. Be informed of evolving technologies and development efforts for existing or new CDSs.

d. Facilitate CD testing and evaluation as follows:

(1) Establish standardized CD security test controls to be used by certifiers for a CDS security control assessment.

(2) Establish security control assessment (certification) criteria to qualify community laboratories to test CDSs.

(3) Lead development of a process to certify community laboratories to test CDSs.

(4) Lead development of a process to provide centralized scheduling of CD test laboratories.

(5) Review recommendations regarding CT&E and ST&E results, when required.

e. Provide centralized coordination and managerial oversight for DOD and IC CD activities IAW DOD CIO and the Associate Director of National Intelligence (ADNI) & CIO memorandum titled, "Unified Cross Domain Management Office Charter" (reference aaa).

f. Maintain visibility of operational CD information transfer requirements.

g. Coordinate research and development efforts for CD technologies, including the development of unique CD capabilities and partnerships with academia, industry, and USG agencies, consistent with applicable law.

h. Develop, maintain, and oversee a baseline list of validated CDS for DOD and IC use.[17]

(1) Manage process for sponsorship of new CDS to be placed on the UCDMO Baseline List.

(2) Manage a process for identifying CDS to be placed on the UCDMO Sunset List.

i. Maintain an inventory of DOD CDSs, including operational as well as planned CDSs or CDSs in research and development.

[17] UCDMO CD Baseline and Sunset Lists can be found at https://www.intelink.gov/sites/ucdmo/Pages/Default.aspx

j. Develop and maintain a CD roadmap building on UCDMO inventory, validated CD requirements, capability gaps, and emerging technologies to establish necessary CD capabilities.

k. DISN Related Panels, Boards, and Working Groups

(1) Appoint a representative in the military grade of O-6 or USG civilian equivalent primary representative to the DSAWG and USG alternates with UCDMO DSAWG voting authority.

(2) Appoint a CD advisor to the DISN/GIG Flag Panel.

11. DISN Related Panels, Boards, and Working Groups. The following paragraphs outline the responsibilities and processes of DISN related panels, boards, and working groups as prescribed in DODDs, DODIs, and charters.

a. DISN/GIG Flag Panel

(1) The DISN/GIG Flag Panel consists of the following voting members:

(a) Enterprise Information Environment Mission Area (EIEMA) PAA, WMA PAA, Defense Intelligence Mission Area (DIMA) PAA, Business Mission Area (BMA) PAA, and flag-level representatives from DISA, DIA, NSA/CSS, USSTRATCOM, and ADNI CIO.

(b) Additional voting members may be added to the Flag Panel through regular and/or directed charter changes in coordination with the four Mission Area PAAs and the Panel Chair.

(2) Other organizations, such as the UCDMO or DSS, may be invited to attend the DISN/GIG Flag Panel as advisors on a regular basis.

(3) The following DISN/GIG Flag Panel responsibilities are IAW the current DISN/GIG charter (reference bbb); these responsibilities may be changed through regular or directed charter updates in coordination with the four Mission Area PAAs and the Panel Chair. The DISN/GIG Flag Panel shall:

(a) Assess DOD Information Enterprise risk and authorize connection of DOD enterprise ISs IAW the DOD memorandum titled, “DOD Information System Certification and Accreditation Reciprocity” (reference ccc).

(b) Make or delegate risk decisions for information exchanges and connections among mission area (MA) ISs.

(c) Make or delegate DOD, mission partner, or defense contractor information connection risk decisions including interagency and foreign military IS connections.

(d) Make or delegate approval of CD services and CDSs including DOD first time use of a CDS Baseline product.

(e) Review and provide advice to the DOD CIO and MA PAAs on IA standards and implementing guidance (e.g., DIACAP[18] and DOD 8500 Series).

(f) Oversee and define risk decision and connection authorities of the DSAWG and adjudicate decisions.

(g) Provide oversight and review authorization to operate (accreditation) decisions for operation of enterprise-level ISs (e.g., applications, enclaves, or outsourced IT services) and/or networks based on mission impact, security risk, and resource calculations.

(h) Provide IA advice and risk management recommendations to the PAAs, CC/S/A Authorizing Officials (DAAs), milestone decision authorities, Joint Requirements Oversight Council (JROC), and other capabilities boards and bodies that approve deviations from policy that may impact the DOD IA posture.

(i) Review and adjudicate CD conflicts and issues brought forward from the CDRB.

(j) Forward unresolved authorization to operate (accreditation) issues to the PAAs with DISN/GIG Flag Panel recommendations for final decisions as required.

b. Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG).[19]

(1) The DSAWG consists of representatives from the Joint Staff, Office of the Under Secretary of Defense for Intelligence, DOD CIO, USSTRATCOM, Services, DISA, DIA, NSA/CSS, Deputy Chief Management Office, Office of the Director of National Intelligence (DNI) CIO, and the UCDMO. Other organizations may be invited to attend as technical advisors.

(2) The DSAWG chairperson is appointed at direction of the DOD CIO.

[18] DIACAP Knowledge Service site: https://diacap.iaportal.navy.mil/
[19] DSAWG Web site: http://www.us.army.smil.mil/suite/page/14735

(3) The DSAWG, IAW its charter (reference ddd), shall:

(a) Support DISN/GIG Flag Panel in its role as the final risk decision authority for DISN connections.

(b) Decide on or approve actions for those classes of ISs and circumstances delegated by the DISN/GIG Flag Panel (e.g., similar architectures, enterprise ISs, and CDSs previously approved by the DISN/GIG Flag Pane).

(c) Make connection approval recommendations to the DISN/GIG Flag Panel for those classes of ISs not delegated by the DISN/GIG Flag Panel (e.g., new technology or high risk connections).

(d) Recommend to the DISN/GIG Flag Panel disconnection or disapproval of a CDS.

(e) Oversee and provide guidance to the Cross Domain Technical Advisory Board (CDTAB).

(f) Recommend changes to DOD security policy and responsibilities.

(g) Guide or assist development of DISN integrated system/security architecture changes.

(h) Provide community risk assessments.

(i) Report results of the assessments (and possible alternative proposals to mitigate risk) to the DISN/GIG Flag Panel as required.

(j) Monitor life cycle of the DISN-provided transport and information services to identify and resolve security issues.

(k) Coordinate with the ADNI & CIO through the UCDMO on CD connections between TOP SECRET/SCI and other DOD classified domains including connections to the DISN.

(l) Provide security assessments and recommendations to the DOD CIO GWP and to the CDRB, as required.

c. DOD GIG Waiver Panel (GWP)

(1) The DOD GWP voting membership consists of the GWP Chair and representatives from USD(AT&L), Cost Assessment and Program Evaluation Office, Under Secretary of Defense (Comptroller), Joint Staff, USSTRATCOM, and Services.

(2) DSAWG, DISA and DOD CIO Identity, and Information Assurance provide technical advisors to the GWP.

(3) The panel may request representatives from other DOD components and government agencies to participate in panel meetings as required.

(4) The GWP chair is appointed by the DOD CIO and governed by the DOD CIO memorandum titled, "Global Information Grid Waiver Charter" (reference eee).

(5) The GWP shall:

(a) Adjudicate all requests for waivers and appeals to the GIG including networks, cross component computing, Internet connectivity, satellite communications, information assurance, and oversight of the migration of legacy networks into the DISN IAW GIG Waiver Charter (reference eee).

(b) Provide waiver recommendations to the DOD CIO for approval.

d. Cross Domain Technical Advisory Board (CDTAB). The CDTAB[20] shall:

(1) Assess technical risk of CDSs.

(2) Report results of CD risk assessments and propose alternate solutions to mitigate risk to DSAWG.

(3) Advise and make recommendations to the CDRB and DSAWG on CDS technical issues and details for resolution by the DSAWG or DISN/GIG Flag Panel.

[20] CDTAB Web site: http://iase.disa.smil.mil/cds/cdtab/index.html

(INTENTIONALLY BLANK)

ENCLOSURE D

JOINT STAFF, COMBATANT COMMAND, SERVICE, DEFENSE AGENCY, DOD FIELD ACTIVITY, AND JOINT ACTIVITY (CC/S/A) COLLECTIVE RESPONSIBILITIES

1. DISN-Provided Transport and Information Services Responsibilities. C/S/As shall:

a. Submit connection requirements between installations and facilities or connections to external mission partner or defense contractor ISs and networks through their chain of command and their responsible enterprise oversight organizations to DISA, IAW the DISA Connection Process Guide (reference p). Requirements that DISA cannot fulfill will be submitted to the DOD CIO GWP for a Commercial ISP Connection Waiver.

b. Submit requirements for connections to the Public Switched Telephone Network (PSTN) or Internet Telephony Service Provider (ITSP) that include the capability for automated long-distance on-netting and/or off-netting of voice traffic between the public/commercial networks and the DISN for approval by DOD CIO.

c. Identify to DISA each DOD IS requiring connection services between a CC/S/A installation/base with an external mission partner or defense contractor IS or network for DISN planning purposes. The ISs and requirements must be identified to DISA as soon as requirements for these services are validated.

d. Provide geographic combatant commands visibility of connection requirements for a Service/post/camp/station or agency operated facility (i.e., courtesy copy of DISN request) outside the United States.

e. Ensure ISs comply with DODI 8551.1 (reference j).

f. Coordinate with DISA customer provisioning of Web services such as data interfaces for alarm, configuration, and trouble ticketing.

g. Process CC/S/A sustaining base and deployable segment requirements IAW DODI 8100.04 (reference f) and the supporting CC/S/As' procedures.

h. Minimize

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

(2) Notify NMCC, USSTRATCOM, and DOD CIO when communications traffic controls are implemented for CC/S/A communications.

2. DISN Connection Responsibilities. CC/S/As shall:

a. Implement DOD PAA and DISN/GIG Flag Panel decisions on the enterprise deployment, operation, and connection of ISs.

b. Ensure that DOD, mission partner, or defense contractor ISs connected to DISN-provided transport and information services are authorized to operate IAW DOD, IC, or other governing policy and processes.[21]

c. Ensure ISs comply with DODI 8551.1 (reference j).

d. Ensure CC/S/A organizations provide for or align with an accredited CNDSP to acquire CND support for each IS.

(1) When aligning with an accredited CNDSP, organizations will ensure an MOA is completed detailing the CND services that will be provided by the CNDSP and which services will be accomplished by the organization operating the IS.

(2) DISN connected ISs will implement CND service capabilities to continuously protect, monitor, detect, analyze, and respond to unauthorized activity within CC/S/A ISs and networks IAW DODD O-8530.1 (reference ll). These capabilities will be available during IS periods of operations (i.e., 24 hours/7 days a week).

e. Ensure transmission of classified information is secured through use of authorized cryptographic equipment and algorithms and/or protected distribution systems (PDSs).

f. 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 United States Security Authority for NATO Affairs Instruction 1-07 (reference yy).[22]

g. Endorse connection requirements and maintain oversight for CC/S/A connections and requests.

---

[21] DODI 8510.01 (reference h) for DOD, ICD 503 (reference m) for the IC, DOD 5220.22-M (reference kk) for contractor classified ISs, and (for example) NIST SP 800-37 (reference ff) for other federal agencies.

[22] The Central United States Registry (CUSR) Web site lists registered enclaves at https://secureweb.hqda.pentagon.mil/cusr/.

(1) Document and endorse the requirements for connections.

(2) Endorse requests, validate operational requirements, and prioritize mission partner and defense contractor connection requests.

(3) Ensure that foreign entity connection requests are endorsed by a combatant command headquarters.

(4) Assign a primary (in military grade of O-6 or civilian equivalent) and alternate to validate and endorse mission partner and defense contractor DISN connection requirements for CC/S/A Headquarters.

h. 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.

i. Ensure ISs are compliant with DOD IA requirements IAW DODI 8500.2 (reference g), CJCSI 6510.01 series (reference k), and DISN Connection Process Guide (reference p).

j. Ensure that defense contractor classified ISs are compliant with IA requirements IAW DOD 5220.22-M (reference kk).

k. Ensure at least annually that ISs are reviewed for compliance with DOD IA requirements, including mission partner and defense contractor ISs sponsored by the CC/S/A.

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

m. Provide guidance, in writing, on authorized and prohibited uses of DISN IAW DOD 5500.7-R (reference mm). Ensure user agreement and IA awareness training includes authorized and prohibited uses of DISN and potential penalties IAW DODD 5500.7 (reference fff).

3. Owned/Leased Telecommunications Equipment and Services. CC/S/As shall:

a. Acquire effective, efficient, and economical base telecommunications equipment and services.

b. Maintain an inventory of all base telecommunications equipment and services.

c. Review and revalidate all requirements for CC/S/A telecommunications equipment and services.

d. Terminate services that are uneconomical or no longer needed.

e. Manage controlled interfaces between the DSN and the PSTN to fulfill communications requirements between DOD and non-DOD networks/systems and to provide alternative communications in the event of DSN disruptions.

4. Cyber Security Inspection Program (CSIP) and Monitoring. CC/S/As shall:

a. Conduct internal[23] vulnerability assessments, 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 specific technologies used IAW CJCSI 6510.01 (reference k).

b. Conduct remote monitoring of DISN connections and connected enclaves. When scanning for network compliance is conducted by DOD organizations external to another CC/S/A, notification must be provided at least 24 hours prior to the event or within an identified time period (e.g., 1 week) to the organization being scanned for compliance in coordination with USSTRATCOM/USCYBERCOM.

c. Monitor scanning and monitoring notices issued by USSTRATCOM or posted to the USCYBERCOM Web site[24] and ensure that current, accurate, and complete contact information is provided to applicable DISN network/service databases.

d. Use published USSTRATCOM CCRI criteria and tools employed for CCRIs as the baseline for cyber security inspections.

(1) Support and comply with USSTRATCOM-directed CCRIs.

(2) Meet post-inspection requirements including POA&Ms, after-action plans, and other mitigation efforts directed by USSTRATCOM.

e. Ensure CDS and connections are included in cyber security inspection program assessments, evaluations, and cyber security inspections.

[23] Examples of organizations conducting external inspections include USSTRATCOM-directed CCRI, DOD and CC/S/A component inspectors general, the Government Accountability Office (GAO), and other authorized entities.
[24] https://www.cybercom.smil.mil/

f. For defense contractor systems directly connected (for example, not through the FED-DMZ) to DISN-provided transport and information services, CC/S/A sponsors shall:

(1) Ensure new or renewed contracts include the provision that defense contractor ISs connected to DISN-provided transport and information services are subject to cyber security inspections.

(2) Ensure sponsored defense contractor ISs processing classified information connected to DISN-provided transport and information services are determined in compliance with DOD 5220.22-M (reference kk) as determined by DSS, Defense Federal Acquisition Regulation System (DFARS)[25] contract IS security provisions, and CC/S/A supplemental contract IS security provisions.

(3) Ensure sponsored defense contractor unclassified ISs connected to DISN-provided transport and information services are in compliance with DFARS[26] contract IS security provisions and CC/S/A supplemental contract IS security provisions.

(4) Ensure defense contractor unclassified and classified ISs connected to the DISN monitor and implement USSTRATCOM warning and tactical orders and directives under the provisions of contract and DOD 5220.22-M (reference kk) for classified IS.

(5) Ensure sponsored defense contractor systems operating on behalf of the Department of Defense are authorized to operate.

(6) Provide coordination support for DSS cyber security inspections of a sponsored defense contractor ISs processing classified information connected to DISN-provided transport and information services, when requested.

(7) Conduct periodic cyber security inspections of defense contractor ISs that process unclassified information connected to DISN-provided transport and information services to ensure compliance with contract IS security provisions.

(8) Ensure CND services are provided by a certified and accredited CNDSP for sponsored defense contractor ISs connected to DISN-provided transport and information services before connection is implemented.

[25] DFARS: http://www.acq.osd.mil/dpap/
[26] DFARS and Procedures, Guidance, and Information (PGI) at: http://www.acq.osd.mil/dpap/dars/

g. For mission partner ISs directly connected to DISN-provided transport and information services CC/S/A sponsors shall:

(1) Ensure sponsored mission partner ISs directly connected to DISN-provided transport and information services are covered by a signed formal agreement (e.g., an MOA) with the mission partner organization.

(2) Ensure formal agreement requires compliance with DOD security controls and requirements or equivalent controls and requirements (e.g., NIST SP 800-37 (reference ff)) for connection to DISN-provided transport and information services.

(3) Ensure mission partner provides documentation on implementation of required DOD security controls.

(4) Ensure formal agreement includes provision that mission partner ISs connected directly to DISN-provided transport and information services are subject to compliance inspections.

h. CC/S/A sponsoring a mission partner IS connection to DISN-provided transport and information services through an established DISN DMZ (e.g., FED DMZ) will follow DISA guidance for connection of defense contractors or mission partners to a DISN established DMZ.

i. Provide results of inspections upon request to USSTRATCOM and DISA. DSS will provide results upon request to USSTRATCOM or DISA for defense contractor IS processing classified information.

5. Cross-Domain Information Transfer Responsibilities. In support of DOD and DNI CD information transfer requirements, CC/S/As shall:

a. Designate a CDSE or a CC/S/A office under authority of CC/S/A CIO to carry out CDSE functions to provide oversight and management of CD activities throughout the CD System Development Life Cycle (SDLC). Designation of a supporting CDSE external to the CC/S/A requires an MOA outlining CC/S/A's and supporting CDSE's responsibilities. The CDSE shall:

(1) Act as focal point for and manage all CD-related activities in their CC/S/A.

(2) Maintain knowledge of published (e.g., UCDMO or DISA) available CD capabilities provided by enterprise services and the baseline CDSs.

(3) Endorse enterprise services as the preferred method of addressing CD requirements.

(4) Ensure that any new CD technology developments:

(a) Are fully coordinated with UCDMO and USSTRATCOM.

(b) Align with the goals and objectives of the CD Community Roadmap.

(c) Fill identified capability gaps.

(5) Provide coordination and support to CC/S/A CD related assessment (certification) and authorization to operate (accreditation) activities.

(6) Review, validate, and prioritize CD requirements, in coordination with USSTRATCOM throughout the implementing CC/S/A's acquisition and SLDC.

(7) Ensure IA requirements for CD-related activities are addressed throughout the SDLC.

(8) Participate in applicable CD community forums (e.g., boards, tiger teams, or working groups) to represent CC/S/A CD needs.

(9) Maintain access to information regarding CD requirements, implementations, installations, and configurations within the supported CC/S/A's jurisdiction.

(10) Enter and update, as required, CD technology and operational data to include updates and patches for technologies via the SGS.

b. Employ CD information transfer requirements solutions and products from CD baseline list.

(1) CD solutions and products will be employed in the following order:

(a) Enterprise CD services and centralized CDSs will be established to fulfill operational requirements across the DOD enterprise or across three or more CC/S/As.

(b) Point-to-point CDSs or products will only be used when an enterprise service or centralized CDS does not meet operational mission requirement(s). The CDSE proposing a point-to-point CDS must justify its use to meet the operational mission requirement(s) to the UCDMO.

(c) Recommend new solutions or products only when existing CDSs and products on the CD baseline list cannot meet operational requirements IAW this instruction.

(2) Ensure CD connections assessed with the risk ratings above the level the DSAWG can accept (approve) have POA&Ms or a documented and funded strategy describing their risk mitigation strategy approved IAW established DISN/GIG Flag Panel governance policy.

(3) Submit a letter of exception or POA&M detailing the planned transition to a baseline solution through the CDRB, DSAWG review to the DISN/GIG Flag Panel for approval, if utilizing a product that is not on the CD Baseline List.[27]

(4) Assist with rapid migration from use of solutions on the CD sunset list.

c. Obtain combatant command validation, endorsement, and prioritization of information transfer requirements submitted by Service, Defense agency, and DOD field or joint activities in support of combatant command operations.

d. Ensure proposed UCDMO baseline products are reviewed by CDSE prior to acquisition.

e. Provide funds within CC/S/A budget authority to support the lifecycle for their CDSs including acquisition, engineering, security testing, security mitigation, and annual sustainment operating costs.

f. Develop transition plans for obsolete or aging CDSs identified with an end of lifecycle date in the UCDMO CD sunset list.

g. CDSE prior to initiating new CD development shall:

(1) Obtain UCDMO and DISN/GIG Flag Panel concurrence prior to expending funding for new CD services, products, or technologies.

(2) Forward CD information transfer requirement(s) to the UCDMO, DSAWG, and DISN/GIG Flag Panel for review prior to initiating any CD development.

h. Conduct life cycle costs, sustainment, management,[28] and support of a CC/S/A CD service, product, or technology through a program management office or specified CC/S/A organization IAW DODI 5000.02 (reference ggg) and DODI 8580.1 (reference hhh).

---

[27] UCDMO CD baseline and sunset lists can be found at https://www.intelink.gov/sites/ucdmo/Pages/Default.aspx

[28] Life-cycle activities include capabilities, resources, acquisition, security, operations, deactivation, and retirement/reutilization or demilitarization of a service or solution.

i. 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.

(1) Either the POA&M or funded risk mitigation strategy must be presented to the DSAWG to review and for the Flag Panel to adjudicate prior to gaining approval to connect.

(2) In the event of risk rating, definition, or process changes, risk ratings beyond that which the DSAWG can accept still require either the POA&M or evidence of a funded risk mitigation strategy.

j. Support, if required, the implementation of a CD product or technology for which they are a proponent in coordination with other CC/S/A CDSEs, the UCDMO and DISA, support site personnel, and developers.

6. Cross-Domain Requirement Prioritization. CC/S/As shall:

a. Prioritize CD information transfer requirements based on impact on readiness and ability of the DOD organization to execute assigned missions.

b. Provide an impact description based on Readiness Level Assessment definitions in CJCSI 3401.01E, "Joint Combat Capability Assessment" (reference iii).

c. Identify impact on readiness and ability to execute specific assigned mission by the requesting organization if a CD capability is not provided for a CD information transfer requirement.

d. CDS information transfer requirements impact will be identified as:

(1) CRITICAL --when **failure to provide** CD information transfer capability **will preclude accomplishment** of assigned mission(s).

(2) HIGH -- when **failure to provide** CD information transfer capability **will have significant impact** on readiness and ability to execute assigned mission(s).

(3) MEDIUM -- when **failure to provide** CD information transfer capability **will have limited impact** on readiness and ability to execute assigned mission(s).

(4) LOW -- when **failure to provide** CD information transfer capability **will have negligible impact** on readiness and ability to execute assigned mission(s).

e. Provide to USSTRATCOM CD Capability Requirement Prioritization Information.

(1) Title and Reporting Organization: Subject title of the CD Capability Deficiency and the Reporting Organization.

(2) Current Requirement Not Being Met and Corresponding Source Document: Brief description of the CD information transfer requirement deficiency and a list of the source documents from which the requirement is derived (e.g., Guidance for the Employment of the Force (GEF), Joint Capabilities Plan (JSCP), concept plan (CONPLAN) XXXX, operations plan (OPLAN) XXXX, Theater Security Cooperation (TSC) plan, etc.).

(3) Quantified Shortfall/Operational Impact/Mission Essential Tasks Impacted: Objective information quantifying the shortfall, the critical effects the CD capability deficiency has on the organization's ability to conduct its mission(s) (e.g., preclude, significantly impact, limited impact, or negligible impact ability to execute mission(s)) and the associated Joint/Agency Mission Essential Task Lists (JMET/AMET) affected (e.g., OP 3.1.5. Publish Air Tasking Order(s)).

(4) Actions Taken/Needed To Fix Deficiency: Actions currently taken to date to meet CD information transfer requirement to execute mission(s) and recommendation needed to fix current CD capability deficiency.

(5) Risk and Planned/Potential Mitigation Action: Assess current risk CD deficiency contributes to execution and the planned/potential mitigation steps necessary to manage this risk until CD capability deficiency is implemented.

(6) Point of contact (POC) Information: Name, rank, and organization.

7. DOD Information Assurance Risk Management Framework (i.e., DIACAP). CC/S/As shall:

a. Ensure DOD, mission partner, and defense contractor ISs have an authorization to operate (accreditation) IAW DODD 8500.01E (reference e), DODI 8510.01 (reference h) and DOD 5220.22-M (reference kk).

b. Document and maintain the IA controls compliance status for deploying IS IAW DODI 8510.01 (reference h).

8. Security Control Assessment (Certification) and Authorization to Operate (Accreditation) Reciprocity. CC/S/As shall:

a. Provide security control assessment (certification) and authorization to operate (accreditation) documentation IAW DODI 8510.01 (reference h), ICD

503 (reference m), or NIST SP 800-37 (reference ff) as appropriate for deploying IS to receiving CC/S/As. For defense contractor classified ISs, DOD 5220.22-M (reference kk) documentation will be provided.

b. Resolve security issues IAW the DOD memorandum titled, "DOD Information System Certification and Accreditation Reciprocity" (reference ccc).

c. Accept security control assessment (certification) and authorization documentation developed IAW ICD 503 (reference m), NIST SP 800-37 (reference ff), DOD 5220.22-M (reference kk), or DIACAP (reference h) requirements reciprocally, without the need to expend manpower and resources performing additional security control assessment (certification) or on reformatting the security authorization documentation packages into alternate forms IAW the DOD memorandum titled, "DOD Information System Certification and Accreditation Reciprocity" (reference ccc) and the DOD CIO and IC CIO agreement titled, "Agreement between the Department of Defense Chief Information Officer and the Intelligence Community Chief Information Officer" (reference jjj).

9. Approval for Mission Partner and Defense Contractor Connections to the DISN. CC/S/As shall:

a. Require a CC/S/A sponsor for connection of mission partner or defense contractor ISs to DISN-provided transport and information services or to a CC/S/A enclave connected to DISN-provided transport and information services, to include the Fed-DMZ.

b. Ensure all requests for mission partner and defense contractor connections to the DISN-provided transport and information services or to a DOD enclave connected to DISN-provided transport and information services are DOD CIO approved prior to implementation IAW the DISN Connection Process Guide (reference p).

c. Validate and endorse mission partner or defense contractor entity connection requests IAW the DISN Connection Process Guide (reference p). CC/S/A office will provide to DISA the contact information for the office/individual responsible for connection validation.

d. Ensure combatant command guidance for approval of mission partner or defense contractor DISN connections within their AOR outside the United States are followed.

e. Identify funding source for mission partner or defense contractor connection request.

f. Ensure mission partner or defense contractor ISs are authorized to operate prior to connection.

g. Ensure each mission partner or defense contractor connection is a separate connection request and that mission partner or defense contractor access is filtered and limited to only those data and services required to support the DOD-approved mission and **filtered access**.

h. Ensure mission partner or defense contractor entities with DISN-provided transport and information services are connected to DISN via a DISA engineered and approved DISN solution. The DISN solution **must be ordered** by CC/S/A through DISA request fulfillment process (e.g., the DISA Direct Order Entry (DDOE) system/ telecommunications request (TR)/ telecommunications service order (TSO) process).

i. Ensure ISs directly connected to DISN-provided transport and information services are aligned with an accredited CNDSP and costs for CNDSP support are included in defense contracts or other formal agreements (e.g., MOU or MOA).

j. Ensure CC/S/A sponsors monitor information system security practices and sponsored defense contractor or mission partner ISs that are connected to the DISN are inspected for IA compliance.

(1) Ensure the inspection requirement is in the new or renewed contract or other formal agreements.

(2) Ensure an inspection for compliance with IA requirements is conducted at the start period of the contract or other formal agreement and periodically as required (e.g., by recent security incidents, changes in architecture or contract requirements, or follow-up from other evaluations or inspections).

(3) Conduct at least annually a security assessment of compliance with security controls IAW applicable governing policy (e.g., DODI 8510.01 (reference h), NIST SP 800-37 (reference ff), CNSSI 1253, “Security Categorization and Control Selection for National Security Systems” (reference kkk), or DOD 5220.22-M (reference kk).

k. Ensure mission partner or defense contractor entities are advised of and acknowledge through formal agreements (e.g., contract, MOA, or MOU) the conditions for connection to DISN-provided transport and information services.

l. Prohibit providing connections from mission partner or contractor ISs connected to DISN-provided transport and information services to any other facility or IS without explicit DOD CIO approval authority.

m. Ensure non-U.S. mission partner and defense contractor access to DOD information is in compliance with DODD 5230.11 (reference hh), the International Traffic in Arms Regulations (ITAR) (reference ii), and the Export Administration Regulations (EAR) (reference jj).

n. Ensure DOD CIO and DISA are notified of all renewals and modifications to approved renewal requests for mission partner or defense contractor connection to the DISN-provided transport and information services or to a DOD enclave connected to the DISN-provided transport and information services.

(1) The DOD 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 DOD CIO original approval conditions. DISA will forward to or post for appropriate CC/S/A all renewal approval packages.

(2) Renewal requests will require CC/S/A validation and endorsement and DOD CIO approval if there has been a change in one or more of the following: sponsor, mission, location, contract, architecture/topology, or DOD CIO original approval conditions.

10. Commercial Internet Service Provider (ISP) Connection Waiver.[29]

a. Use of commercially provided transport as an alternative to available DISN-provided transport requires a Commercial ISP Connection Waiver IAW the DISA Connection Process Guide (reference p).[30]

b. DOD Commercial ISP Connection Waivers require DSAWG review and DOD GWP approval as outlined in the DISA Connection Process Guide (reference p).

[29] For more information on regulation of foreign and domestic commerce in communications, see the Federal Communications Act of 1996, Telecommunications Act of 1996, Public Law No. 104-104, 110 Stat. 56 (1996) (reference u).
[30] DISA Web site: http://www.disa.mil/connect/waivers/internet_enclave.html

c. CC/S/As shall:

(1) Utilize the DDOE process or authorized acquisition to provision commercial ISP upon approval of Commercial ISP Connection Waiver.[31]

(2) Register the Commercial ISP Connection Waiver in the systems/networks approval process (SNAP) database.

d. Any specific questions on whether a Commercial ISP Connection Waiver is required for commercially-provided transport should be directed to the DOD GWP through the CC/S/A designated office/representative.[32]

e. Urgent Operational Requirements for Temporary Commercial ISP Connection Waiver

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

(a) Service Executive Agents shall register combatant command-validated requests for Commercial ISP Connection Waiver in support of urgent operational requirements.

(b) Defense Agency SNAP POCs shall register their agency urgent operational requirements.

(2) DISA will provide DISN transport or a commercial ISP connection within 24-48 hours.

(3) The DSAWG and DOD CIO GWP Chairs will be notified to ensure connection is properly documented and managed until commercial ISP connection requirement is no longer required.

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

[31] CC/S/As are encouraged to synchronize the accreditation of IS(s) using a commercial transport and services connection with the DOD CIO Waiver approval date/timeframe to avoid possible delays.
[32] For assistance in identifying your CC/S/A representative, contact the CAO via cao@disa.mil.

11. Commercial ISP Connection Waiver for ISP Connections Not Connected to the DISN

a. The DOD CIO may grant waiver status to a commercial ISP request/requirement nominated by a service representative to the GWP if it is deemed a recurring mission unable to be satisfied with a DISN solution in the foreseeable future and is not connected to the DISN.

b. Initially, a Commercial ISP Connection Waiver request for a CC/S/A requirement shall be submitted to the GWP for approval as a waiver (e.g., recruiting center(s), public affairs office(s), or another ISP connection or service requirement) IAW the DISN Connection Process Guide (reference p).

c. If approved, the implementation conditions (e.g., security, investment, interoperability, SNAP registration, etc.) for the Commercial ISP Connection Waiver will be published for use by the CC/S/As.

d. Commercial ISP Connection Waiver without DISN Connection Responsibilities

(1) CC/S/As shall:

(a) Ensure their GWP service representative is notified and reviews the Commercial ISP Connection Waiver prior to implementation and registration in SNAP.

(b) Submit through their GWP service representative a request for a Commercial ISP Connection Waiver to DISA, if an approved waiver does not exist.

(c) Register the Commercial ISP Connections in SNAP IAW GWP implementation conditions.

(d) Ensure IT assets employed are not physically or logically connected to DISN infrastructure.[33]

1. CC/S/As shall ensure that cable infrastructure available for common-use or general support transport requirements, commercial or DISN, is terminated on the main distribution frame (MDF) to ensure contamination between DISN services and commercial services does not occur. Also, the same equipment (e.g., modems, encryption devices, servers, etc.) shall not be used for both DISN and commercial services.

[33] DISN Infrastructure includes any equipment (e.g., communications cabinets, modems, servers, encryption cabinets, and/or cabling) owned by DISA.

2. Multiplexing equipment owned by the CC/S/As shall be employed in such a way as to ensure the DISN services and commercial services are separated on different circuit card assemblies (CCAs) and clearly noted on the multiplexing equipment as well as in any electronic or manual record maintained by the CC/S/A at that location.

(e) Implement ISP connection(s) IAW with the GWP implementation conditions for the Commercial ISP Connection Waiver.

(f) Ensure IT assets and information processed, stored, and transmitted meet DOD security protection requirements and applicable security controls.

(g) Ensure that controlled unclassified information or information exempted under the Freedom of Information Act (FOIA) IAW DOD 5400.7-R, "DOD Freedom of Information Act (FOIA)" (reference lll), is protected IAW DOD 5200.1-R, "Information Security Program" (reference mmm), and IAW DODI 8500.2 (reference g).

(h) Update the commercial ISP connection information in SNAP if registration information changes.

(i) Review/update registered Commercial ISP Connection Waiver requirement and SNAP registration information IAW waiver stipulated timelines.

(2) DISA shall:

(a) Inform the GWP if DISN-provided connection and services are available for a proposed Commercial ISP Connection Waiver request.

(b) Review CC/S/A commercial ISP connection(s) registered in SNAP.

(c) Notify DOD CIO approval authority if a CC/S/A registered commercial ISP connection is not meeting implementation conditions approved by the GWP.

(d) Notify the GWP, if DISN-provided connection and services become available to meet Commercial ISP Connection Waiver requirement(s).

(e) Plan, in coordination with the appropriate DOD customer, transition plan for moving a Commercial ISP Connection Waiver requirement from a commercial ISP to DISN-provided connection, if required due to the withdrawal of a waiver by the DOD CIO.

(3) GWP shall:

(a) Adjudicate Commercial ISP Connection Waivers submitted by CC/S/A GWP representative(s).

(b) Set conditions for implementation of a Commercial ISP Connection Waiver.

(c) Annually review Commercial ISP Connection Waivers to determine if the waiver is still warranted based on original requirement(s) and the current DOD investment, security, and interoperability guidance.

(d) Revise Commercial ISP Connection Waiver implementation conditions, if required.

(e) Notify CC/S/As if authorization for Commercial ISP Connection Waiver is withdrawn by the DOD CIO and GWP and ensure CC/S/A sponsor to verifies termination of connection.

12. Improper Commercial ISP Connection Implementation

a. A commercial ISP connection found to be operating without a Commercial ISP Connection Waiver 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.

b. A commercial ISP connection found to be operating without approved Commercial ISP Connection Waiver or current authorization to operate must be brought 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. Support to Civil-Military Operations. DOD policy provides provisions for the resourcing and extension of information services and capabilities to mission partners (civil-military partners) during civil-military operations IAW DODI 8220.02, “Information and Communications Technology (ICT) Capabilities for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations” (reference nnn), and DODI 3000.05, “Stability Operations” (reference ooo). CC/S/As may:

a. 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 DOD mission, and when the access is not in conflict with host-nation post, telephone or telegraph ordinance IAW DODI 8220.02 (reference nnn) and DODI 3000.05 (reference ooo). These information services and capabilities may include:

(1) Unclassified voice and data services.

(2) 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.

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

b. CC/S/As will 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 provide assistance, and subject to applicable statutory and regulatory restrictions and limitations.

d. Access provided to mission partner (civil-military partner) individuals through DOD provisioned and provided information services and capabilities for U.S. task forces to support mission partners in stability operations will be IAW DODI 8500.2 (reference g) and CJCSI 6510.01 (reference k).

(1) Connections of mission partner ISs to unclassified DISN-provided transport infrastructure will be requested and approved IAW the DISN Connection Process Guide (reference p).[34]

(2) Mission partner customer connections require separate connection requests and filtered access.

[34] http://www.disa.mil/connect/

14. CC/S/A Provided Connections to Other DOD Entities, Mission Partners, and Defense Contractors. These connections are also termed "backside connections" -- connection between two enclaves (e.g., CC/S/A and a defense contractor) that do not traverse the DISN but can provide a connection to the DISN through the CC/S/A enclave.

a. CC/S/A Connections Between DOD Entities

(1) A CC/S/A Authorizing Official (DAA) may authorize connections between DOD facilities operated by another CC/S/A to provide access to DISN-provided transport and information services (e.g., DOD tenant connecting to 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 STIG.[35]

(2) The DOD 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. CC/S/A Connections to Mission Partner or Defense Contractor Facilities and ISs

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

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

(a) Once approved by the DOD CIO, mission partner and DOD contractor connections must be ordered through the DDOE process IAW the DISA Connection Process Guide (reference p).

(b) 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).

[35] DOD tenants are encouraged to maximize limited resources and share network connectivity whenever possible to reduce total cost of ownership.

(c) Providing an unauthorized DISN connection to a mission partner or defense contractor will be grounds for individual or organizational sanctions including immediate disconnection of the CC/S/A connection to DISN-provided transport and information services.

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

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

(2) Accept responsibility for the connection in the security authorization documentation IAW DODI 8510.01 (reference h) and update DISN connection package with the DISA, to include a copy of any interconnection agreements and detailed topology diagrams including all connections.

(3) 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.

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

(5) Provide supporting encryption equipment, keying material, or a channel servicing unit/data servicing unit except for what may be ordered with vendor leasing action and the TSO.

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

(7) Ensure mission partners and defense contractors do not provide a backside connection to another organization.

15. Use of Tunneling. The following guidance will be followed when a CC/S/A determines the use of an IP tunnel is required to transport classified or sensitive data. IP tunnels enable hosts to send data securely over another network's connections by encapsulating the packets, thus securing the information. CC/S/As will:

a. Classified Data

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

(2) Ensure the Authorizing Official (DAA) validates all requirements to tunnel classified information across unclassified IP infrastructure.

(3) Obtain DSAWG approval before tunneling classified data across unclassified IP infrastructure.

(4) Use only IA and IA-enabled IT products evaluated IAW National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products" (reference ppp) and CNSS Policy No. 15, "National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems" (reference qqq).

(5) Ensure transmission of classified information is secured through use of authorized cryptographic equipment and algorithms and/or PDSs.

(6) Ensure IP tunnel endpoints are facilities authorized to process the information at the proper classification level.

(7) 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.

b. Sensitive Data

(1) Use NIST certified medium-robustness encryption or stronger for tunneling sensitive data over unclassified networks.

(2) Comply with the NSA/CSS protection profile for tunneling sensitive information over unclassified networks.

(3) Document the tunneling solution in the enclave's (including standalone enclaves) security authorization package prior to installation.

c. Use of Suite B Cryptography in Support of Requirements. Products utilizing Suite B Cryptography may be used IAW NSTISSP No. 11 (reference ppp) and successor policies that require products to have met NSA/CSS approved standards. CC/S/A will:

(1) Request NSA/CSS review and approval prior to any specific implementation of Suite B Cryptography for classified or controlled unclassified information.

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

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

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

(5) Provide implementation plan associated with the approved key and key management activities.

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

d. Nothing in this IP tunnel guidance will supersede the existing authorities and policies of the DNI regarding the protection of SCI and special access programs for intelligence as directed in Executive Order 12333 (reference rrr) and other laws and regulations.

16. DISN Voice Precedence. CC/S/As will:

a. Review and approve or disapprove all requests for IMMEDIATE and PRIORITY precedence capability. Combatant commands and Services may tailor the information requests for which they have approval authority.

b. Validate and forward requirements for FLASH and FLASH OVERRIDE to the Joint Staff J-8 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 combatant commands, Services, or Defense agencies have been coordinated with those affected organizations.

(3) Requests for FLASH and FLASH OVERRIDE are accompanied by trade-off of equal precedence.

(4) Appropriate communication service priorities are identified.

(5) All DISN voice services (e.g., DRSN) requests for voice connections and precedence requirements must be forwarded through the requestor's CC/S/A chain of command to the appropriate approval authority (see Table D-1).

		REQUEST ORIGINATOR				
		Military Service	**U.S. Command**	**DOD Agency**	**NMCS Joint Staff**	**Mission Partner Agency/ Organization**
APPROVAL	**FLASH OVERRIDE**	**Joint Staff/J-8**	**Joint Staff/J-8**	**Joint Staff/J-8**	**Joint Staff/J-8**	**DOD CIO**
	FLASH	**Joint Staff/J-8**	**Joint Staff/J-8**	**Joint Staff/J-8**	**Joint Staff/J-8**	**DOD CIO**
	IMMEDIATE	**Service Chief[1]**	**Combatant Commander**	**Agency Director[1]**	**Joint Staff/J-8**	**DOD CIO**
	PRIORITY	**Service Chief[1]**	**Combatant Commander**	**Agency Director[1]**	**Joint Staff/J-8**	**DOD CIO**

[1] Combatant command approves requests in AOR OCONUS

Table D-1. Voice Precedence Request Approval

d. FLASH and FLASH OVERRIDE requests from mission partners outside the Department of Defense must be sponsored by a CC/S/A and must be forwarded through the Joint Staff J-8 to the DOD CIO for approval.

e. Requests for DISN voice services requiring precedence will 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 (TSP).

(9) Servicing switch (End Office (EO), Small End Office (SMEO), Private Branch Exchange (PBX), Multi-Function Switch (MFS), and Multi-Function SoftSwitch (MFSS)).

(10) Terminating equipment; e.g., type, brand, PBX model, facsimile, data terminal/modem, video teleconference (VTC) studio terminal equipment, video End Instrument (EI), Integrated Services Telephone (IST), emergency action console, and Secure Telephone Equipment (STE).

(11) Number of extensions required. Indicate if extensions are to be located in geographically separate locations that will require extension of connectivity to servicing switch.

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

(13) DISA or Joint Staff waivers 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 of traffic.

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

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

17. JWICS Connection Process Requests. CC/S/As shall request connection to JWICS IAW "Network Connection Policy for the Joint Worldwide Intelligence Communications System" (reference sss).

18. Official and Authorized Use of the DISN. CC/S/As shall:

a. Authorize categories of personal use of DISN communication after determining that such communications:

(1) Do not adversely affect the performance of official duties by the DOD employee or CC/S/A.

(2) Are of reasonable duration and frequency and, whenever possible, are made during the DOD employee's or military member's personal time (such as after normal duty hours or during lunch periods).

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

(4) Do not overburden the communications system and create no significant additional cost to the Department of Defense or CC/S/A.

b. Ensure DOD ISs used to access the Internet are used for official and authorized purposes IAW DOD Regulation 5500-7R, (reference mm) and DTM 09-026, "Responsible and Effective Use of Internet-Based Capabilities" (reference nn).

c. DOD 5500.7-R (reference mm) states that authorized purposes might include brief communications made by military members and DOD employees during official travel to notify family members of transportation or schedule changes. They may also include reasonable personal communications from the military member or DOD employee at his or her workplace (such as checking with spouses or minor children; scheduling doctor, automobile or home repair appointments; brief Internet searches; or e-mailing directions to a visiting relative).

d. CC/S/A directors or military commanders may prohibit use of government communications systems and equipment, or filter access to commercial Web sites or services, to defend DOD's IT resources, safeguard missions by preserving operational security, and ensure sufficient bandwidth is available for DOD operations IAW DTM 09-026, "Responsible and Effective Use of Internet-Based Capabilities" (reference nn). 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, AOL, etc.) from government computers.

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

e. Prohibited use of DISN includes the following:

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

(2) Accessing pornography.

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

(4) Improperly handling classified information.

(5) Using the DISN to gain unauthorized access to other ISs.

(6) Endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

(7) Posting DOD information to external newsgroups, bulletin boards, or other public forums without authorization.

(8) Other uses incompatible with public service.

f. Individual and Organization Accountability. CC/S/As shall:

(1) Ensure users complete initial IA orientation and annual refresher training IAW DODD 8570.01 (reference z).

(2) Use a DOD CIO-approved consent banner and user agreement on all DOD ISs IAW the DOD CIO memorandum titled, “Department of Defense Information System Standard Consent Banner and User Agreement” (reference ttt).

(3) Ensure privileged users sign an information system privileged access agreement and acknowledgement of responsibilities IAW DOD 8570.01-M, “Information Assurance Workforce Improvement Program” (reference uuu).

(4) 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 DOD security requirements IAW this instruction, DOD Regulation 5200.1-R (reference mmm), DOD 5500.7-R (reference mm), and supplemental CC/S/A policies and procedures.

(a) DODD 5500.7 (reference fff) states penalties for violation of the standards of conduct prescribed in DOD 5500.7-R (reference mm) that include

statutory and regulatory sanctions such as judicial (criminal and civil) and administrative actions for DOD civilian employees and members of the Military Departments.

(b) The provisions concerning the official and authorized use of the DISN (federal communications) in DOD 5500.7-R (reference mm) constitute lawful general orders or regulations within the meaning of Article 92 (section 892 of reference vvv) of the Uniform Code of Military Justice (UCMJ), are punitive, and apply without further implementation. In addition to prosecution by court-martial under the UCMJ, a violation may serve as a basis for adverse administrative action and other adverse action authorized by the United States Code or federal regulations. In addition, violation of any provision in DOD 5500.7-R (reference mm) may constitute the UCMJ offense of dereliction of duty or other applicable punitive articles.

(5) Sanctions for military personnel may include, but are not limited to, some of the following administrative actions: oral or written warning or reprimand; adverse performance evaluation; and loss or suspension of access to classified material and programs. Sanctions for military personnel may also include any administrative measures authorized by Service directives and any administrative measures or nonjudicial or judicial punishments authorized by the UCMJ.

(6) Sanctions for civilian personnel may include, but are not limited to, some or all of the following administrative action: oral or written warning or reprimand; adverse performance evaluation; suspension with or without pay; loss or suspension of access to classified material and programs; any 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.

(7) 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 the Military Extraterritorial Jurisdiction Act of 2000, 18 USC 3261, et seq. (reference www). For additional information on defense contractor

personnel authorized to accompany U.S. Armed Forces, see DODI 3020.41 (reference xxx).

ENCLOSURE E

REFERENCES[36]

a. Unified Command Plan, 6 April 2011

b. DODD 5100.20, 26 January 2010, "National Security Agency/Central Security Service (NSA/CSS)"

c. DODD 5105.19, 25 July 2006, "Defense Information Systems Agency (DISA)"

d. DODD 8000.01, 10 February 2009, "Management of the Department of Defense Information Enterprise"

e. DODD 8500.01E, 24 October 2002, "Information Assurance (IA)"

f. DODI 8100.04, 9 December 2010, "DOD Unified Capabilities (UC)"

g. DODI 8500.2, 6 February 2003, "Information Assurance (IA) Implementation"

h. DODI 8510.01, 28 November 2007, "DOD Information Assurance Certification and Accreditation Process (DIACAP)"

i. DODI 8410.02, 19 December 2008, "NETOPS for the Global Information Grid (GIG)"

j. DODI 8551.1, 13 August 2004, "Ports, Protocols and Services Management (PPSM)"

k. CJCSI 6510.01 Series, "Information Assurance (IA) and Support to Computer Network Defense (CND)"

l. CJCSI 6250.01 Series, "Satellite Communications"

m. ICD 503, 15 September 2008, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation"

---

[36] Current DOD Issuances (30 August 2010) - http://www.dtic.mil/whs/directives/
Current CJCS Directives (30 August 2010) – http://www.dtic.mil/cjcs_directives/

n. CJCSI 6211.02C Series, "Defense Information Systems Network (DISN): Policy and Responsibilities" (Canceled)

o. CJCSI 6215.01C Series, "Policy for Department of Defense Voice Networks with Real Time Services (RTS)" (Canceled)

p. DISA Guide, Version 3.0, May 2010, "DISN Connection Process Guide"

q. DODI 8110.1, 6 February 2004, "Multinational Information Networks Implementation"

r. CJCSI 6285.01 Series, "Multinational Information Sharing (MNIS) Operational Systems Requirements Management Process"

s. JP 1-02 Series, "Department of Defense Dictionary of Military and Associated Terms"

t. CNSSI No. 4009, 26 April 2010, "National Information Assurance (IA) Glossary"

u. Telecommunications Act of 1996, Public Law No. 104-104, 110 Stat. 56 (1996).

v. Title 41, United States Code, Chapter 1, "defense contractor"

w. DISA Circular 310-130-02, 21 April 2000 (last reviewed 10 September 2008), "Communications Requirements"

x. "Global Information Grid (GIG) 2.0 Concept of Operations," 11 March 2009, Version 1.1

y. JROCM 095-09, 1 June 2009, "Global Information Grid (GIG) 2.0 Initial Capabilities Document (ICD)"

z. DODD 8570.01, 15 August 2004, "Information Assurance Training, Certification and Workforce Improvement"

aa. CJCSI 6212.01 Series, "Interoperability and Supportability of Information Technology and National Security Systems"

bb. DOD CIO, 15 December 2010, Change 2, "Department of Defense Unified Capabilities Requirements (UCR)"[37]

[37] UCR APL: http://www.disa.mil/ucco/

cc. DODI 4630.8, 30 June 2004, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

dd. DTM 09-016, 25 March 2010, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems"

ee. DOD CIO memorandum, 10 August 2009, "DOD IT Portfolio Repository (DITPR) and DOD SIPRNET IT Registry Guidance"

ff. NIST Special Publication 800-37, February 2010, "Guide for Applying the Risk Management Framework to Federal Information Systems"

gg. DODI 5220.22, 18 March 2011, "National Industrial Security Program (NISP)"

hh. DODD 5230.11, 16 June 1992, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"

ii. Title 22, Code of Federal Regulations, Parts 120-130, "International Traffic in Arms Regulation (ITAR)"

jj. Title 15, Code of Federal Regulations, Parts 730-799, "Export Administration Regulation"

kk. DOD 5220.22-M, 1 February 2006, "National Industrial Security Program Operating Manual"

ll. DODD O-8530.1, 8 January 2001, "Computer Network Defense (CND)"

mm. DOD Regulation 5500.7-R, 1 August 1993, "Joint Ethics Regulation (JER)"

nn. DTM 09-026, Change 1, 16 September 2010, "Responsible and Effective Use of Internet-based Capabilities"

oo. Title 44, United States Code, Chapters 31, 33, and 41

pp. DODD 5015.2, 6 March 2000, "DOD Records Management"

qq. DOD 5015.02-STD, 25 April 2007, "Electronic Records Management Software Applications Design Criteria Standard"

rr. CJCSI 5760.01 Series, "Records Management Policy for the Joint Staff and Combatant Commands"

ss. DODD 8115.01, 10 October 2005, "Information Technology Portfolio Management"

tt. CJCSI 3280.01 Series, "National Military Command System (U)"

uu. DISA Circular 310-130-4, 18 August 1993 (last reviewed 5 May 2006), "Defense User's Guide to the Telecommunications Service Priority (TSP) System"

vv. DODD 5100.03, 9 February 2011, "Support of the Headquarters of Combatant and Subordinate Unified Commands"

ww. CJCS Volume IX (CJCS LERTCON Procedures (U))

xx. CJCS, 8 February 2011, "The National Military Strategy of the United States of America"

yy. United States Security Authority for NATO Affairs Instruction 1-07, 2007, "Implementation of NATO Security Requirements"

zz. DODI 8523.01, 22 April 2008, "Communications Security (COMSEC)"

aaa. ASD(NII)/DOD CIO and ADNI & CIO, March 2007, "Unified Cross Domain Management Office Charter"

bbb. Charter, July 2008, "Defense Information System Network (DISN) Global Information Grid (GIG) Flag Panel "

ccc. DOD memorandum, 23 July 2009, "DOD Information System Certification and Accreditation Reciprocity"

ddd. Charter, 26 March 2004, "DISN Security Accreditation Working Group (DSAWG)"

eee. DOD CIO memorandum, 24 July 2002, "Global Information Grid Waiver Charter"

fff. DODD 5500.7, 29 November 2007, "Standards of Conduct"

ggg. DODI 5000.02, 8 December 2008, "Operation of the Defense Acquisition System"

hhh. DODI 8580.1, 9 July 2004, "Information Assurance (IA) in the Defense Acquisition System"

iii. CJCSI 3401.01E Series, "Joint Combat Capability Assessment"

jjj. DOD CIO and IC CIO Agreement, August 2008,"Agreement between the Department of Defense Chief Information Officer and the Intelligence Community Chief Information Officer"

kkk. CNSSI No. 1253, October 2009, "Security Categorization and Control Selection for National Security Systems"

lll. DOD 5400.7-R, September 1998, "DOD Freedom of Information Act Program"

mmm. DOD 5200.1-R, 14 January 1997, "Information Security Program"

nnn. DODI 8220.02, 30 April 2009, "Information and Communications Technology (ICT) Capabilities for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations"

ooo. DODI 3000.05, 16 September 2009, "Stability Operations"

ppp. NSTISSP No. 11, Revised June 2003, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products"

qqq. Committee on National Security Systems (CNSS) Policy No. 15, 29 March 2010, "National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems"

rrr. Executive Order 12333, 4 December 1981, "United States Intelligence Activities"

sss. "Network Connection Policy for Joint Worldwide Intelligence Communications System," January 1995

ttt. DOD CIO memorandum, 9 May 2008, "Department of Defense Information System Standard Consent Banner and User Agreement"

uuu. DOD 8570.01-M, 19 December 2005 (CH 2, 20 April 2010), "Information Assurance Workforce Improvement Program"

vvv. Armed Forces, Uniform Code Military Justice, Article 92, Section 892

www. Military Extraterritorial Jurisdiction Act of 2000, 18 U.S.C. 3261, et seq.

xxx. DODI 3020.41, 3 October 2005, "Personnel Authorized to Accompany the U.S. Armed Forces"

yyy. Newton's Telcom Dictionary

zzz. Alliance for Telecommunications Industry Solutions, Telecom Glossary 2011

GLOSSARY

PART I -- ABBREVIATIONS AND ACRONYMS

A

ADNI	Associate Director of National Intelligence
ALERTORD	alert order
AMET	Agency Mission Essential Task List
AOR	area of responsibility
APL	approved products list
ATC	approval to connect

B

BMA	Business Mission Area

C

CAM	Coordination Alert Message
CAO	Connection Approval Office
CCA	circuit card assemblies
CCRI	Command Cyber Readiness Inspection
CC/S/A	combatant command/Service/Agency/DOD and joint activities
CD	cross domain
CDR	Commander
CDRB	Cross Domain Resolution Board
CDS	Cross Domain Solution
CDSE	Cross Domain Support Element
CDTAB	Cross Domain Technical Advisory Board
CENTRIXS	Combined Enterprise Regional Information Exchange System
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CND	computer network defense
CNDSP	Computer Network Defense Service Provider
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COMSEC	communications security
CONOPS	concept of operations
CONPLAN	concept plan
CSIP	Cyber Security Inspection Program
CSS	Central Security Service
CT&E	Certification Test and Evaluation
CTO	Communications Tasking Order

C

CUSR	Central United States Registry

D

DAA	Designated Accrediting Authority
DDOE	DISA Direct Order Entry
DEPORD	deployment order
DFARS	Defense Federal Acquisition Regulations System
DIA	Defense Intelligence Agency
DIACAP	DOD Information Assurance Certification and Accreditation Program
DIMA	Defense Intelligence Mission Area
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISN-LES	DISN-Leading Edge Services
DITPR	DOD Information Technology Portfolio Repository
DMZ	demilitarized zone
DNI	Director of National Intelligence
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DOS	Department of State
DOT&E	Director, Operational Test and Evaluation
DREN	Defense Research Engineering Network
DRSN	Defense Red Switch Network
DSAWG	Defense IA Security Accreditation Working Group
DSN	Defense Switched Network
DSS	Defense Security Service
DTM	Directive-Type Memorandum
DVS	DISN Video Services

E

EAR	Export Administration Regulations
EI	End Instrument
EIEMA	Enterprise Information Environment Mission Area
EMSS	Enhanced Mobile Satellite Services
EO	End-office
EXORD	execute order

F

FOIA	Freedom of Information Act
FRAGO	fragmentary order

G

GAO	Government Accountability Office

G

GEF	Guidance for the Employment of the Force
GIAP	GIG Interconnection Approval Process
GIG	Global Information Grid
GWP	GIG Waiver Panel

I

IA	information assurance
IATC	interim approval to connect
IAW	in accordance with
IC	intelligence community
ICD	Intelligence Community Directive; initial capabilities document
ICT	information and communications technology
IP	internet protocol
IS	information system
ISP	Internet Service Provider
IST	Integrated Services Telephone
IT	information technology
ITAR	International Traffic in Arms Regulations
ITSP	Internet Telephony Service Provider

J

JER	Joint Ethics Regulation
JMET	Joint Mission Essential Task List
JP	Joint Publication
JROC	Joint Requirements Oversight Council
JSCP	Joint Strategic Capabilities Plan
JWICS	Joint Worldwide Intelligence Communication System

M

MA	mission area
MAC	mission assurance category
MDF	main distribution frame
MFS	Multi-function Switch
MFSS	Multi-function SoftSwitch
MNIS	Multinational Information Networks Implementation
MOA	memorandum of agreement
MOU	memorandum of understanding

N

NATO	North Atlantic Treaty Organization
NDTM	Network Defense Tasking Message

N

NIPRNET[38]	Non-Secure Internet Protocol Router Network
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NMCC	National Military Command Center
NMCS	National Military Command System
NSA	National Security Agency
NSS	national security system
NSTISSP	National Security Telecommunications and Information Systems Security Policy

O

ODM	Operational Directive Message
OPLAN	operation plan
OPORD	operations order

P

PAA	Principal Accrediting Authority
PBX	public branch exchange
PDS	protected distribution system
PGI	procedures, guidance and information
PLANORD	planning order
PMO	Program Management Office
POA&M	plan of action and milestones
POC	point of contact
POP	point of presence
PPSM	Ports, Protocols, and Service Management
PSTN	Public Switched Telephone Network

R

RTS	real time services

S

SCI	sensitive compartmented information
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SDREN	SECRET Defense Research Engineering Network
SGS	SIPRNET GIAP System
SIPRNET	SECRET Internet Protocol Router Network
SMEO	Small End Office
SNAP	systems/networks approval process
SP	Special Publication

[38] The acronym is based on the DOD Dictionary and JP 1-02 (reference s). Other uses of this acronym include Unclassified But Sensitive Internet Protocol Router and Non-Classified Internet Protocol Router Network.

S

ST&E	Security Test and Evaluation
STE	Secure Telephone Equipment
STIG	Security Technical Implementation Guides

T

TASKORD	tasking order
TR	telecommunications request
TSC	Theater Security Cooperation
TSO	telecommunications service order
TSP	telecommunications service priority

U

UC	Unified Capabilities
UCDMO	Unified Cross Domain Management Office
UCMJ	Uniform Code of Military Justice
UCP	Unified Command Plan
UCR	Unified Capabilities Requirements
UN	United Nations
U.S.C.	United States Code
USCYBERCOM	United States Cyber Command
USD AT&L	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USG	U.S. government
USSOCOM	U.S. Special Operations Command
USSTRATCOM	U.S. Strategic Command

V

VMS	Vulnerability Management System
VoIP	Voice over Internet Protocol
VoSIP	Voice over Secure Internet Protocol
VTC	video teleconference

W

WARNORD	warning order
WMA	Warfighting Mission Area

(INTENTIONALLY BLANK)

PART II -- DEFINITIONS

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

accreditation. See CNSSI No. 4009 (reference t).

authorizing official. See CNSSI No. 4009 (reference t).

authorization to operate. See CNSSI No. 4009 (reference t).

backside connection. Use of another organization's direct connection for connectivity into the Defense Information System's Network (DISN) backbone by another DOD entity, mission partner, or contractor. (CJCSI 6211.01D)

baseline point-to-point cross domain solution (CDS). Point-to-point cross domain solution providing the ability to access or transfer information between two or more security domains. Note: A baseline point-to-point solution may require tailoring or modification for implementation. (CJCSI 6211.02D)

Blue Team. See CNSSI No. 4009 (reference t).

centralized cross domain solution (CDS). Cross domain solution that is centrally managed and operated to provide the ability to access or transfer information between two or more security domains. (CJCSI 6211.02D)

certification. See CNSSI No. 4009 (reference t).

Certification Test and Evaluation (CT&E). See CNSSI No. 4009 (reference t).

civil-military partners. U.S. departments and agencies, foreign governments and security forces, global and regional international organizations, U.S. and foreign nongovernmental organizations, and private sector individuals and for-profit companies ("private sector") working in partnership with U.S. and allied military forces. (DODI 8220.02, reference nnn)

cloud computing. See CNSSI No. 4009 (reference t).

Communications Security (COMSEC). See CNSSI No. 4009 (reference t).

community risk. See CNSSI No. 4009 (reference t).

compromise. See CNSSI No. 4009 (reference t).

Computer Network Defense (CND). See CNSSI No. 4009 (reference t).

Configuration management. See CNSSI No. 4009 (reference t).

connection approval. See DODD 8500.01E (reference e).

connectivity. Anything physically or logically connected to a customer's/user's enclave/network. (CJCSI 6211.01D)

core enterprise services. A common set of enterprise services within the enterprise information environment, which provide awareness of, access to, and delivery of information on the GIG. (As defined in Enterprise Information Environment, DODI 8115.01, reference ss.)

Cross Domain Resolution Board (CDRB). Senior DOD and IC members jointly acting to provide CD risk mitigation recommendations to DOD and IC approval authorities fostering a common resolution approach to evaluate and address CD requirements, test and evaluation of products, and reciprocity between the Department of Defense and IC. (CJCSI 6211.02D)

cross domain solution (CDS). See CNSSI No. 4009 (reference t).

data. See CNSSI No. 4009 (reference t).

defense contractor. Means an employer engaged in (1) the production, maintenance, or storage of arms, armament, ammunition, implements of war, munitions, machinery, tools, clothing, food, fuel, or any articles or supplies, or parts or ingredients of any articles or supplies; or (2) the construction, reconstruction, repair, or installation of a building, plant, structure, or facility; under a contract with the United States or under any contract which the President, the Secretary of War [the Secretary of the Army and the Secretary of the Air Force], the Secretary of the Navy, or the Secretary of Transportation certifies to such employer to be necessary to the national defense. (Title 41, Chapter 1, reference v)

Defense Information Systems Network (DISN). See JP 1-02 (reference s).

Defense Red Switch Network (DRSN). This global, secure voice service provides the President, Secretary of Defense, Joint Chiefs of Staff, combatant commanders and selected agencies with command and control secure voice and voice-conferencing capabilities up to the Top SECRET SCI level. (CJCSI 6211.02).

Defense Switch Network (DSN). See JP 1-02 (reference s).

Demilitarized Zone (DMZ). See CNSSI No. 4009 (reference t).

Designated Accrediting Authority (DAA). See CNSSI No. 4009 (reference t).

DOD information networks. Globally interconnected, end-to-end set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel. DOD information networks include owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. (UCP 2011, reference a)

enclave. See CNSSI No. 4009 (reference t).

enterprise cross domain (CD) service. A cross domain solution provided as a system across an enterprise infrastructure, fully integrated to provide the ability to access or transfer information between two or more security domains. (CJCSI 6211.02D).

enterprise services. A common set of information resource capabilities designed to provide awareness of, access to, and delivery of information. (DODD 8000.01, reference d)

external network. See CNSSI No. 4009 (reference t).

Global Information Grid (GIG). See CNSSI No. 4009 (reference t).

incident. See CNSSI No. 4009 (reference t).

information assurance (IA). See CNSSI No. 4009 (reference t).

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. (Telecommunications Act of 1996, reference u)

information system. See CNSSI No. 4009 (reference t).

Information Technology (IT). See CNSSI No. 4009 (reference t).

interconnection. See JP 1-02 (reference s).

Internet. See CNSSI No. 4009 (reference t).

Internet-based capabilities. All publicly accessible information capabilities and applications available across the Internet in locations not owned, operated, or controlled by the Department of Defense or the federal government. Internet-based capabilities include collaborative tools such as social networking sites, social media, user-generated content, social software, e-mail, instant messaging, and discussion forums (e.g., YouTube, Facebook, Myspace, Twitter, Google Apps). (DTM 09-026, "Responsible and Effective Use of Internet-based Capabilities," reference nn)

Internet Protocol (IP). See CNSSI No. 4009 (reference t).

minimize. See JP 1-02 (reference s).

Mission Assurance Category (MAC). See CNSSI No. 4009 (reference t).

Mission Partners. Those with whom the Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. government; state and local governments; allies, Coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector. (DODD 8000.01, reference d)

National Security System (NSS). See CNSSI No. 4009 (reference t).

network. See CNSSI No. 4009 (reference t).

off-net calling. Telephone calls that are carried in part on a network but are destined for a phone not on the network, i.e., some part of the conversation's journey will be over the public switched network or over someone else's network. (CJCSI 6211.02D from Newton's Telcom Dictionary (reference yyy))

on-net. Telephone calls that stay on a customer's private network, traveling by private line from beginning to end. (CJCSI 6211.02D from Newton's Telcom Dictionary(reference yyy))

precedence. In communications, a priority of importance designation assigned by the originator. Example: The ascending order of precedence for military telephonic communications is:

- ROUTINE. Precedence designation applied to official U.S. government communications that require rapid transmission by telephonic means but do not require preferential handling.

- PRIORITY. Precedence reserved generally for telephone calls requiring expeditious action by called parties and/or furnishing essential information for the conduct of U.S. government operations.

- IMMEDIATE. Precedence reserved generally for telephone calls pertaining to (1) situations that gravely affect the security of national and allied forces; (2) reconstitution of forces in a post-attack period; (3) intelligence essential to national security; (4) conduct of diplomatic negotiations to reduce or limit the threat of war; (5) implementation of federal government actions essential to national survival; (6) situations that gravely affect the internal security of the United States; (7) civil defense actions concerning the U.S. population; (8) disasters or events of extensive seriousness having an immediate and detrimental effect on the welfare of the population; and (9) vital information having an immediate effect on aircraft, spacecraft, or missile operations.

- FLASH. Precedence reserved generally for telephone calls pertaining to (1) command and control of military forces essential to defense and retaliation; (2) critical intelligence essential to national survival; (3) conduct of diplomatic negotiations critical to the arresting or limiting of hostilities; (4) dissemination of critical civil alert information essential to national survival; (5) continuity of federal government functions essential to national survival; (6) fulfillment of critical U.S. internal security functions essential to national survival; and (7) catastrophic events of national or international significance.

- FLASH OVERRIDE. A capability available to: (1) The President of the United States, Secretary of Defense, and Joint Chiefs of Staff. (2) Commanders of combatant commands when declaring Defense Condition One or Defense Emergency. (3) USNORAD when declaring either Defense Condition One or Air Defense Emergency and other national authorities the President may authorize. (4) FLASH OVERRIDE cannot be preempted in the DSN. (5) FLASH OVERRIDE. A DRSN capability available to: (a). The President of the United States, Secretary of Defense, and Joint Chiefs of Staff. (b). Commanders of combatant commands when declaring Defense Condition One or Defense Emergency. (c). USNORAD when declaring either Defense Condition One or Air Defense Emergency and other national authorities that the President may authorize in conjunction with Worldwide Secure Voice Conferencing System (WWSVCS) conferences. FLASH OVERRIDE cannot be preempted. (CJCSI 6211.02D)

Protected distribution system (PDS). See CNSSI No. 4009 (reference t).

Readiness Assessment (RA) Level Definitions

- RA-1: Issues and/or shortfalls **have negligible impact** on readiness and ability to execute assigned mission(s) in support of the National Military Strategy (NMS) as directed in the Guidance for the Employment of the Force (GEF) and Joint Strategic Capabilities Plan (JSCP).

- RA-2: Issues and/or shortfalls **have limited impact** on readiness and ability to execute assigned missions in support of the NMS as directed in the GEF and JSCP.

- RA-3: Issues and/or shortfalls **have significant impact** on readiness and ability to execute assigned mission(s) in support of the NMS as directed in the GEF and JSCP.

- RA-4: Issues and/or shortfalls **preclude accomplishment** of assigned mission(s) in support of the NMS as directed in the GEF and JSCP. (CJCSI 3401.01E, reference iii)

reciprocity. See CNSSI No. 4009 (reference t).

records. See CNSSI No. 4009 (reference t).

records management. See CNSSI No. 4009 (reference t).

risk management. See CNSSI No. 4009 (reference t).

secure communications. See CNSSI No. 4009 (reference t).

Secure Internet Protocol Router Network (SIPRNET). See JP 1-02 (reference s).

security control assessment. See CNSSI No. 4009 (reference t).

security domain. See CNSSI No. 4009 (reference t).

security inspection. See CNSSI No. 4009 (reference t).

Security Test and Evaluation (ST&E). See CNSSI No. 4009 (reference t).

Sensitive Compartmented Information. See CNSSI No. 4009 (reference t).

services. A set of functionality enabled by a provider for consumers. Examples: cloud services, video services, and instant messaging. (CJCSI 6211.02D from Alliance for Telecommunications Industry Solutions, Telecom Glossary 2011 (reference *zzz*))

sub-network. A section of a large network that functions as an independent network but does not appear separate to remote networks. (CJCSI 6211.02D)

Suite B Cryptography. A specific set of cryptographic algorithms suitable for protecting both classified and unclassified national security systems and information throughout the U.S. government and to support interoperability with allies and Coalition partners. See CNSS No. 4009 (reference t).

system. See CNSSI No. 4009 (reference t).

system connection. See CNSSI No. 4009 (reference t).

transport. To convey information from one location to another. (CJCSI 6211.02D from Alliance for Telecommunications Industry Solutions, Telecom Glossary 2011 (reference *zzz*))

tunneling. See CNSSI No. 4009 (reference t).

Unified Capabilities (UC). The integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities. (DODI 8100.04, reference f)

UC transport. The secure and highly available enterprise network infrastructure used to provide voice, video, and/or data services through a combination of DOD and commercial terrestrial, wireless, and satellite communications capabilities. (DODI 8100.04, reference f)

vulnerability assessment. See CNSSI No. 4009 (reference t).

(INTENTIONALLY BLANK)

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu