CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6
DISTRIBUTION: A, B, C, J, S

CJCSI 6211.02C
9 July 2008

DEFENSE INFORMATION SYSTEM NETWORK (DISN): POLICY AND 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) to the Defense Information System Network (DISN).

a. Additional policies governing other subnetworks of the DISN networks are covered in the following instructions:

(1) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6250.01, “Satellite Communications” (reference a).

(2) CJCSI 6215.01, “Policy for Department of Defense Voice Networks” (reference b).

b. Policy on sensitive compartmented information (SCI) is covered in Director of Central Intelligence Directive (DCID) 6/3, “Protecting Sensitive Compartmented Information within Information Systems” (reference c).

c. This instruction does not cover connection policy to research, development, test, and evaluation networks such as the Defense Research and Engineering Network or Advanced Concept Technology Demonstration networks.[1]

[1] These networks must follow DISN connection and DOD cross domain processes and procedures if connecting to the DISN.

2. Cancellation. CJCSI 6211.02B, 31 July 2003, "Defense Information System Network (DISN): Policy, Responsibilities and Processes," is canceled.

3. Applicability. This instruction applies to the Joint Staff; combatant commands, Services, and Defense agencies (CC/S/As); and DOD field and joint activities, including DOD and Service Nonappropriated Fund Instrumentalities. This instruction also applies to non-DOD governmental DISN users and contractors in facilities that interconnect with the DISN.

4. Policy. See Enclosure A.

5. Responsibilities. See Enclosure B.

6. Summary of Changes. This revision updates CJCSI 6211.01B. It further:

a. Moves to the concept of baseline CD services and solutions (i.e., enterprise CD services, centralized CD solutions, and baseline point solutions) providing the primary capabilities for information sharing between different security domains.

b. Replaces DISN Designated Approving Authorities (DISN DAAs) with the new DOD Principal Accrediting Authorities (PAAs). Additionally, replaces the DISN Flag Panel with the DISN/Global Information Grid (GIG) Flag Panel.

c. Updates certification and accreditation (C&A) guidance based on the DOD Information Assurance Certification and Accreditation Process (DIACAP) implementation in accordance with (IAW) DOD Instruction (DODI) 8510.01 (see reference d).

d. Focuses on policy and responsibilities. Specific process steps will be maintained and updated as required by the Defense Information Systems Agency (DISA).

e. Transfers Cross Domain Solutions Assessment Panel responsibilities to Cross Domain Resolution Board (CDRB) chaired by the Director, Unified Cross Domain Management Office (UCDMO).

f. Makes CC/S/A headquarters responsible for endorsing and validating requirements for CC/S/A organization CD information transfer and non-DOD connection requests.

g. Adds DOD requirement to register ISs connected to the DISN in the DOD Information Technology (IT) Portfolio Repository (DITPR) or the SECRET Internet Protocol Router Network (SIPRNET) IT Registry.

h. Adds UCDMO responsibilities and roles.

i. Provides updated guidance on official and authorized use of DISN IAW DOD Regulation 5500.7-R (reference e). Additionally, updates guidance covering violations of standards of conduct prescribed in the regulation IAW DODD 5500.7 (reference f).

j. Provides reciprocity guidance for connection of ISs to facilitate the establishment of joint bases, combatant command operational requirements, and the migration to net-centric warfare.

7. 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 g) and Committee on National Security Systems (CNSS) Instruction (CNSSI) 4009, "National Information Assurance Glossary" (reference h).

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (including 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/doctrine.

9. Effective Date. This instruction is effective immediately.

For the Chairman of the Joint Chiefs of Staff:

STEPHEN M. GOLDFEIN
Major General, USAF
Vice Director, Joint Staff

Enclosures:

A	-- Policy
B	-- Responsibilities
C	-- Connection Process
D	-- DISN Security Information Assurance Program
E	-- References
GL	-- Glossary

(INTENTIONALLY BLANK)

DISTRIBUTION

Distributions A, B, C, and J plus the following:

	Copies
Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer	2

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages. Use this list to verify the currency and completeness of the document. An “O” indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 through 4	O	C-A-1 through C-A-8	O
i through viii	O	C-B-1 through C-B-6	O
A-1 through A-8	O	D-1 through D-8	O
B-1 through B-22	O	E-1 through E-4	O
C-1 through C-4	O	GL-1 through GL-8	O

(INTENTIONALLY BLANK)

RECORD OF CHANGES

Change No.	Date of Change	Date Entered	Name of Person Entering Change

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

Page

ENCLOSURE A -- POLICY

ENCLOSURE B -- RESPONSIBILITIES

ENCLOSURE C -- CONNECTION PROCESS

APPENDIX A -- DISN CONNECTION

Page

ENCLOSURE A

POLICY

1. Defense Information System Network (DISN) Background

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

(1) The sustaining base infrastructure (i.e., base, post, camp or station, and Service enterprise enclaves) interfaces with the long-haul infrastructure to support strategic/fixed environment user telecommunications requirements. The sustaining base segment is primarily the responsibility of the CC/S/A.

(2) The long-haul telecommunications infrastructure and its associated services are the responsibility of the DISA.

(3) The deployed warfighter and associated combatant commander telecommunications infrastructures 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 combatant command telecommunications infrastructure within the theater.

b. The DISN provides the GIG transfer infrastructure by connecting separate CC/S/A and field activity ISs into a DOD enterprise-wide network to meet common-user and special purpose information transfer requirements.

c. DISN information transfer facilities support secure transport requirements for subnetworks such as the Defense Switched Network (DSN), Defense Red Switch Network (DRSN), Non-Secure Internet Protocol Router Network (NIPRNET),[2] SIPRNET, DISN Video Services

[2] Based on DOD dictionary and JP 1-02 (reference g). Other uses of the acronym include Unclassified But Sensitive Internet Protocol Router Network (DOD IT Portfolio Registry) and Non-Classified Internet Protocol Router Network (DODI 8500.2 (reference k)).

(DVS) Network, Enhanced Mobile Satellite Services (EMSSs), and other government agency networks.

d. The DISN's long-haul telecommunications infrastructure is designated as a mission critical[3] and mission assurance category (MAC) I national security system (NSS). The DISN and its subnetworks must be operated and protected IAW DODD 8500.01E (reference i) and other 8500 series issuances.

(1) The DISN SIPRNET, NIPRNET, DRSN, and EMSS subnetworks are designated as mission critical IAW DODI 5000.2 (reference j).

(2) The DISN SIPRNET, DRSN, and EMSS subnetworks are designated as MAC I ISs handling information vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of content and timeliness. These subnetworks must implement designated MAC I information assurance (IA) controls IAW DODI 8500.2 (reference k) and DODI 8510.01 (reference d).

2. Policy

a. DOD will use DISN services to satisfy DOD long-haul and wide area network transfer communications requirements IAW DODI 4640.14 (reference l).

b. The DISN will use secure configurations of approved IA and IA-enabled IT products (i.e., National Information Assurance Partnership/Federal Information Processing Standards evaluated/approved products), certified IA personnel, and strict configuration control.

c. DOD ISs[4] connected to DISN must be certified and accredited IAW applicable guidance and processes (i.e., DODI 8510.01 (reference d), DODI 8100.3 (reference m), or DCID 6/3 (reference c)).

[3] A system that meets the definitions of "information system" and "national security system" in the Clinger Cohen Act, the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. See DODI 5000.2 (reference j).
[4] Includes DOD-owned ISs and DOD-controlled ISs operated on behalf of the Department for Defense that receive process, store, display, or transmit DOD information, regardless of classification or sensitivity.

d. Non-DOD (see Glossary) ISs operating on behalf of the Department of Defense must be certified and accredited IAW applicable DOD guidance and processes (i.e., DODI 8510.01 (reference d) or DOD 5220.22-M, "National Industrial Security Program Operating Manual" (NISPOM) (reference n)).

e. DOD ISs must be registered in the DITPR or the SIPRNET IT registry by the responsible CC/S/As or field activities IAW DOD Chief Information Officer (CIO) memorandum (reference o).

f. Non-DOD ISs operating on behalf of the Department of Defense must be registered in the DITPR or the SIPRNET IT registry by the sponsoring CC/S/As or field activities IAW DOD CIO memorandum (reference o).

g. Unclassified IS applications connected to the DISN must be registered in the systems/networks approval process (SNAP) system Web-based application, the systems approval process (SysAP).

h. DOD ISs connected to the DISN must be covered by accredited Computer Network Defense Service (CNDS) providers IAW DODD O-8530.1 (reference p).

i. Non-DOD ISs connected to the DISN must be covered by accredited CNDS providers IAW DODD O-8530.1 (reference p).[5]

j. Direct or indirect DISN connections must follow the connection policies and responsibilities established in this instruction. They must also follow DISA connection request procedures, requirements, and processes. Connections for SCI ISs will be IAW DCID 6/3 (reference c).

k. Tunneling of classified Secret information over transport other than SIPRNET must use National Security Agency (NSA)/Central Security Service (CSS) approved cryptography. Data must be encrypted by NSA/CSS approved Type-1 cryptography when transported over a network not cleared at or above the highest level of classification of the data.

[5] The sponsoring CC/S/A or field activity must ensure that the CNDS provider requirement is defined in a contract, MOA, or MOU with the non-DOD organization or entity.

l. Connections among ISs of different security domains will be IAW this instruction, DODD 8500.01E (reference i), DODD O-8530.1 (reference p), and other applicable DOD issuances and instructions. Connections to SCI ISs must be IAW DCID 6/3 (reference c).[6]

(1) Connections of non-DOD ISs to the DISN must be sponsored, endorsed, and validated by the CC/S/A or field activity headquarters and approved by the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD(NII)/DOD CIO).

(2) All non-DOD connections to DISN require a DOD sponsor, separate connection request, and filtered access.

(3) Contractor ISs connected to the DISN must comply with this instruction, guidelines issued by DISA as the operating entity, and DOD 5220.22-M, NISPOM (reference n).[7]

m. Cross Domain Information Transfer Requirements and Capabilities

(1) CD information transfers must be used only to meet CC/S/A and field activity compelling mission requirements and must be validated by CC/S/A or field activity headquarters.

(2) CD information transfer requirements will be prioritized based on the National Military Strategic Plan for the War on Terrorism (reference q) priorities and the military objectives in the National Military Strategy (reference r).

(3) CD information transfer requirements will employ baseline capabilities and technologies[8] in the following order:

(a) Enterprise CD services, which are used to connect ISs of different security domains, will be established to fulfill operational requirements across the DOD enterprise.

(b) Centralized CD solutions, which are centrally managed and owned by a single DOD component, will be established to fulfill operational requirements across multiple organizations.

[6] SCI CD connections to a collateral DISN system will be documented in the system's DOD accreditation package.
[7] Defense Security Service has been assigned as the Cognizant Security Office for DOD implementation of the NISPOM.
[8] The Cross Domain Baseline can be found at https://www.intelink.gov/mypage/ucdmo.

(c) Baseline point CD solutions approved for operational use will be used only when an enterprise CD service or centralized CD solution is not available.

(4) When existing CD baseline services or capabilities cannot meet operational requirements, the development of new solutions must be approved IAW this instruction.

n. A DOD inspection, site visit, and assessment program[9] will support connected ISs.

(1) All ISs connected to the DISN are subject to electronic monitoring for communications management and network security. This includes site visits, compliance inspections, and remote vulnerability assessments to check system compliance with configuration standards.

(2) Scanning and monitoring by organizations external to a CC/S/A or field activity must be pre-coordinated at least 24 hours prior to the event.[10]

o. Survivability enhancements in transmission paths, routing, equipment, and associated facilities must be implemented in ISs supporting critical CC/S/A mission requirements based on the commander's or director's formal risk management process IAW DODI 8510.01 (reference d).

p. Personnel with access or privileged access to the DISN will meet the personnel security requirements IAW DOD 5200.2-R (reference s).

q. The DISN is the DOD's worldwide enterprise-level telecommunications infrastructure. It is critical to planning, mobilizing, deploying, executing, and sustaining U.S. military operations (DODD 3020.40 (reference t)).

3. Official and Authorized Use of DISN. The DISN must be used only for official and authorized purposes IAW DOD 5500.7-R (reference e).[11] Use of the DISN for non-official purposes must be authorized in writing by the CC/S/A Component head.

[9] See Enclosure D, DISN Security Information Assurance Program.

[10] This will occur with at least 24 hours notification and coordination with the CC/S/A or field activity DAA or appointed representative and U.S. Strategic Command (USSTRATCOM).

[11] 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.

a. CC/S/As may authorize categories of non-official communication after determining that such communications:

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

(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 communication system and create no significant additional cost to DOD, CC/S/A, or field activity.

b. DOD 5500.7-R (reference e) 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).

c. 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 and ensure sufficient bandwidth is available for DOD operations. 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.

d. Unauthorized DISN uses include 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 systems and/or networks.

(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.

e. DODD 5500.7 (reference f) states penalties for violation of the standards of conduct prescribed in DOD 5500.7-R (reference e) 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.

(1) The provisions concerning the official and authorized use of the DISN (federal communications) in DOD 5500.7-R (reference e) constitute lawful general orders or regulations within the meaning of Article 92 (section 892 of reference u) 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 United States Code (USC) or federal regulations. In addition, violation of any provision in DOD 5500.7-R (reference e) may constitute the UCMJ offense of dereliction of duty or other applicable punitive articles.

(2) Violation of any provision in DOD 5500.7-R (reference e) by DOD civilian employees may result in appropriate criminal prosecution, civil judicial action, disciplinary or adverse administrative action, or other administrative action authorized by USC or federal regulations.

(INTENTIONALLY BLANK)

ENCLOSURE B

RESPONSIBILITIES

1. Chairman of the Joint Chiefs of Staff (CJCS). The Chairman is responsible for developing DISN joint policy IAW DODD 8500.01E (reference i), DODI 8510.01 (reference d), and DODD 8115.01 (reference v).

a. The Chairman, Joint Chiefs of Staff, delegates to the Director for Command, Control, Communications, and Computer Systems (J-6) authority for developing joint DISN policy in support of the Warfighting Mission Area (WMA) in coordination with OASD(NII)/DOD CIO, CC/S/A, and field activities.

b. The Director for Command, Control, Communications, and Computer Systems (J-6) will:

(1) Serve as PAA for WMA IAW DODI 8510.01 (reference d).[12]

(2) Issue DOD PAA and DISN/GIG Flag Panel decisions for connection of ISs for enterprise deployment and acceptance of risk as required.

(3) Appoint a flag-level WMA PAA representative to serve as chair on the DISN/GIG Flag Panel.

(4) Appoint a flag-level representative to the UCDMO Oversight Panel IAW UCDMO charter (reference w).

(5) Appoint an O-6 or civilian equivalent as primary representative to the Defense IA/Security Accreditation Working Group (DSAWG) and alternate representatives with Joint Staff DSAWG voting authority. Provide a copy of the appointment letter to the DISN/GIG Flag Panel and the DSAWG chairperson.

(6) Appoint an O-6 or civilian equivalent representative to the CDRB.

(7) Prioritize combatant command operational CD information transfer requirements based on the CJCS priorities, the National Military Strategic Plan for the War on Terrorism (reference q), and the military objectives in the National Military Strategy (reference r).

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

(8) Monitor and report significant DISN network operations (e.g., major mission degradation) to the Chairman.

2. Combatant Commanders. In addition to responsibilities outlined in paragraph 9 (CC/S/As, DOD Field Activities, and Joint Activities), the combatant commanders will:

a. Approve the connection of deployed ISs to theater networks and their subsequent operation.

b. Endorse and validate combatant command CD and non-DOD connection requests in support of mission requirements.

c. Review and submit service restoration priority requests IAW with DISA Circular 310-130-4 (reference x).

d. Submit DISN requirements through designated Service Executive Agent channels to DISA IAW DODD 5100.3 (reference y). Commander, U.S. Special Operations Command (CDRUSSOCOM) may submit requirements directly to DISA from USSOCOM headquarters.

e. Act to prevent or mitigate the loss or degradation of Defense Critical Infrastructure supporting the DISN and retain risk decision authority for Unified Command Plan (UCP) (reference z) assigned missions and responsibilities.

3. Commander, U.S. Strategic Command (CDRUSSTRATCOM). In addition to the responsibilities outlined in paragraph 2 (above) and paragraph 9 (CC/S/As, DOD Field Activities, and Joint Activities), CDRUSSTRATCOM will:

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

b. Appoint an O-6 or government civilian equivalent as combatant command primary representative to the DSAWG and appoint alternates with USSTRATCOM DSAWG voting authority. Provide a copy of the appointment letter to the DISN/GIG Flag Panel and the DSAWG chairperson.

c. Plan, integrate, and coordinate with CC/S/As on DOD global operations by directing GIG operations and defense IAW the UCP and responsibilities in CJCSI 6510 (reference aa).

d. Assist DISA (Defense Critical Infrastructure Program (DCIP) Sector Lead for GIG) in identifying, analyzing, and assessing the DISN and its subnetwork assets and related mission impacts in coordination with other CC/S/As.

e. Issue disconnection warning orders and orders IAW with Appendix A of Enclosure C.

f. Direct joint vulnerability assessment process (JVAP) visits to assess cross domain solutions, as required.

4. Service Chiefs. In addition to responsibilities outlined in paragraph 9 (CC/S/As, DOD Field Activities, and Joint Activities), the Service Chiefs will:

a. Provide local data distribution capability to meet combatant command validated connectivity requirements. ISs must be focused on supporting operational requirements of the combatant command or parent Service and be capable of supporting contingency operations.

b. Appoint an O-6 or government civilian equivalent as primary representative to the DSAWG and alternates with Service DSAWG voting authority. Provide a copy of the appointment letter to the DISN/GIG Panel and the DSAWG chairperson.

c. In addition to the responsibilities outlined in paragraph 9.h., Services will perform the following tasks in support of Service CD information transfer requirements:

(1) Appoint an O-6 or civilian equivalent representative to the CDRB.

(2) Designate an office to work on CD activities and issues with the UCDMO.

(3) Conduct certification testing of CD technologies IAW DOD and Intelligence Community (IC) guidance and security controls as required.[13]

d. Validate operational requirements, endorse sponsoring Service organization requests, and prioritize Service CD and non-DOD connection requests.

[13] UCDMO, in coordination with DOD and IC organizations, is developing a security controls catalog for certification testing of CD technologies.

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 on these bases, posts, camps, and stations. Site support must be specified by DISA in procedural documentation and coordinated with the Service.

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

5. Director, Defense Information Systems Agency (DISA). In addition to responsibilities outlined in paragraph 9 (CC/S/As, DOD Field Activities and Joint Activities), Director, DISA will:

a. Provide transport services used for voice, data, and video services through a combination of terrestrial and satellite assets and services IAW DODD 5105.19 (reference bb).

b. Direct operation and management of DOD-owned and leased telecommunications DISN subsystems and networks.

c. Provide DISN services to satisfy CC/S/A and field activity long-haul and wide area network information transfer requirements.

d. Appoint a flag-level representative to the DISN/GIG Flag Panel.

e. Appoint an O-6 or government civilian equivalent as chairperson of the DSAWG. Provide a copy of the appointment letter to the DISN/GIG Flag Panel and DSAWG chairperson

f. Appoint an O-6 or government civilian equivalent as a primary DSAWG representative as well as alternates with DISA DSAWG voting authority. Provide a copy of the appointment letter to the DISN/GIG Flag Panel and the DSAWG chairperson.

g. Appoint an O-6 or civilian equivalent representative to the CDRB.

h. Assess the technical, programmatic, and operational feasibility of adding new services and capabilities to the DISN.

(1) Add new DISN services and capabilities in response to validated and prioritized user requirements and planned technology insertion.

(2) Analyze and satisfy requests for new DISN services in coordination with the CC/S/As.

(3) Identify capability gaps to OASD(NII)/DOD CIO when the CC/S/A requirements cannot be met feasibly by new DISN services.

i. Approve DISN connections based on validated requirements. Ensure that the connection meets technical and interoperability requirements IAW DODI 4630.8 (reference cc), CJCSI 6212.01 (reference dd), and CJCSI 6215.01 (reference b). Additionally, ensure the IS is accredited IAW DODI 8510.01 (reference d) or DCID 6/3 (reference c).[14]

j. Accredit the DISN SIPRNET to process SECRET information, including North Atlantic Treaty Organization (NATO) information, IAW DODI 8510.01 (reference d).[15]

k. Conduct network management and meet CC/S/A and field activity requirements to acquire DOD long-haul telecommunications infrastructure and services.

l. Maintain configuration management of the DISN. For example, this includes maintaining an accurate, appropriately classified, and physically and electronically protected database of existing DISN user activities (including non-DOD agencies and contractor activities). It also includes monitoring system service restoration.

m. Monitor the effectiveness of the DISN-provided services in satisfying user requirements and respond to combatant command requests for reports on system performance.

n. Plan and coordinate with the CC/S/A and field activities to identify, analyze, and assess DISN assets and mission impacts IAW DODD 3020.40 (reference t).

o. Perform required system engineering and modeling to achieve the optimal network design and implementation approach. Identify performance standards for DISN services (e.g., availability and response time) and mission survivability requirements.

[14] DISA will also ensure ISs provide adequate security, usually through remote compliance monitoring and vulnerability assessments.

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

p. Advise the Chairman, CDRUSSTRATCOM, and other combatant commanders on DISN resource allocation or events that significantly degrade the network.

q. Conduct onsite and remote compliance assessments of DISN enclaves and connections.

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

s. Serve as the primary coordinator for processing, reviewing, and implementing all DISN connection requests.

(1) Track and approve all single-level connections, employing standard equipment configuration conforming to published security configuration guidelines.

(2) Identify vulnerabilities and configuration or operational changes that affect individual or classes of accredited CD information transfer requirement implementations. Notify the DSAWG, affected CC/S/A, field activity designated accrediting authorities (DAAs), and UCDMO of such changes.

(3) Monitor connected enclave (e.g., base, camp, post, or station) accreditation and security status IAW DOD 8510.01 (reference d). Assess enclave compliance with DOD vulnerability management requirements.

(4) Provide quarterly status reports on operational DISN CD services and solutions to the OASD(NII)/DOD CIO, the DISN/GIG Flag Panel, the DSAWG, the UCDMO, and the CC/S/As.

(5) In coordination with DSAWG, review commercial Internet waiver requests to DOD ISs (network and standalone) and make recommendations to the GIG Waiver Board.

(6) Develop, maintain, and promulgate a customer connection process guide describing steps that must be followed to request and implement a DISN connection (including but not limited to NIPRNET, SIPRNET, DSN, or DVS connections). The guide will also include processes for requesting non-DOD connections to DISN and for DISN CD services and solutions.

(7) Develop and maintain databases and Web sites[16] that include the following:

(a) The SIPRNET GIG Interconnection Approval Process (GIAP) System (SGS) used to record the technical and operational characteristics of active connections. This database must also record pending and operational CC/S/A and field activity CD information transfer requirements. Access to data will be provided to the UCDMO for incorporation into a combined DOD and IC CD database.

(b) The SNAP unclassified systems database and Web site to record technical and operational characteristics of active connections and systems.

t. Conduct SIPRNET and NIPRNET compliance validation visits to high-risk connection locations. Compliance validation visits will, at a minimum, consist of traditional security checks, scanning of the connected network, enhanced compliance visits (ECVs), and a JVAP if a CD solution is operational. This includes the following tasks:

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

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

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

(4) 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).

u. In addition to responsibilities outlined paragraph 9.h., DISA will perform the following tasks in support of DOD and IC CD information transfer connection requirements:

(1) Appoint a representative to the CDRB.

(2) Coordinate, manage, and maintain the implementation of DISA-provided enterprise CD services, centralized CD solutions, and

[16] Ensure databases and Web sites are appropriately classified and have appropriate physical and electronic security.

baseline point CD solutions. Ensure feedback between DISA, the supported CC/S/A and field activities, and the UCDMO on CD services and solutions.

(3) Operate enterprise CD services on behalf of the DOD components.

(4) Designate an office to work CD activities and issues with the UCDMO.

(5) Develop the JVAP to ensure that CD information transfer requirements are assessed annually in coordination with NSA/CSS and the UCDMO.

v. Execute responsibilities IAW DODD 3020.40 (reference t) as the DCIP Defense Sector Lead Agent for the GIG.

w. Develop and maintain a central Ports, Protocols, and Services (PPS) registry IAW DODI 8551.1 (reference ff) of DOD ISs with PPS that are visible to DOD-managed network components.

6. Director, Defense Intelligence Agency (DIA). In addition to responsibilities outlined in paragraph 9 (CC/S/As, DOD Field Activities, and Joint Activities), the Director, DIA, will:

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

b. Provide threat assessments to support CC/S/A and field activity ISs and network risk assessments and decisions.

c. Appoint a flag-level representative to the DISN/GIG Flag Panel.

d. Appoint an O-6 or government civilian equivalent as primary representative to the DSAWG and alternates with DIA DSAWG voting authority. Provide a copy of the appointment letter to the DISN/GIG Flag Panel and the DSAWG chairperson.

e. In support of IC CD information transfer connection requirements, DIA will perform the following in addition to the responsibilities outlined in paragraph 9.h.:

(1) Appoint a representative to the CDRB.

(2) Coordinate, manage, and maintain the implementation of DIA-provided enterprise CD services, centralized CD solutions, and baseline point CD solutions. Ensure there is feedback among DIA and supported CC/S/A and field activities and the UCDMO on CD services and solutions.

(3) Designate an office to work on CD activities and issues with the UCDMO.

(4) Conduct certification testing of CD technologies IAW DOD and IC guidance and security controls as required.[17]

7. Director, National Security Agency (NSA)/Central Security Service (CSS). The Director, NSA/CSS (in addition to responsibilities outlined in paragraph 9 (CC/S/As, DOD Field Activities, and Joint Activities) will:

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

b. Appoint an O-6 or government civilian equivalent primary representative to the DSAWG and alternates with NSA/CSS DSAWG voting authority. Provide a copy of the appointment letter to the DISN/GIG Flag Panel and the DSAWG chairperson.

c. Appoint a representative to the CDRB.

d. Recommend techniques and procedures to minimize DISN information security vulnerabilities IAW DODD 8500.01E (reference i) and CJCSI 6510.01 (reference aa).

e. Develop and/or certify Communications Security (COMSEC) solutions. Produce keying material for all COMSEC.

f. Establish and maintain methods for performing, analyzing, and evaluating security countermeasures and attacks in support of the community evaluation of the global risk for CD solutions.

g. In support of DOD and IC CD information transfer requirements, and in addition to responsibilities outlined in paragraph 9.h., NSA/CSS will:

(1) Identify vulnerabilities that affect individual or classes of accredited implementations. Coordinate with DISA, DISN/GIG Flag Panel, DSAWG, UCDMO, and USSTRATCOM on notification of CC/S/As

[17] UCDMO, in coordination with DOD and IC organizations, is developing a security controls catalog for certification testing of CD technologies.

appointed CIOs, senior information assurance officers (SIAOs), and DAAs for affected ISs.

(2) Provide technical support to DISA for development and conduct of a CD JVAP.

(3) Designate an office to work on CD activities and issues with the UCDMO.

(4) Conduct certification testing of CD technologies IAW DOD and IC guidance and security controls as required.[18]

8. Director, Defense Security Service (DSS). The Director, in addition to responsibilities outlined in paragraph 9 (CC/S/As, DOD Field Activities, and Joint Activities), will:

a. Administer the National Industrial Security Program on behalf of DOD and non-DOD federal agencies that have entered into an agreement with the Secretary of Defense for the purpose of rendering industrial security services.

b. Serve as the DAA for all classified contractor connections to the DISN IAW DOD 5220.22-M, NISPOM (reference n).

9. CC/S/As, DOD Field Activities, and Joint Activities. The CC/S/As, DOD Field Activities, and Joint Activities will:

a. Submit long-haul, common-user transmission requirements to DISA, IAW DODI 4640.14 (reference l).

(1) Identify to DISA each DOD IS requiring long-haul, common-user information transfer services for DISN planning purposes. ISs and requirements must be identified to DISA as soon as requirements for these services are validated.

(2) Coordinate long-haul requirements for DISN access within a combatant commander's geographic AOR, combatant commander/Service/post/camp/station or agency operated facility, and DISA prior to submission.

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

[18] UCDMO, in coordination with DOD and IC organizations, is developing a security controls catalog for certification testing of CD technologies.

(4) Process sustaining base and deployable segment requirements IAW DODI 4640.14 (reference l) and the supporting components' procedures.

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

c. Appoint DAA(s) for CC/S/A and field activity ISs IAW DODD 8500.01E (reference i), DODI 8500.2 (reference k), and DODI 8510.01 (reference d).

(1) The DAA must be a U.S. citizen, an employee of the U.S. government (USG) (minimum grade of O-6 or civilian equivalent), and hold USG security clearance commensurate with ISs under the DAA's jurisdiction.

(2) The DAA may delegate accreditation approval authority if necessary. The individual delegated must be at least an O-6 or civilian equivalent and meet the requirements specified in DODD 8500.01E (reference i), DODI 8500.2 (reference k), and paragraph c. (1) above. The delegation of authority must be in writing.

d. Ensure that ISs connected to the DISN are certified and accredited IAW DOD[19] or IC C&A guidance.

e. Ensure the CC/S/A sponsoring organization provides for or aligns with an accredited CNDS provider to acquire computer network defense (CND) support for each IS or network.

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 ee). Additionally, ensure the enclaves are accredited IAW DODI 8510.01 (reference d).[20]

g. Endorse connection requirements and maintain oversight for component connections and requests.

(1) Document and endorse the requirements for connections including alternate connections.

[19] DODI 8510.01 (reference d).

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

(2) Endorse requests, validate operational requirements, and prioritize CC/S/A non-DOD connection requests.

(3) Ensure all sponsored non-DOD unclassified connections are accredited IAW DODI 8510.01 (reference d) or DCID 6/3 (reference c).

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

(5) Assign and identify to DISA a primary (O-6 or civilian equivalent) and alternate to validate and endorse CC/S/A non-DOD DISN connection requirements for CC/S/A or field activity headquarters.

h. Program, budget, fund, and provide support for assigned portions of the DISN (including procurement, training, operation, maintenance, usage fees, CD service, solution development, and physical and electronic security survivability measures).

i. Manage the DISN connected ISs in conformance with DOD NetOps and GIG policies and procedures.

j. Provide guidance in writing on authorized and prohibited uses of DISN IAW DOD 5500.7-R (reference e). Ensure user agreement and IA awareness training includes CC/S/A authorized and prohibited uses of DISN and potential penalties IAW DODD 5500.7 (reference f). See Enclosure A (Policy).

k. In support of DOD and Director of National Intelligence (DNI) CD information transfer requirements, CC/S/As will:

(1) Identify an office or point of contact (POC) to work CD activities and issues with the UCDMO.

(2) Use the CD products and solutions listed in the UCDMO CD baseline.

(3) Employ enterprise or centralized CD services whenever possible as the preferred solution for an information transfer requirement.

(4) Provide the UCDMO with information on any CC/S/A CD solution or program improvement and research and development activities.

(5) Provide the UCDMO with CD information transfer requirements.

(6) Endorse, validate, and prioritize CC/S/A or field activity operational CD information transfer requirements.

(7) Obtain combatant command validation, endorsement, and prioritization of information transfer requirements submitted in support of combatant command operations.

(8) Support development of CD strategy, roadmap, and process as required.

(9) Coordinate with UCDMO to determine availability and suitability of a CD service or solutions to meet CC/S/A CD information transfer requirement(s) prior to initiating any CD development.

(10) If required, support implementation of CC/S/A baseline CD solutions for which they are a proponent in coordination with other CC/S/A CD support offices, the UCDMO and DISA, support site personnel, and system developers.

(11) Conduct life cycle management[21] and support of a CC/S/A CD service and solution through a program management office or specified CC/S/A organization IAW DODI 5000.2 (reference j) and DODI 8580.1 (reference gg).

l. Ensure ISs are compliant with DOD IA requirements IAW DODD 8500.01E (reference i), CJCSI 6510.01 (reference aa), and DISN policy and procedures.

m. Maintain direct management responsibility to coordinate, install, test, and accept their users' host and terminal access circuits according to DOD and DISA-established criteria.

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

o. Conduct compliance inspections, assistance visits, technical engineering inspections, remote monitoring, and vulnerability assessments of DISN connections and connected enclaves in support of the DISN Information Assurance Program (Enclosure D).

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

p. Establish procedures to ensure prompt management action is taken as a result of classified information compromise or determination that classified information is at risk of compromise IAW DOD 5200.1-R (reference hh).

q. Identify and assess critical assets and supporting infrastructures required to operate CC/S/A and field activity ISs.

(1) Identify physical infrastructure assets critical to the operation of ISs and networks connected to DISN and GIG.

(2) Identify dependencies on supporting infrastructure (e.g., electrical power) or supporting networks (e.g., commercial telecommunications).

(3) Assess the susceptibility of ISs to natural or manmade damage to identify remediation or mitigation measures. Implement formal risk assessment, management, and remediation processes to ensure remediation or mitigation actions are implemented IAW risk management decisions.

(4) Ensure IS DCIP requirements are included in contingency, continuity of operations, and/or disaster preparedness plans IAW DODD 3020.40 (reference t).

r. Ensure DOD and non-DOD personnel (including supporting contractor personnel) are held personally and individually responsible and accountable for providing proper protection of classified information, controlled unclassified information, ISs, and/or networks under their custody and control IAW CJCSI 6510.01 (reference aa). DOD officials who hold command, management (e.g., DAA and Information Assurance Manager), or supervisory positions (e.g., Information Assurance Officer or supervisors) will ensure that the Information Security Program is efficiently implemented and managed within their areas of responsibility IAW DOD 5200.1-R (reference hh).

10. <u>Director, Unified Cross Domain Management Office (UCDMO)</u>. The Director will:

a. Appoint an O-6 or government civilian equivalent primary representative to the DSAWG and alternates with UCDMO DSAWG voting authority. Provide a copy of appointment letter to DISN/GIG Flag Panel and DSAWG chairperson.

b. Appoint a CD advisor to the DISN/GIG Flag Panel.

c. Chair the CDRB to review and evaluate all CD information transfer requirements.

d. Provide centralized coordination and managerial oversight for DOD and IC CD activities IAW DOD CIO and Associate Director of National Intelligence (ADNI) CIO memorandum (reference ii).

e. Develop, coordinate, and align DOD and IC CD standards, policies, guidance, and processes.

f. Maintain visibility of operational CD information transfer requirements.

g. Review and evaluate DOD and IC CD information transfer requirements and capability gaps to make recommendations on priorities, research and development, common problem sets, opportunities for requirements consolidation, and elimination of redundant or duplicative ISs development and acquisition.

h. 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.

i. Develop, maintain, and oversee a CD baseline.

(1) Establish selection criteria for the UCDMO baseline list of CD mechanisms approved for use in the DOD and IC.

(2) Develop and maintain a CD roadmap that builds on the UCDMO CD baseline, validated CD requirements, capability gaps, and emerging technologies to establish necessary capabilities for CD services.

j. Monitor, coordinate, and recommend resource allocation for CD activities.

k. Support other CD-related activities as directed by the DOD CIO and the ADNI CIO Chaired Oversight Panel.

11. <u>Principal Accrediting Authorities (PAAs)</u>. The PAAs will:

a. Approve connection of ISs to the DISN and their subsequent enterprise-wide operation.[22]

b. Resolve accreditation issues among mission areas (MAs), as required.

c. Represent the interests of the MA and, as required, issue accreditation guidance specific to the MA, consistent with DODI 8510.01 (reference d).

d. Appoint flag-level (e.g., general officer or senior executive) PAA representatives to the DISN/GIG Flag Panel.

e. Designate a DAA for MA ISs, if required, in coordination with appropriate CC/S/A or field activity.

12. DISN/GIG Flag Panel. The DISN/GIG Flag Panel will:

a. Consist of the Enterprise Information Environment Mission Area (EIEMA); WMA; Defense Intelligence Mission Area (DIMA); and Business Mission Area (BMA) PAA and flag-level representatives from DISA, DIA, NSA/CSS, and USSTRATCOM. Other organizations, such as ADNI CIO and UCDMO, may be invited to attend the DISN/GIG Flag Panel as advisors on a regular basis.

b. Make or delegate risk decisions for information exchanges and connections among MA ISs.

c. Make or delegate DOD and non-DOD information connection risk decisions including interagency and foreign military IS connections.

d. Approve or delegate connection authority to include CD services and solutions.

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

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

[22] The DOD Component DAA responsible for an enterprise service will register the service as a system, maintaining C&A documentation and managing the service IAW DODDs and DODIs. The DAA for an enterprise service may be appointed by a PAA.

g. Provide oversight and review accreditation decisions for operation of enterprise-level systems (e.g., applications, enclaves, or outsourced IT services) and/or networks based on mission impact, security risk, and resource calculations. Examples of enterprise-level systems include Network Centric Enterprise Services, Network Enabled Command and Control, the Armed Forces Health Longitudinal Technology Application, and the Defense Finance and Accounting System.

h. Provide accreditation and GIG IA advice and risk assessment recommendations to the PAAs, CC/S/A and field activity DAAs, milestone decision authorities, Joint Requirements Oversight Council, and other capabilities boards and bodies that approve deviations from policy that may impact the IA posture of the GIG (e.g., GIG Waiver Board).

i. Resolve security disputes among MAs.

j. Review and adjudicate CD conflicts and issues brought forward from the CDRB.

k. Forward unresolved issues to the PAAs with DISN/GIG Flag Panel recommendations for final decisions as required.

13. Defense IA/Security Accreditation Working Group (DSAWG). The DSAWG will:

a. Consist of representatives from the Joint Staff, Office of the Under Secretary of Defense for Intelligence, OASD(NII), USSTRATCOM, Services, DISA, DIA, NSA/CSS, Office of the DNI CIO, and the UCDMO. Other organizations may be invited to attend as technical advisors.

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

c. Decide on or approve actions under authority delegated by the DISN/GIG Flag Panel.

d. Make connection approval recommendations to the DISN/GIG Flag Panel.

e. Make connection approval and risk decisions for those classes of ISs and circumstances delegated by the DISN/GIG Flag Panel (e.g., similar architectures and CD solutions previously approved by the DISN/GIG Flag Panel).

f. Recommend to the DISN/GIG Flag Panel disconnection or disapproval of a CD solution.

g. Recommend changes to DOD security policy and responsibilities.

h. Guide or assist development of DISN integrated system/security architecture changes.

i. Provide community risk assessments.

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

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. Establish a Cross Domain Technical Advisory Board (CDTAB). The CDTAB will:

(1) Assess technical risk of cross domain solutions.

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

(3) Advise and make recommendations to the DSAWG and CDRB on CD technical issues and details.

m. Monitor life cycle of the DISN long-haul service to identify and resolve security issues.

n. Recommend DISN resource prioritization for DISN connection requests to the DISN/GIG Flag Panel.

o. Provide security assessments to the Office of the Secretary of Defense (OSD) GIG Waiver Board in support of the DOD CIO GIG Waiver Process. Note: The OSD GIG Waiver Board supports the DOD CIO Executive Board for Requests for Waiver pertaining to the DISN.

14. <u>CC/S/A, DOD Field Activities, and Joint Activities Designated Accrediting Authorities (DAAs)</u>. The DAAs will:

a. Ensure IS certification is accomplished and accreditation decision granted IAW DODI 8510.01 (reference d).

b. Ensure ISs comply with the DISN connection approval process (CAP) and that system and enclave information in SGS and SNAP databases is current and accurate.

c. Ensure annual IS security reviews are completed and documented IAW DODI 8510.01 (reference d).

d. Identify and inform other DAAs affected by the connection and assist in developing the associated community risk assessment.

e. Ensure a local risk assessment of each connection implementation is conducted to determine whether the local risk level is acceptable.

f. Maintain configuration control of the connections.

g. Conduct the following in support of DOD CD information transfer requirements and connections.

(1) Ensure operational and functional requirements for CD information transfer requirement requests are correct.

(2) Develop and maintain the CD documentation to sustain configuration control of the connection implementation, as required.

(3) Ensure and validate annual testing of CD solution security controls, operational requirements, and configuration.

(4) Notify the DISA connection office that the annual security review has been completed[23] and/or if the CD information transfer connection is no longer required.

h. Monitor and maintain IS and network compliance and vulnerability assessment results and oversee remediation and mitigation actions.[24]

i. When classified or sensitive information is exchanged between logically connected components at the same classification level and traverses areas not cleared to the same or a higher level, ensure that the

[23] The organization completing an annual security review will maintain the record copy of the annual security review and provide it to the DISA connection office if requested.

[24] Failure to complete required remediation or mitigation of CAT I and II weaknesses can result in the decision to issue a denial of authorization to operate (DATO) or disconnection from the DISN.

content of this communication is protected from unauthorized observation by acceptable means such as encryption or protected distribution systems. (See National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, reference jj.)

j. Coordinate implementation-independent information protection requirements with other affected CC/S/A or field activity DAAs.

k. Submit and maintain current information on connection requests through the DISA connection Web sites.

15. Reciprocity -- Connection to Joint/Combined Networks. The following guidance facilitates the establishment of joint bases, combatant command operational requirements, and migration to net-centric warfare. Delays to connectivity caused by CC/S/A customization of connection requirements impede mission accomplishment.

a. ISs (hardware and software) with DOD or IC accreditation documentation meeting DOD 8500 series security requirements, IA controls, and DAA-approved mitigations in place will not be denied connection for security reasons to a joint/combined network. A combatant command can deny connection based on other reasons, such as interoperability and integration factors. Services and agencies may also deny connection for interoperability or integration reasons as long as this does not conflict with combatant command authorities and missions.

b. ISs meeting DOD security requirements will not be required to meet CC/S/A unique security requirements in order to connect to the DISN.

c. Organizations requesting IS connection must provide the required DOD or IC security accreditation documentation.[25] This documentation must include any identified DAA accepted risks and an existing IT Security plan of action and milestones (POA&M) so that the joint/combined network DAA is aware of risks incurred.

d. DOD PAA or DISN/GIG Flag Panel risk decisions for a specific IS's DISN deployment will be considered the DOD and IC security standard for that IS's implementation globally.

[25] DIACAP documentation requirements include the system identification profile, DIACAP scorecard (certification determination and accreditation decision, and IT Security POA&M. The IT Security POA&M must provide information as required IAW DODI 8510.01 (reference d).

e. Accreditation decision and IS operation disputes will be resolved using the chain of command (see paragraph 16).

16. Resolution of Accreditation Decision and Information System Operation Disputes

a. Periodically, disputes over the connection and operation of specific ISs (e.g., applications) may emerge between CC/S/A and field activities. The method for resolving these issues is to use the CC/S/A and field activity chain of command.

b. The Commander, Service Chief of Staff, or Director of a CC/S/A and field activity or designated representative (e.g., CIO or DAA) is responsible for approving the deployment of ISs and accepting the risk for operating those ISs within their enclaves.

c. CC/S/A or field activity ISs deployed by forces assigned to a combatant command are under the authority of the combatant commander. In these cases, the combatant commander or his/her designated representative (e.g., CIO or DAA) is responsible for approving the deployment and operation of ISs in his/her area of responsibility.

d. The Chairman, DOD CIO, Under Secretary of Defense for Intelligence, and Under Secretary of Defense for Acquisition, Technology, and Logistics or their designated representatives (i.e., PAAs or PAA representatives) are responsible for approving enterprise-wide operation of ISs on the DISN.

(1) MA PAA decisions for enterprise-wide operation and acceptance of IS risk will be formally issued by appropriate means determined by MA PAAs (e.g., DMS message or DOD memorandum).

(2) The CC/S/A and field activity must deploy and operate ISs IAW the MA PAAs decision and conditions.

e. If CC/S/A or field activity headquarters cannot resolve a disagreement concerning the connection to and/or operation of a IS on the DISN, the following occurs:

(1) The CC/S/A or field activity headquarters will elevate the issue to the OASD(NII)/DOD CIO or Joint Staff using the appropriate chain of command.[26]

[26] Issues from the combatant commands and Service staffs should be forwarded to the Chairman. Issues from the offices of the Service Secretaries, Defense agencies, and other defense activities should be forwarded to the DOD CIO.

(2) The OASD(NII)/DOD CIO and Joint Staff will coordinate and determine the appropriate level required to resolve the issue (e.g., DISN/GIG Flag Panel, MA PAAs, DOD CIO, Chairman, or Secretary of Defense).

17. Relationship Between the GIG Waiver Board, DSAWG, and Information Assurance Panel (IAP)

a. The GIG Waiver Board approves waivers for any DOD use of non-DISA Services (i.e., DISN) IAW ASD(NII) memorandum (reference kk) and DODI 4640.14 (reference l).

b. The DSAWG provides, interprets, and implements security policy as authorized under DOD 8500 and CJCS 6500 series directives, instructions, and manuals. Additionally, DSAWG develops accreditation approval and/or accreditation recommendations to the four MA PAAs, PAA representatives, DISN/GIG Flag Panel, or DOD SIAO.

c. The IAP is jointly chaired by the Director, Defense-Wide Information Assurance Program, and the Chief, Joint Staff, Assured Information Sharing Division. IAP is responsible for acting on behalf of the Military Communications Electronics Board (MCEB) and the Director, Information and Identity Assurance, OASD(NII) to review, develop, and coordinate recommended DOD positions on IA.

d. Relationships

(1) The IAP serves as the planner level forum to vet, coordinate, and synchronize Joint IA issues raised by the DSAWG. The DSAWG members serve as the IAP's subject matter experts for DISN connection approval and security issues.

(2) The DSAWG, as requested, performs analysis on GIG waiver requests to determine compliance with security policies. It develops recommendations on the acceptability of the waiver in meeting DOD security policy and determines whether any DOD security policy waiver should be granted. In addition, the DSAWG provides recommendations to DISA as a part of the assessment of the waiver and to the OSD GIG Waiver Board Chair.

ENCLOSURE C

CONNECTION PROCESS

1. Connection Process. This enclosure provides CC/S/A and field activity responsibilities and links to DISA connection process requirements. Services and agencies may centrally develop specific technology that will be fielded to multiple sites. In such cases, those program offices will follow this process to gain approval to connect the technology/system[27] to a specific network.

a. Appendix A. Provides guidance on connection responsibilities.

b. Appendix B. Provides guidance on CD information transfer requirement responsibilities.

2. Approval for Non-DOD Connections to DISN. The OASD(NII)/DOD CIO will approve all non-DOD connections to the DISN. CC/S/As must validate and endorse non-DOD entity requests for connection to the DISN.

3. Backside Connection

a. Backside connections are permissible only between DOD entities.

b. Contractor and other non-DOD customers must be connected via a DISN solution, ordered through the DISA via the DISA Direct Order entry (DDOE)/telecommunications request (TR)/telecommunications service order (TSO) process.

(1) Contractors and other non-DOD customers cannot be backside connected.

(2) Contractors and other non-DOD customer connections require a DOD sponsor. They must also have separate connection requests and filtered access.

c. The owner of the frontside connection to the SIPRNET must only permit backside connections to be implemented behind appropriately protected enclaves within his/her infrastructure.

d. The CC/S/A or field activity DAA of the frontside connection must accept responsibility for the backside connection in his/her accreditation documentation and update his/her DISN connection package with the DISA.

[27] For example, PPS compliance or CD solutions.

e. DISA has no responsibility for providing 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.

f. In the event of a circuit problem associated with a backside connection, the backside customer will contact his or her support activity instead of the SIPRNET Monitoring Center.

4. Tunneling Classified Information. The following procedures will be followed for tunneling classified information.

a. NSA/CSS approved Type-1 cryptography must be employed for data protection.

b. Tunnel terminuses must be in facilities authorized to process the classified information being tunneled when it is not encrypted.

c. For enclaves with existing SIPRNET connections, instantiation of this solution must be documented in the enclave’s accreditation package prior to implementation. An approval to connect (ATC) or interim approval to connect (IATC) amending the current connection approval must be in place.

d. For standalone enclaves, the solution must be documented in the enclave’s accreditation package prior to implementation.

5. JWICS Connection Process Requests

a. DIA is responsible for the JWICS connection process.

b. The connection process for JWICS is documented in “Network Connection Policy for the Joint Worldwide Intelligence Communications System” (reference ll).

6. Interim Certification to Operate (ICTO) Requests

a. An ICTO is required for authority to field new ISs or capabilities for a limited time and a limited number of platforms in support of interoperability testing developmental efforts, demonstrations, exercises, or urgent operational needs.

b. <u>ICTO Approval Authority</u>

(1) The OASD(NII)/DOD CIO is the approval authority for all waivers to DOD voice network policy and for ICTO requests involving DOD voice networks.

(2) The decision to grant an ICTO[28] for all other ISs will be made by the Interoperability Test Panel (ITP) based on the sponsoring component's initial laboratory test results and the assessed impact (if any) on the operational networks to be employed.

(3) An ICTO is granted only in exceptional cases where an IS cannot complete interoperability certification testing requirements before fielding for the following reasons:

(a) Urgent operational needs require fielding prior to testing.

(b) The IS is the first to implement an interface.

(c) Similar situations may warrant granting an ICTO and are approved by the ITP.

(1) An ICTO is not granted for ISs that have completed interoperability testing and failed to meet the identified interoperability requirements.

(2) An ICTO must not exceed 6 months in duration. Extensions may be considered by the ITP.

c. <u>Accreditation Decision</u>. Authority to field new ISs or capabilities for a limited time (with a limited number of platforms to support developmental efforts, demonstrations, exercises, or urgent operational needs) also requires an interim authorization to test or interim authorization to operate (IATO) accreditation decision IAW DIACAP. The accreditation decision expiration date cannot exceed the ICTO.

[28] Spectrum certifications, IA certifications or accreditations, network manager approval, and other validations/approvals may be required and are not necessarily satisfied by Joint Interoperability Test Certification.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE C

DISN CONNECTIONS

1. Classified Connections

a. Classified CAP requirements and sample documents are found at http://iase.disa.mil/cap/.[29]

b. SIPRNET internet protocol (IP) addresses must be registered IAW requirements defined at the DOD SIPRNET Support Center (SSC) Services Web site at http://www.ssc.smil.mil/dodssc (select registration templates).[30]

c. CC/S/A and field activities will ensure that DOD IS PPSs that are externally accessible to the DOD Enterprise or CC/S/A and field activity managed networks are implemented and registered IAW DODI 8551.1 (reference ff).

2. Unclassified Connections

a. Requesting organization must register an unclassified DISN connection by completing the online CAP form, which is submitted electronically through the SNAP system Web-based application (https://snap.dod.mil/).

b. Unclassified DOD ISs connected to the DISN must be registered in the SNAP SysAP. ISs requiring registration include IS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

c. CC/S/A and field activities will ensure that DOD IS PPSs that are externally accessible to the DOD Enterprise or CC/S/A and field activity managed networks are implemented and registered IAW DODI 8551.1 (reference ff).

3. Defense Switched Network (DSN) Connection. Requesting organization must register its unclassified DOD telecommunication switches through the SNAP Web-based application (https://snap.dod.mil/).[31]

[29] Access to this area requires a DOD certificate.

[30] Only those requirements identified within an approved DOD or CJCS-level publication and/or those approved by the DSAWG will be included within the briefing slides.

[31] DSN requirements for connection can be found on the DISA DSN Web site: (http://www.disa.mil/gs/dsn/index.html)

a. The general categories of DOD unclassified switches are:

(1) DSN switch.

(2) DOD telecom switch that is part of an Interoperability and Supportability certified and J-6 validated Information Support Plan IAW CJCSI 6212.01 (reference dd).

b. An IS must have current approved products list (APL) certification or be included in the Defense Approved Products List Removal Page (end of life cycle).[32]

c. CC/S/A and field activities must request waiver and OASD(NII)/DOD CIO approval for equipment that does not appear on the DSN APL. The request waiver must be submitted IAW DODI 8100.3 (reference m) to the ITP. The waiver must state the mission critical requirement and the reason compliance is not possible or necessary.

d. Switches installed in contractor facilities must have a valid requirement and proper authorization to operate (ATO) IAW DODI 8510.01 (reference d).

e. Upon receipt of a DAA approved ATO or IATO, DISA will issue the requesting organization/user an IATC/ATC letter signed by the DSN Senior Service Manager that meets the CAP requirements to connect.

4. DISN Video Services (DVS). DVS are currently transitioning from a contractor-owned and -operated system to a government-owned and contractor-operated global system. DVS is conducting ongoing work to integrate with Net-Centric Enterprise Services (NCES).

a. Information on registering for the NCES Program is located at http://www.nces.dod.mil (NIPRNET) and http://www.disa.smil.mil/nces/ (SIPRNET).

b. Information on registering for DVS is located at http://www.disa.mil/disnvtc/ (NIPRNET).

5. Connection Documentation Requirements. The following organization documents are required for DISN connection approval.

[32] Current APL certified products can be found at the following link: http://jitc.fhu.disa.mil/apl/.

a. Statement of accreditation. The accreditation decision[33] (DIACAP scorecard) must be signed by the DAA on record. An ATO is required for a request for an ATC. An ATC will not be granted based on an IATO.

b. Detailed Enclave Topology Diagram. Outlines and reflects the network topology and all the devices (with device IP devices) that are connected logically/physically to the enclave infrastructure, including hardware, software, and firmware versions of the premise router, firewall, and internal network intrusion detection system. Examples can be found at https://iase.disa.mil/cap/.

c. Consent to Monitor (CTM) Statement[34] to DISA. Allows DISA to assess its network infrastructure. The CTM form acknowledges DISA's right to conduct remote initial and periodic vulnerability assessments of the connected host system(s) or network. The form must be submitted before the connection is granted approval to connect to the DISN.

d. Site IS security documentation IAW DODI 8510.01 (reference d) will be submitted to the appropriate Connection Approval Office (CAO), including a copy of the DIACAP scorecard. If the DISN customer has not transitioned to DIACAP, the system security authorization agreement (SSAA)[35] will be provided to DISN CAO upon request.

e. For SIPRNET connections, provide a completed SIPRNET Connection Questionnaire (SCQ).[36]

f. Register IS applications connected to the unclassified network in the SNAP system Web-based application, the SysAP.

6. Connection Approval Scan. DISA will perform an initial remote compliance assessment of the customer's enclave as part of the DISN connection approval process, and periodically thereafter. The customer's connection approval decision is based on the results of these scans.

7. Enclave Changes Requiring Notification and/or Approval

a. The following enclave changes require notification and approval of DISA.

[33] An accreditation decision is expressed as an ATO, IATO, IATT, or DATO. An IATO cannot exceed 180 days, nor may consecutive IATOs exceed 360 days IAW DODI 8510.01 (reference d).
[34] The CTM form can be found at http://iase.disa.mil/cap/.
[35] For systems that have not transitioned to DIACAP.
[36] The SCQ is available at http://iase.disa.mil/cap/.

(1) Addition or deletion of backside connection.

(2) Addition of new CD solution to an enclave.

b. The following enclave changes require notification of DISA:

(1) Change in DAA.

(2) Addition of contractors or foreign national employees, if not previously identified.

(3) Modifications to approved backside connections.

(4) Topology notifications.

8. Non-DOD Connection Requirements.[37] In addition to standard DISN connection requirements, the CC/S/A or field activity headquarters will:

a. Submit the CC/S/A or field activity headquarters memorandum[38] that validates and endorses the connection request and certifies OASD(NII) has granted approval. The CC/S/A or field activity memorandum must be submitted to DISA before a non-DOD connection is granted approval to connect to the DISN.

b. Provide proof of the connection requirement's validity before a contractor facility is granted approval to connect to the DISN. Official proof of valid connection requirement includes, but is not limited to, non-proprietary contract documents that include the following: contract dates, contract number, and contractor identification information. The contractor identified in the proof of valid connection requirement documentation must be listed in the electronic registration form.

c. Endorse the connection package for contractor and other non-DOD facility DISN connections and submit the request to DISA.

d. Ensure the CC/S/A organization sponsoring the non-DOD organization registers the classified or unclassified IS in the DITPR or SIPRNET IT registry as a contractor or non-DOD IS operated on behalf of the Department of Defense. The sponsoring organization is responsible for maintaining the current IS status in the DITPR or SIPRNET IT registry.

[37] See glossary for a definition of a non-DOD entity.

[38] At a future date, this step will be integrated into the automated registration process.

e. Maintain oversight of continuing operational justification of connection for non-DOD (see Glossary) organization requirements.

f. Notify the DSS Office of Designated Approving Authority of possible future contractor facility classified connection requirements, if applicable.

g. Ensure OASD(NII)/DOD CIO approves non-DOD connections.

h. Ensure that for contractor classified connections, DSS accredits the IS and issues the contractor facility clearance.

9. Exercise Connection. In addition to standard DISN connection requirements, the CC/S/A or field activity headquarters will endorse the connection requirement for exercises.

10. Contingency Connection

a. For contingency connections, the requesting CC/S/A or field activity organization will submit at least:

(1) An IATO issued by CC/S/A or field activity DAA.

(2) Interim enclave topology diagram and changes as needed.

(3) A CTM statement.

(4) For the SIPRNET, a completed SCQ.

b. The completed package containing IATO, diagrams, CTM, and SCQ is forwarded to DISA via the combatant commander's J-6 validation and endorsement process. The package must also identify the CD solution to be employed.

11. Disconnection

a. DISA will:

(1) Inform the DISN/GIG Flag Panel via the DSAWG of site non-compliance.

(2) Notify the site and the CC/S/A or field activity representative.

(3) Continue contact with the site to monitor remedial actions. If actions are unsatisfactory, the DISA advises USSTRATCOM IAW USSTRATCOM guidance.

b. USSTRATCOM will:

(1) Initiate coordination with enclave component to assess operational impact of the potential disconnects.

(2) Release a notification message giving 30 days to bring the connection into compliance or submit a plan to achieve compliance within 60 days of the notification message release.

(3) Issue a coordinated USSTRATCOM order to disconnect, if compliance is not achieved within 30- or 60-day windows.

(4) Issue a USSTRATCOM order for immediate disconnection, if severe non-compliance issues warrant this action.

c. DISA Network Operations will verify and implement disconnections as directed.

d. CC/S/A or field activity appointed DAA will:

(1) Upon receipt of USSTRATCOM disconnection order, notify the DISA via routine letter/message and submit disconnection request (telecommunications request (TR) through their telecommunications certification officer (TCO)).

(2) Disconnect any CD device and notify the DISA.

(3) The CC/S/A or field activity DAA may terminate a connection if the DAA determines that a connection is no longer required. The DAA will notify the DISA via routine letter/message and submit disconnection request (TR through TCO).

12. Alternate Connections. DOD long-haul communications requirements must be submitted to DISA IAW DODI 4640.14 (reference l). Section 6.2.1.4 of DODI 4640.14 (reference l) allows CC/S/A to satisfy requirements that DISA has determined cannot be filled by a conventional connection. Alternate connections require the OSD GIG Waiver Board to grant a waiver prior to operation.

a. Types of Waivers Required for Alternate Connections

(1) An Internet waiver is required for temporary approval for a CC/S/A connected to the unclassified DISN to connect to the Internet (e.g., a CC/S/A connected to the Internet using a NIPRNET Internet Access Point).

(2) A User Enclave Waiver is required for a connection to the Internet by a CC/S/A that is not connected to the unclassified DISN (e.g., a stand-alone IS connected to the Internet by a commercial Internet Service Provider).

b. Consideration for waiver approval will be based on compliance with DOD IA and CND policies and USSTRATCOM directives.

c. Requesting organization will:

(1) Acquire CC/S/A or field activity validation and endorsement of the alternate connection.

(2) Record the Waiver Approval Form for the alternate connection requested via the SNAP system Web-based application, the Waiver Registration (https://snap.dod.mil/).

(3) Provide required connection documentation.

(4) Prepare a brief IAW the standard brief format contained on the DSAWG Web site[39] and submit the prepared brief to the DSAWG for waiver approval review. The DSAWG will perform a technical review of the IA compliance assessment of the waiver and make a recommendation to the required reviewing body.

(5) Prepare an explanatory brief IAW OSD GIG Waiver Presentation instruction located on the SNAP system Web site.

d. The OSD GIG Waiver Board will review assessments from DISA, DSAWG, and other IA technical review activities before making a recommendation to the DOD CIO.

[39] The DSAWG standard brief format can be found at http://iase.disa.mil/ia-working-groups.html.

(INTENTIONALLY BLANK)

APPENDIX B TO ENCLOSURE C

CROSS DOMAIN (CD) INFORMATION TRANSFER REQUIREMENTS

1. CD Information Transfer Requirements. Requirements for CD information transfers between different security domains (e.g., classified to unclassified or SECRET to foreign allies, coalition, non-DOD government organizations, contractors, etc.) can be found on the GIAP Web site.[40]

2. CC/S/A and Field Activities Headquarters. CC/S/A and field activity headquarters will:

a. Ensure requesting organization determines and documents the information transfer and protection requirements. Documentation will include the following:

(1) Operational requirement(s).

(2) Information types and classifications.

(3) Type of user access required.

(4) Applicable policy (e.g., Security Classification guidance for classified information, Freedom of Information Act exempted information protection guidance, or Privacy Act information protection requirements).

(5) Characterization of threats to the information types and classifications (types and characterization of adversaries, adversary attack types, and motivations).

b. Conduct initial technical review of information transfer requirement and provide initial recommendation on whether an approved UCDMO enterprise service, centralized solution, or baseline point solution can be used; or whether a new or modified CD solution must be developed.

(1) Combatant command headquarters and its subordinate joint commands should initially request assistance[41] from its Service Executive Agent. This will enable it to determine if the information transfer requirement can be met by the supporting Service.[42]

[40] The GIAP Web site location is as follows: https://giap.disa.smil.mil/

[41] Combatant commands should provide a courtesy copy of request to Joint Staff J-6for JS prioritization.

[42] This is consistent with the DODD 5100.3 (reference y) requirement for Service Executive Agents to provide base operating support and move to joint basing.

(2) Other agencies or field activities unable to conduct technical review should contact UCDMO for assistance.

c. Ensure CD information transfer requirement request is submitted IAW DISA SIPRNET CD connection requirements into the SGS database.[43]

d. Endorse requests[44] and validate the operational requirement for CD information transfer between U.S. classified enclaves/networks and non-DOD organizations/entities.

e. Ensure the CD solution resides on an operating system that has been evaluated by NSA/CSS or National Institute of Standards and Technology (NIST).

f. Prioritize CD information transfer requirements requiring modified or new CD solutions quarterly. The Service, agency, or field activity CD office or CD POC will obtain combatant command validation, endorsement, and prioritization of information transfer requirements submitted in support of combatant command operations. Joint Staff will maintain a consolidated, prioritized list of combatant command information transfer requirements.

g. Ensure the CD solution completes NSA/CSS certification test and evaluation (CT&E) prior to use. The CC/S/A will ensure the CD solution developer provides NSA/CSS with requested artifacts prior to the CT&E. Examples include independent verification and validation test results and other independent CC/S/A test results.

h. Ensure the developer corrects vulnerabilities/problems discovered in evaluations of previous versions of the product before submitting the new revision. Alternatively, ensure that continuation of the vulnerability will be approved by DSAWG because of operational necessity.

[43] Can be found at Information Assurance Support Environment (IASE) URL: http://iase.disa.mil/cap/index.html -- Connection Approval Process -- SIPRNET Connection Approval Process.

[44] See Enclosure B, Paragraph 9.g.(5) for CC/S/A identification of personnel with endorsement authority.

i. Ensure the developer agrees to provide the CD solution source code upon request during the CT&E.

j. Ensure the CD solution developer leverages source code analysis tools to analyze the security and stability of its CD solution code and provides NSA/CSS with requested artifacts from this analysis.

k. CC/S/A owner of the centralized CD solution will integrate new CD information transfer requirements into the CC/S/A's centralized CD solution as directed by DSAWG or DISN/GIG Flag Panel.

l. Compete CD implementation actions that include the following:

(1) Coordinate the protection requirements for the interconnected domains, if the security domains to be interconnected are under a DOD or non-DOD DAA(s) with no DISN managed connectivity.

(2) Implement the protection requirements for the assigned domain.

(3) Operate the approved enclave connection in compliance with approved conditions provided by DISA through an ATC/IATC letter.

(4) Maintain CD architecture as a configuration record for cross domain implementation.

3. Defense Information Systems Agency (DISA). DISA will:

a. Ensure the required information is complete in SGS.

b. Determine whether or not DISN connectivity is involved.

c. Determine if existing DISN enterprise CD service can satisfy the information transfer requirement.

d. Integrate new CD information transfer requirements into DOD enterprise CD services as directed by DSAWG or DISN/GIG Flag Panel.[45]

e. Forward request packages to the CDRB if existing DISN enterprise CD service cannot meet the information transfer requirement.

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

f. DISA will accomplish the following for baseline point CD solution implementation:

(1) Work with CC/S/A CD offices, the baseline point CD program manager, and UCDMO to adapt the baseline point CD solution to the specific environment.

(2) Ensure the resulting baseline point CD solution is consistent with the overall DOD and IC architectures.

(3) Approve the engineering documentation and implementation of the adapted baseline point CD solution.

(4) Coordinate with DOD security evaluation organizations (e.g., DISA, NSA/CSS, and DIA) in performing security evaluations and risk assessments of the baseline point CD solution.

(5) Cross Domain Technical Advisory Board (CDTAB) will:

(a) Review security evaluations and risk assessments.

(b) Provide technical assistance to the DSAWG and CDRB.

(c) Forward connection recommendations to the DSAWG.

g. Issue an ATC/IATC letter notifying the site and CC/S/A DAA of the DSAWG or DISN/GIG Flag Panel decision and operating conditions (including time limits).

h. Ensure the enclave package is complete.

i. Notify the site and CC/S/A DAA of connection approval or disapproval.

4. Unified Cross Domain Management Office (UCDMO). The UCDMO will:

a. Review the information transfer request package and recommended solution forwarded by DISA.

b. Concur in CC/S/A or field activity modified CD solution recommendation or identify requirement to develop new CD solution.

c. Forward a recommendation for approval through DSAWG to the DOD component (e.g., Service, DIA, or NSA/CSS) for implementation of a CD information transfer request that can be met by a DOD-approved centralized CD solution or baseline point CD solution and circumstances authorized by DISN/GIG Flag Panel.

d. Forward a new CD development solution requirement to CDRB.

e. CDRB, chaired by the UCDMO, will:

(1) Review, maintain, and update DOD and IC prioritization lists for information transfer requirements.

(2) The DOD and IC CDRB lead representatives will conduct organization Prioritization Working Groups as needed and develop DOD and IC prioritization lists.

(3) Review SGS list of operational baseline point CD solutions and centralized CD solutions at the end of the second quarter of each fiscal year. Recommend to DISN/GIG Flag Panel and DSAWG those that can now be met by DOD enterprise CD solutions.

(4) Make recommendations on the level of change required for CD solutions and the type of security testing required to test organizations (CT&E or Security Test and Evaluation).

(5) Review test results to identify any significant issues.

5. DISN/GIG Flag Panel. The DISN/GIG Panel will:

a. Approve the connection of the enclave to the long-haul transport infrastructure if the CD information transfer requirement involves DISN-managed connectivity.

b. Delegate authority to the DSAWG for some CD information transfer decisions.

c. Resolve CD issues forwarded by the CDRB.

6. Defense IA/Security Accreditation Working Group (DSAWG). DSAWG or designated sub-working group will:

a. Review security evaluations and risk assessments.

b. Forward CD information transfer connection recommendations to the DISN/GIG Flag Panel.

(1) Review and approve CD information transfers (as delegated) or forward recommendation(s) to the DISN/GIG Flag Panel.

(2) Review continued CD connections that are considered high risk[46] annually. Approval of high-risk connections requires completion of an annual JVAP by DISA. An onsite JVAP is conducted annually or as directed by USSTRATCOM.

[46] High-risk information transfer requirement connections include those to non-DOD entities, including contractors, or those that use a baseline point CD solution.

ENCLOSURE D

DISN SECURITY INFORMATION ASSURANCE PROGRAM

1. Background. The DISN Security Information Assurance program integrates CC/S/A IA inspection and assistance visit programs to assess DISN security status.

2. Inspections and Visits

a. Site Inspections/Visits. The program consists of three levels of onsite inspections: compliance inspections, assistance visits, and technical engineering inspections/visits. Organizations will integrate the types of inspections/visits described below to determine enclave and connection security posture. Inspections will be conducted by subject matter experts familiar with IA control implementation for the organizations and specific technologies used. Examples of assets to conduct onsite inspections are inspectors general (IGs) and various assistance teams.

b. Compliance Inspections. Compliance inspections include organizations/teams (e.g., CC/S/A IG, auditors, and DSS) that provide a systemic perspective for several aspects of information assurance. The inspectors provide local accrediting authorities with a basis for immediate improvement.

(1) Compliance inspections are performed during scheduled visits.

(2) The primary focus is on documentation and synchronization between local information and centralized repositories maintained by CC/S/A and DISN network operators. Also covered are training and certification deficiencies, network and enclave documentation, and systemic issues.

c. Assistance Visits. Assistance visits include organizations/teams (e.g., CC/S/A IA organizations and DSS) able to identify and evaluate more complex security issues to provide a basis for assessing information assurance training, implementation, and operation.

(1) Assistance visits support CC/S/A respective IA programs.

(2) Assistance teams provide assistance in correcting deficiencies noted by compliance teams, assess operational procedures and practices,

and evaluate documentation and information handling. The primary focus is to identify and resolve deficient operational practices and procedures as well as device configuration issues.

(3) Assistance teams validate previous compliance inspection results and assist in resolving remaining deficiencies. They also perform repository synchronization. Unresolved training and certification deficiencies will be noted for resolution within Service and agency channels.

d. Technical Engineering Inspections. Technical Engineering inspections include organizations/teams (e.g., CC/S/A teams and the SIPRNET Inspection Team). These entities ensure that trusted devices are maintained and operated in a manner that minimizes community risk. They also provide training when necessary.

(1) Technical engineering inspections (e.g., JVAP) primarily focus on the secure engineering, implementation, and (if applicable) operation of devices that move information across security domain boundaries.

(2) Teams validate previous compliance inspection and assistance visit results. If possible, they resolve remaining deficiencies.

3. Coordination and Frequency of Inspections and Visits

a. Sites should undergo a compliance inspection and/or JVAP once per 12-month period.

b. Teams conducting IA inspections and visits must coordinate with the CC/S/A and field activities being inspected. Inspections or visits to a theater must be coordinated with the combatant command.

c. Organizations conducting IA inspections and visits will coordinate their annual inspection and visit schedules. Coordination is required by Service and agency organizations (e.g., DISA, Defense Threat Reduction Agency (DTRA), DOT&E, DSS, and NSA/CSS) to avoid multiple redundant IA inspections and visits during a 12-month period.

d. Commanders have the authority to deny additional site/inspection and assistance visits by external organizations during a 12-month period if they determine the visits would negatively impact mission accomplishment.

4. Remote Monitoring and Vulnerability Assessments. Remote monitoring and IA vulnerability assessments develop a profile of potential configuration vulnerabilities and alert the site of potential problems. Remote monitoring and vulnerability assessments begin before an enclave requests approval to connect.

a. DISA conducts remote monitoring of DISN and its long-haul infrastructure.

b. Sampling is conducted to evaluate service quality and efficiency, or to support engineering actions designed to improve network performance.

c. Security assessments will examine consistency of site topology documentation and the conformance of network resident devices with DOD IA directives, instructions, manuals, and guides (e.g., Security Technical Implementation Guides (STIGs)). DISA, CC/S/As, and DSS (for contractor sites) will perform SIPRNET enclave security assessments. CC/S/As will perform NIPRNET enclave security assessments.

5. Joint Vulnerability Assessment Methodology

a. DOD assessment teams conducting IA assessments of DISN will use the Joint Common IA Assessment Methodology (reference mm).

b. The objectives of this guide are to provide necessary background information and to define the core elements of network IA assessments. This will improve information sharing of assessment results, reduce duplication of effort by assessment teams, and allow CC/S/As to focus teams on their priorities.

c. Results of assessments using this guide can be used to satisfy multiple CC/S/A and DOD requirements (e.g., Federal Information Security Management Act annual testing requirements).

6. Inspection Criteria

a. Site visit inspections should follow published criteria for the respective CC/S/A or criteria for a particular device when classification boundaries are involved. Criteria will be established during the initial accreditation of the device.

b. The criteria for remote monitoring will be based on DOD IA directives, instructions, manuals, STIGs, vulnerability notices issued through network operations channels, or other criteria established by the CC/S/A organization conducting the monitoring and provided to monitored sites.

7. Reporting

a. Inspection/visit findings and results will be published through existing command and technical management channels and made available to the respective CC/S/A, USSTRATCOM, and DISA.

b. Results for contractors will be reported to the following: the contract management organization, the contract sponsor, long-haul network operator(s), and the supporting information assurance management organization of the contract sponsor.

c. Connection documentation formats should be modified to allow an enclave to report when it was last inspected and the type of inspection, including self-assessments.

8. Enclave Categorization. Criteria for categorizing an enclave are provided in subparagraph 9 below. This categorization will support allocating limited technical assets to enclaves having the greatest IA benefit for the interconnected community as a whole. Additionally, categorization will be used to establish inspection scope and periodicity (subparagraph 10).

9. Enclave Inspection Categories. The following categories will be applied to connected enclaves as a means to assign inspection responsibility and frequency. Categories reflect enclave configurations that potentially affect enclave/network security posture. The categories identify who will accomplish the inspection/visit, the criteria used, and the frequency of inspections/visits. Unless specifically referenced, the category criteria apply to both NIPRNET and SIPRNET enclaves.

a. Category One

(1) Enclave operates at a single classification level.

(2) Enclave employs a firewall or firewall-like device between local area network and wide area network.

(3) Enclave does not support remote access.

(4) Internet service is through a DISA-provided gateway for NIPRNET connected enclaves.

(5) No CD information transfer requirement connection(s) exist for connected enclaves.

b. Category Two

(1) Enclave operates at a single classification level.

(2) Enclave has a firewall in place.

(3) Internet service is via DISA-provided gateway for NIPRNET connected enclaves.

(4) NIPRNET enclave has central dial-in/dial-out modem banks.

(5) NIPRNET enclave has remote access virtual private network (VPN) capability.

(6) NIPRNET access with aremote access Web portal is provided via secure socket layer capability.

c. Category Three

(1) Enclave operates at a single classification level.

(2) Contractor facility has NIPRNET connectivity.

(3) SIPRNET enclave is without firewalls.

(4) SIPRNET enclave supports a dial-in capability.

d. Category Four

(1) Enclave has CD information transfer connection(s) that move information between two different classification levels (includes foreign ISs).

(2) Contractor site has SIPRNET connectivity.

(3) Site has non-U.S. personnel integrated into work force/work area with SIPRNET access.

(4) NIPRNET enclave has Internet connection but no firewall, or a firewall that is not via a DISA-provided gateway.

(5) USSTRATCOM or DISA identify the site as non-compliant in providing requested connection approval documentation or in not meeting the compliance timeline in a failed DISA remote network assessment.

10. Inspection Responsibility and Frequency Table. “DISN Networks Security Inspection Table” (Table D -1) summarizes the execution concept for the DISN Security Information Assurance Program.

	NIPRNET		SIPRNET	
Category	Frequency	Inspecting Element	Frequency (Minimum)	Inspecting Element
1	Every 3 Years	CC/S/A	Every 3 Years	CC/S/A
2	Every 3 Years	CC/S/A	Every 3 Years	CC/S/A
3 (DOD)	Every 2 Years	CC/S/A	Every 2 Years	CC/S/A
3 (Contractor)	Annual	CC/S/A	Annual	DSS
4	Annual	CC/S/A	Annual	DISA

Table D-1. DISN Networks Security Inspection Table

11. Joint Vulnerability Assessment Process (JVAP)

a. Sites with an approval to connect to the DISN are subject to an annual onsite JVAP, or as directed by USSTRATCOM.

b. The JVAP is a process using checklists as well as DISA and NSA/CSS procedures to assess specific configurations, operation, and administration of the CD solution. Types of JVAPS are as follows:

(1) Scheduled JVAP. DISA scheduled JVAPs will be performed annually and will be coordinated and scheduled in advance with the CC/S/A or field activity appointed DAA or appointed representative and the site POC.

(2) Short Notice JVAP. Short notice JVAPs will be performed as required. This may occur with limited (24 hours) notification and coordination with the CC/S/A or field activity DAA or appointed representative and POC.

c. The JVAP verifies the configuration and identifies possible security vulnerabilities of a CD solution. A CD solution connects two different security domains and restricts the information that transfers between the domains. The security posture and operations of the CD solution must comply with approved conditions to maintain connection authorization.

d. A DISA Field Security Operations (FSO) team lead will notify the CC/S/A or field activity DAA and the site representative for both scheduled and short notice JVAP visits. In cases when the DAA is not available, the CC/S/A site representative will be asked to assist in the coordination of the visit.

e. DISA and NSA/CSS will perform data collection and analysis on the CD solution(s). The collection and analysis will result in a detailed listing of vulnerabilities with recommended corrective actions. DISA will maintain the results in a secure database and provide it with appropriate electronic and physical security protections. The site will be responsible for updating status of corrective action through the CC/S/A or field activity DAA. The final report including recommended corrective action(s) will be made available to the CC/S/A or field activity DAA.

f. High-risk vulnerabilities will be corrected (when possible) before the JVAP team leaves the site. The CC/S/A or field activity DAA or appointed representative will report the status of remaining vulnerabilities until they are closed.

(INTENTIONALLY BLANK)

ENCLOSURE E

REFERENCES

a. CJCSI 6250.01, Series, “Satellite Communications”

b. CJCSI 6215.01, Series, “Policy for Department of Defense Voice Networks”

c. DCID 6/3, Series, “Protecting Sensitive Compartmented Information within Information Systems”

d. DODI 8510.01, 28 November 2007, “DoD Information Assurance and Certification and Accreditation Process (DIACAP)”

e. DOD Regulation 5500.7-R, 30 August 1993, “Joint Ethics Regulation (JER)”

f. DODD 5500.7, 29 November 2007, “Standards of Conduct”

g. Joint Pub 1-02, Series, “Department of Defense Dictionary of Military and Associated Terms”

h. CNSS Instruction No. 4009, Revised June 2006, “National Information Assurance Glossary”

i. DODD 8500.01E, 24 October 2002, “Information Assurance (IA)”

j. DODI 5000.2, 12 May 2003, “Operation of the Defense Acquisition System”

k. DODI 8500.2, 6 February 2003, “Information Assurance (IA) Implementation”

l. DODI 4640.14, 6 December 1991, “Base and Long-Haul Telecommunications Equipment and Services”

m. DODI 8100.3, 16 January 2004, “Department of Defense (DoD) Voice Networks”

n. DOD 5220.22.M, Series, “National Industrial Security Program Operating Manual”

o. CIO memorandum, 6 September 2007, "Department of Defense (DoD) Information Technology (IT) Portfolio Repository (DITPR) and DoD SIPRNET IT Registry Guidance 2007-2008"

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

q. CJCS, 4 March 2005, "National Military Strategic Plan for the Global War on Terrorism"

r. CJCS, 2004, "The National Military Strategy of the United States of America"

s. DOD 5200.2-R, January 1987, "Personnel Security Program"

t. DODD 3020.40, 19 August 2006, "Defense Critical Infrastructure Program"

u. Sections 801-940 and 1060 of title 10, United States Code

v. DODD 8115.1, Series, "Information Technology Portfolio Management"

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

x. DISA Circular 310-130-4, 18 August 1993, "Defense User's Guide to the Telecommunications Service Priority (TSP) System"

y. DODD 5100.3, 15 November 1999, "Support of the Headquarters of Combatant and Subordinate Joint Commands"

z. Unified Command Plan, 5 May 2006

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

bb. DODD 5105.19, 25 July 2006, "Defense Information Systems Agency"

cc. DODI 4630.8, 30 June 2004, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" dd. CJCSI 6212.01, Series, “Interoperability and Supportability of Information Technology and National Security Systems”

ee. United States Security Authority for NATO Affairs Instruction 1-07, 2007, “Implementation of NATO Security Requirements”

ff. DODI 8551.1, Series, “Ports, Protocols, and Services Management (PPSM)”

gg. DODI 8580.1, 9 July 2004, “Information Assurance (IA) in the Defense Acquisition System”

hh. DOD 5200.1-R, Series, “Information Security Program”

ii. Memorandum, 10 July 2006, “Establishment of a Department of Defense/Intelligence Community (ODNI) Unified Cross Domain Management Office (UCDMO)”

jj. NSTISSI No. 7003, 13 December 1996, “Protected Distribution System”

kk. ASD(NII) memorandum, 7 August 2002, “Global Information Grid Waiver Charter”

ll. “Network Connection Policy for Joint Worldwide Intelligence Communications System,” January 1995

mm. Joint Common Information Assurance Assessment Methodology, Series

nn. MCEB Publication 1, 1 March 2002, “MCEB Organization, Mission and Functions Manual”

oo. NIST Special Publication 800-37, Version 1.0, October 2002, “Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems”

pp. National Military Strategy for Cyberspace Operations, November 2006

List of Web Addresses[47]

a. Joint Electronic Library -- http://www.dtic.mil/doctrine

b. UCDMO Cross Domain Baseline -- https://www.intelink.gov/mypage/ucdmo

c. Central United States Registry -- https://secureweb.hqda.pentagon.mil/cusr/index.asp

d. SIPRNET Connection Approval Process documentation -- http://iase.disa.mil/cap/

e. DOD SSC Services -- http://www.ssc.smil.mil/dodssc

f. SNAP system Web-based application -- https://snap.dod.mil/

g. DSN -- http://www.disa.mil/gs/dsn/index.html

h. NCES program -- http://www.nces.dod.mil (NIPRNET) and http://www.nces.dod.smil.mil (SIPRNET)

i. DISN Video Services -- http://www.disa.mil/disnvtc/

j. Joint Interoperability Test Command Approved Products List (APL) -- http://jitc.fhu.disa.mil/apl/

k. Defense/IA Security Accreditation Working Group DSAWG -- http://iase.disa.mil/ia-working-groups.html

l. SIPRNET GIG Interconnection Approval Process -- https://giap.disa.smil.mil/

m. CD connection requirements under SIPRNET Connection Approval Process -- http://iase.disa.mil/cap/

[47] Links available as of 21 May 2008.

GLOSSARY

PART I -- ABBREVIATIONS AND ACRONYMS

A

ADNI	Associate Director of National Intelligence
AOR	area of responsibility
APL	approved products list
ATC	approval to connect
ATO	authorization to operate

B

BMA	Business Mission Area

C

C&A	certification and accreditation
CAO	Connection Approval Office
CAP	connection approval process
CC/S/A	combatant command, Service, and Defense agency
CD	cross domain
CDRB	Cross Domain Resolution Board
CDTAB	Cross Domain Technical Advisory Board
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
CNDS	Computer Network Defense Service
CNSS	Committee on National Security Systems
COMSEC	communications security
CSS	Central Security Service
CT&E	certification test and evaluation
CTM	consent to monitor
CUSR	Central United States Registry

D

DAA	designated accrediting authority
DATO	denial of authorization to operate
DCID	Director of Central Intelligence Directive
DCIP	Defense Critical Infrastructure Program
DDOE	DISA Direct Order Entry

D

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 System Network
DISN DAA	DISN Designated Approving Authorities
DITPR	DOD Information Technology Portfolio Repository
DNI	Director of National Intelligence
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DOT&E	Director, Operational Test and Evaluation
DRSN	Defense Red Switch Network
DSAWG	Defense IA Security Accreditation Working Group
DSN	Defense Switched Network
DSS	Defense Security Service
DTRA	Defense Threat Reduction Agency
DVS	DISN Video Services

E

ECV	enhanced compliance visit
EIEMA	Enterprise Information Environment Mission Area
EMSS	Enhanced Mobile Satellite System

F

FIPS	Federal Information Processing Standards
FSO	Field Security Operations

G

GIAP	GIG interconnection approval process
GIG	Global Information Grid

I

IA	information assurance
IAP	Information Assurance Panel
IASE	Information Assurance Support Environment
IATC	interim approval to connect
IATO	interim authorization to operate
IAW	in accordance with
IC	intelligence community
ICTO	interim certification to operate
IG	inspector general
IP	internet protocol
IS	information system
IT	information technology
ITP	Interoperability Test Panel

J

JP	Joint Publication
JVAP	Joint Vulnerability Assessment Process
JWICS	Joint Worldwide Intelligence Communication System

M

MA	mission area
MAC	mission assurance category
MCEB	Military Communication Electronics Board
MOA	memorandum of agreement
MOU	memorandum of understanding

N

NATO	North Atlantic Treaty Organization
NCES	Net-Centric Enterprise Services
NIPRNET	Non-Classified Internet Protocol Router Network
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	national security system
NSTISSI	National Security Telecommunications and Information Systems Security Instruction

O

OASD(NII)/ DOD CIO	Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer
OSD	Office of the Secretary of Defense

P

PAA	Principal Accrediting Authority
PDS	protected distribution system
POA&M	plan of action and milestones
POC	point of contact
PPS	ports, protocols, and services

S

SCI	sensitive compartmented information
SCQ	SIPRNET Compliance Questionnaire
SGS	SIPRNET GIAP System
SIAO	senior information assurance officer
SIPRNET	SECRET Internet Protocol Router Network
SNAP	systems/networks approval process
SSAA	system security authorization agreement
SSC	SIPRNET Support Center

STIGs	Security Technical Implementation Guides
SysAP	systems approval process
	T
TCO	Telecommunications Certification Office
TR	telecommunications request
TSO	telecommunications service order
	U
UCDMO	Unified Cross Domain Management Office
UCMJ	Uniform Code of Military Justice
UCP	Unified Command Plan
USC	United States Code
USG	United States Government
USSOCOM	U.S. Special Operations Command
USSTRATCOM	U.S. Strategic Command
	V
VPN	virtual private network
	W
WMA	Warfighting Mission Area

PART II -- DEFINITIONS

The following definitions are intended for use in this publication and the activities described herein. Except for definitions that include references to a source document, these terms have not been standardized for general DOD-wide use and inclusion in the DOD Dictionary of Military and Associated Terms (JP 1-02). In some cases, JP 1-02 (reference g) includes a general, DOD-wide definition for a term that has a specialized definition in this instruction.

accreditation. See CNSS Instruction No. 4009 (reference h).

alternate connections. Alternate connections include the following: (1) CC/S/A or field activity temporary connection of a DISN enclave to the Internet; and (2) CC/S/A or field activity connection to the Internet that is not connected to the unclassified DISN (e.g., a stand-alone system connected to the Internet by a commercial Internet Service Provider (ISP)). Both of these connections require an OSD waiver approval (CJCSI 6211.02C).

authentication. See CNSS Instruction No. 4009 (reference h).

backside connection. A connection behind the enclave infrastructure of a DOD organization (CJCSI 6211.02C).

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

centralized cross domain solution. A 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 6211.02).

certification. See CNSS Instruction No. 4009 (reference h).

common criteria. See DODI 8500.2 (reference k).

community risk. See DODD 8500.01E (reference i).

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

connectivity. Anything physically or logically connected to a customer's/user's enclave/network (CJCSI 6211.02C).

cross domain solution. See CNSS Instruction No. 4009 (reference h).

data. See JP 1-02 (reference g).

Defense Critical Infrastructure. See JP 1-02 (reference g).

Defense Critical Infrastructure Program (DCIP). See DODD 3020.40 (reference t).

Defense Information System Network (DISN). See JP 1-02 (reference g).

designated accrediting authority (DAA). See CNSS Instruction No. 4009 (reference h).

DISN user. An individual assigned to an organization having devices directly or indirectly connected to the DISN (CJCSI 6211.02C).

DOD information system. See DODD 8500.01E (reference i).

enclave. See CNSS Instruction No. 4009 (reference h).

end-to-end. The fusion of requisite components to deliver a defined capability. For the GIG, this implies components from the user access and display devices and sensors to the various levels of networking and processing, associated applications, and related transport and management services. For DISN services, end-to-end encompasses service user to service user (e.g., PC-to-PC, phone-to-phone). (See CJCSI 6211.02C.)

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 6211.02).

Global Information Grid (GIG). See JP 1-02 (reference g).

GIG Interconnection Approval Process. Electronic process to submit connection information and register a GIG connection (CJCSI 6211.02C).

information assurance. See JP 1-02 (reference g).

interconnection. Connection of information systems based on acceptance of risk and implementation of established controls (CJCSI 6211.02C).

Interoperability Test Panel (ITP). The mission of the Information Technology (IT) Systems and National Security Systems (NSS) Interoperability Policy and Test Panel (IPTP) is to promote, enhance, and maintain compatibility and interoperability of the following: systems with IT/NSS capabilities and systems that must operate within the defense IT/NSS environment to meet mission-essential needs of joint and combined operational commanders (MCEB Pub 1, reference nn).

Joint Vulnerability Assessment Process (JVAP). A process to assess cross domain solution configurations, operations, and administration using checklists and DISA and NSA/CSS procedures (CJCSI 6211.02C).

mission assurance category. See DODD 8500.01E (reference i).

mission-critical information system. See DODI 5000.2 (reference j).

mission-essential information system. See DODI 5000.2 (reference j).

non-DOD. All organizations and entities that are not components of the Department of Defense. This includes contractors and federally funded research and development centers; other USG federal departments and agencies; state, local, and tribal governments; foreign government organizations/entities (e.g., allies or coalition partners); non-government organizations; commercial companies and industry; academia (e.g., universities, colleges, or research and development centers); etc. (See CJCSI 6211.02C.)

plan of action and milestones (POA&M). A plan of action and milestones is required for any accreditation decision that requires corrective actions. The POA&M is a tool identifying tasks that need to be accomplished. It specifies resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. See DODI 8510.01 (reference d).

peering. Voluntary interconnection of administratively separate Internet networks for the purpose of exchanging traffic between the customers of each network (CJCSI 6211.02C).

protection profile. See CNSS Instruction No. 4009 (reference h).

risk decision authority criteria. Criteria for identifying an acceptable level of community risk for the connection approval authorities to employ in making connection decisions (CJCSI 6211.02C).

robustness. See DODD 8500.01E (reference i).

security domain. See DODD 8500.01E (reference i).

single level connection. Connection of enclaves of like security domains (CJCSI 6211.02C).

type accreditation. See NIST Special Publication 800-37 (reference oo).

type certification. See CNSS Instruction No. 4009 (reference h).