Department of Defense
INSTRUCTION

NUMBER 8540.01
May 8, 2015
Incorporating Change 1, August 28, 2017

DoD CIO

SUBJECT: Cross Domain (CD) Policy

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Establishes policy, assigns responsibilities, and identifies procedures for the interconnection of information systems (ISs) of different security domains using CD solutions (CDSs) in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (a)).

b. Aligns CD guidance for managing the information security risk and authorizing a CDS with the Risk Management Framework (RMF) in accordance with DoD Instruction (DoDI) 8510.01 (Reference (b)) and DoDI 8500.01 (Reference (c)).

c. Supersedes and cancels Assistant Secretary of Defense for Command, Control, Communications and Intelligence Memorandums (References (d) and (e)) and DoD Chief Information Officer (DoD CIO) Memorandum (Reference (f)).

2. APPLICABILITY

a. This instruction applies to:

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

(2) All DoD CDSs providing CD capabilities to, from, within, or between DoD ISs to include mission partner (e.g., international, interagency, State government, or defense contractors) ISs.

b. Nothing in this instruction alters or supersedes the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) as directed by Executive Order 12333 (Reference (g)), associated amendments, and other laws and regulations. DoD ISs with CDSs connected to Top Secret (TS)/SCI IS must comply with DNI policy and guidance.

c. Nothing contained in this instruction relieves, exempts, or authorizes any individual or office to take any action in violation of the section 793 of Title 18, United States Code (Reference (h)) or relieves them from possible criminal prosecution for inadvertent or deliberate transmission of government security information to unauthorized individuals or for failure to establish a bona fide "need to know."

3. POLICY. It is DoD policy that:

a. Information flow between different security domains will be authorized to meet essential mission requirements based on the results of an assessment of the mission requirements, implementation and compliance with security requirements, and the assessment of associated risks in accordance with References (b), (c), and this instruction.

b. Operational need for each CD information flow must be balanced with the risk to all affected ISs and the DoD. The level of risk will be assessed and measured by the DoD risk executive as to whether the risk is acceptable in accordance with References (b), (c), and this instruction.

c. A DoD CD capability requirement must be met by a CDS listed on the Unified Cross Domain Services Management Office (UCDSMO)-managed CDS baseline list. When a CDS baseline list CDS cannot meet the CD capability requirements for the mission, a modified CDS baseline list CDS or new technology will be used in accordance with the selection decision based on analysis of CD alternatives in the procedures of this instruction.

d. New CD technologies proposed to meet modernization or new capability requirements will be assessed by the security control assessor (SCA) for functionality and security requirements.

e. DoD will employ existing enterprise CD service provider's (ECDSP's) enterprise CD service or enterprise-hosted CDS when their use satisfies the CD mission requirements of DoD Components. Leveraging another operational CDS, deployment of a CDS baseline list point to point CDS or development of a new CD technology will be considered as alternative solutions only when an enterprise solution cannot meet the CD capability requirements.

f. DoD ISs with a CDS as a component (e.g., an enclave) or a CDS as a separate IS (e.g., an enterprise CD service) must be authorized to operate by the authorizing official (AO) in accordance with Reference (c) and this instruction.

g. The DoD level risk decision on use of a CDS to access or transfer information between different interconnected security domains must be made by the designated DoD risk executive as a CDS authorization (CDSA) in accordance with this instruction.

h. All CDSs will be deployed and managed on the controlling domain of the CD interconnection. A CDS will be separately authorized for operation as an IS or as a CDS component within the IS in which it is deployed.

i. A CDS on the UCDSMO-managed CDS sunset list or a legacy CDS not on the CDS baseline list must be replaced within a period of time agreed to by the AO and the DoD risk executive. A letter of exception is required to operate a CDS not on the CDS baseline list (see guidance in the procedures of this instruction).

j. A CDS found operating without approval or out of compliance with its approved security configuration requires immediate DoD chain of command notification to determine whether to disconnect or stop use of the CDS (see guidance in the procedures of this instruction).

k. Information transferred between different security domains must be correctly marked, protected, and disseminated in accordance with DoD Manual 5200.01, Volumes 1 through 4 (Reference (i)).

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosures 3, 4, and 5.

6. RELEASABILITY. **Cleared for public release**. This instruction is available on the Directives Division Website at http://www.esd.whs.mil/DD/.

7. SUMMARY OF CHANGE 1. The changes made to this issuance are administrative and update releasability and references for accuracy.

8. EFFECTIVE DATE. This instruction is effective May 8, 2015.

Terry A. Halvorsen
DoD Chief Information Officer

Enclosures
1. References
2. Responsibilities
3. CD Activities

TABLE OF CONTENTS

TABLES

FIGURES

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014
(b) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended
(c) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(d) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, "Secret and Below Interoperability (SABI) Reaffirmation," May 11, 1998 (hereby cancelled)
(e) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, "Secret and Below Interoperability (SABI)," March 20, 1997 (hereby cancelled)[1]
(f) DoD Chief Information Officer (CIO) Memorandum, "Cross Domain Support Element (CDSE) Responsibilities," October 11, 2011 (hereby cancelled)
(g) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(h) Section 793 of Title 18, United States Code
(i) DoD Manual 5200.01, "DoD Information Security Program," Date varies by volume
(j) Joint DoD/IC Memorandum, "Establishment of the Unified Cross Domain Services Management Office (UCDSMO) as the Cross Domain Requirements and Engineering Service Manager," March 26, 2014[2]
(k) DoD Chief Information Officer and Intelligence Community Chief Information Officer Charter, "Unified Cross Domain Management Office Charter," March 21, 2007[2]
(l) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016
(m) Deputy Secretary of Defense Memorandum, "Joint Information Environment Implementation," May 6, 2013
(n) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
(o) Title 15, Code of Federal Regulations, (also known as the "Export Administration Regulations")
(p) Title 22, Code of Federal Regulations, (also known as the "International Traffic in Arms Regulations")
(q) DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014
(r) Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Chief Information Officer (CIO) Executive Board Charter," February 12, 2012
(s) Defense Information Systems Agency Guide, "Connection Process Guide," current version[3]

[1]https://inteldocs.intelink.gov/inteldocs/page/repository#filter=path%7CUser%20Folders/r/ra/rakosky/joseph.m.rakosky1
[2]UCDSMO and UCDMO memos and charter: https://intelshare.intelink.gov/sites/ucdsmo//Documents/Forms/AllItems.aspx

(t) Defense Information Systems Agency, "Cross Domain Technical Advisory Board (CDTAB) Charter," April 18, 2007[4]
(u) National Institute of Standards and Technology Special Publication 800-30, "Guide for Conducting Risk Assessments," September 2012
(v) National Institute of Standards and Technology Special Publication 800-39, Revision 1, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011
(w) DoD Instruction 4000.19, "Support Agreements," April 25, 2013
(x) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015, as amended
(y) Committee on National Security Systems Instruction No. 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014[5]
(z) DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016
(aa) DoD 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, as amended
(ab) DoD Chief Information Officer, "DoD Architecture Framework," current version[6]
(ac) Committee on National Security Systems Policy No. 26, "National Policy on Reducing Risk of Removable Media for National Security Systems," May, 2013
(ad) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(ae) Department of Defense, "Unified Command Plan," April 6, 2011, as amended
(af) DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012, as amended
(ag) DoD CIO and Assistant Director of National Intelligence and Intelligence Community CIO Memorandum, "Use of Unified Cross Domain Management Office (UCDMO) Baseline Cross Domain Solutions (CDSs)," December 1, 2011
(ah) Committee on National Security Systems Policy No. 8, "Policy Governing the Release and Transfer of U.S. Government Cryptologic National Security Systems Technical Security Material, Information, and Techniques to Foreign Governments and International Organizations," August, 2012
(ai) Chairman of the Joint Chiefs of Staff Instruction 6510.06B, "Communication Security Releases to Foreign Nations," November 8, 2013
(aj) National Institute of Standards and Technology Special Publication 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010
(ak) National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013

---

[3] Connection Process Guide: http://www.disa.mil/Services/Network-Services/Enterprise-Connections/Connection-Process-Guide
[4] CDTAB Charter: https://inteldocs.intelink.gov/inteldocs/page/document-details?nodeRef=workspace://SpacesStore/5054bc22-1ec1-46f7-9f65-4b4dc889d19e
[5] CNSS publications: https://www.cnss.gov/CNSS/issuances/Instructions.cfm (Click on CNSSI No. 1253, select "save target as," and "save" to download.) or http://www.iad.nsa.smil.mil/resources/library/cnss_section/cnss_instructions.cfm (Double click on CNSSI-1253.)
[6] DoD Architecture Framework: http://dodcio.defense.gov/dodaf20.aspx

(al) National Institute of Standards and Technology Special Publication 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," September 2011
(am) Unified Cross Domain Management Office, "800-53 Based Cross Domain Solutions (CDS) Risk Analysis Using the 800-53 CDS Overlay," Version 1.0a, April 24, 2014[7]
(an) DoD Instruction 2030.08, "Implementation of Trade Security Controls (TSC) for Transfers of DoD Personal Property to Parties Outside DoD Control," February 19, 2015
(ao) DoD Directive 5100.03, "Support of the Headquarters of Combatant and Subordinate Unified Commands," February 9, 2011
(ap) DoD Instruction 8320.02, "Sharing Data, Information, and Technology (IT) Services in the Department of Defense," August 5, 2013
(aq) Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," April 6, 2015

[7] UCDSMO Website at: https://intelshare.intelink.sgov.gov/sites/ucdsmo/pages/cdstestreq.aspx (Double click on CDS Risk Control Guide.)

ENCLOSURE 2

RESPONSIBILITIES

1. DOD CIO. The DoD CIO:

a. Oversees and provides direction to UCDSMO for implementation of this instruction.

b. Serves as co-chair of the oversight panel that directs, oversees, and approves UCDSMO activities in accordance with Joint DoD and Intelligence Community (IC) UCDSMO Memorandum (Reference (j)) and the UCDSMO Charter (Reference (k)).

c. Provides strategic management, direction, and oversight to plan, program, develop, and implement enterprise CD services into the DoD Enterprise Architecture in accordance with DoDD 8000.01 (Reference (l)) and the evolving Joint Information Environment reference architectures (e.g., a Single Security and Core Data Center) in accordance with Deputy Secretary of Defense Memorandum (Reference (m)).

d. Collaborates with the Under Secretary of Defense for Intelligence (USD(I)) on strategy for DoD enterprise CD services and a CDS risk governance reciprocity.

e. Designates the DoD Information Security Risk Management Committee (ISRMC) as the DoD risk executive for authorizing the information flow between different security domains in accordance with Reference (c).

f. Establishes, via a UCDSMO-led effort, a process to ensure proper release of a CDS or CDS information to foreign mission partners in accordance with DoDD 5230.11 (Reference (n)), chapter VII, subchapter C of Title 15, Code of Federal Regulations (also known as the "Export Administration Regulations") (Reference (o)), part 121 Category XIII of Title 22, Code of Federal Regulations (also known as the "International Traffic in Arms Regulations") (Reference (p)), and DoDI 2040.02 (Reference (q)), in coordination with the Under Secretary of Defense for Policy (USD(P)), the Under Secretary of Defense for Acquisition, Technology, and Logistics, USD(I), the Director, National Security Agency (NSA)/Chief, Central Security Service (DIRNSA/CHCSS), and the CJCS.

g. Resolve CDS, CD enterprise services, and enterprise-hosted CDS priorities, implementation, and information resources issues based on DoD CIO Executive Board recommendations in accordance with Deputy Secretary of Defense Memorandum (Reference (r)).

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). In addition to the responsibilities in section 8 of this enclosure, and under the authority, direction, and control of the DoD CIO, the Director, DISA:

a. Establishes and documents DISA's process for providing enterprise CD services or enterprise-hosted CDSs.

(1) Provides the conditions and criteria under which a DoD Component CD capability requirement can be satisfied by a DISA enterprise CD service or enterprise-hosted CDSs.

(2) Provides the conditions, criteria, and cost model for providing DISA enterprise CD services and enterprise-hosted CDSs to DoD Components and authorized mission partners.

b. Issues and implements CDSAs approved by the DoD ISRMC or as delegated to the Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG) in coordination with the IS owner to allow a CDS to access or transfer information between different interconnected security domains.

c. Maintains the Defense Information Systems Network (DISN) Connection Process Guide (Reference (s)) outlining the business processes for connecting an IS using a DoD Component CDS in accordance with this instruction. The process guide CD appendix and associated updates will be reviewed by the DSAWG.

d. Manages the designated CD repository (i.e., the SECRET Internet Protocol Router Network Global Information Grid Interconnection Approval Process System (SGS)), which maintains an inventory of all CDSs in operation or in the assessment and approval process. Inventories of CDSs in use on SCI information networks will be maintained in accordance with DNI guidance.

e. Develops the security architecture to protect DISA CD enterprise services and enterprise-hosted CDS sites.

f. Provides information on the ability of interconnected DoD information networks (DODIN) to restrict attack avenues or methods to support the CD Technical Advisory Board's (CDTAB's) recommendation for the CDS risk assessment and decision process.

g. Conducts and provides security reviews of CDSs and their operational environments (e.g., a DISN connected enclave) to support the DSAWG or DoD ISRMC CDSA decisions, as required.

h. Develops and provides RMF and DISN connection products and training materials on the IA Support Environment Website at http://iase.disa.mil/Pages/index.aspx or http//iase.disa.smil.mil/index2.html to support DoD Component CDS activities.

i. Establishes and maintains the CDTAB as an advisory board to the DSAWG and provides chair and secretariat support as specified in the CDTAB Charter (Reference (t)).

3. DIRECTOR, UCDSMO. Under the authority, direction, and control of the DoD CIO as co-chair of the oversight panel in accordance with Reference (k), the Director, UCDSMO:

a. Provides centralized management of DoD CD activities, ensuring a common DoD Component approach to implement this instruction.

b. Serves as principal CD advisor to the DoD CIO and provides status of DoD Components' progress in implementing this instruction.

c. Initiates and charters working groups with DoD Component representation to address CD issues (e.g., training, assessments, or CD capability requirements), as needed.

d. Supports DoD information sharing objectives by emphasizing expedited delivery to the field of CD capabilities that meet all applicable security requirements.

e. Provides quarterly status of all plans of action and milestones (POA&Ms) for legacy CDSs not on the CDS baseline list, CDSs operating beyond the CDS sunset list specified time, and CDS not on the CDS baseline list operating with a letter of exception. The POA&M template is available in the reference library at https://rmfks.osd.mil/rmf/General/SecAuthPackage/Pages/POAM.aspx.

f. Provides CD subject matter expertise, managerial oversight, technical support, and recommendations to DoD bodies and organizations for risk-based decisions, strategic and developmental planning, investments, and CD knowledge management.

g. Provides recommendations to the appropriate DoD entities regarding CD issues common to the DoD and IC and initiates ad hoc joint meetings as required.

h. Supports the DoD CIO in the development and alignment of DoD and IC CDS policies.

i. Establishes and provides CD criteria and standards.

(1) Establishes a CD security control overlay for use by DoD in accordance with Reference (b).

(2) Provides standardized guidance in accordance with Reference (b) on CDS implementation and assessments. This guidance must be consistent with National Institute of Standards and Technology (NIST) Special Publication 800-30 (Reference (u)) and NIST Special Publication 800-39 (Reference (v)).

(3) Provides standardized security assessment objectives and common test procedures for the CDS security control overlay.

(4) Develops and maintains a risk model in accordance with References (u) and (v) to support the DoD ISRMC and DSAWG risk decisions to authorize CDSs to access or transfer information between different security domains.

(5) Establishes and oversees the criteria that must be met by ECDSPs when providing advertised services and their compliance with CDS security requirements, including when operating in the deployed environment.

j. Establishes the criteria to certify DoD laboratories for verification and validation of the CD technology's functionality and compliance with security requirements and conduct penetration testing.

k. Advocates for the standardization of CDSs to minimize redundant or duplicative development or acquisition.

l. Identifies common DoD and IC CD capability requirements and problem sets in coordination with those DoD and IC components and elements.

m. Supports CD personnel training.

(1) Consolidates CD personnel training requirements received from DoD Components.

(2) Maintains a catalog of courses available to CD personnel from the NSA, other DoD Components, and non-DoD organizations.

(3) Facilitates the use of available training courses by CD personnel and organizations.

n. Develops and maintains, with assistance from NSA and other DoD Components, a CD security control assessment process guide and security assessment report (SAR) template.

o. Manages CD capabilities portfolio.

(1) Develops and maintains a CD capabilities portfolio, to include a CDS baseline list of verified and validated CDSs, as well as a listing of end of life products on a CDS sunset list, enterprise CD services, and other CD technologies at https://intelshare.intelink.sgov.gov/sites/ucdsmo/default1.aspx.

(2) Manages a process for sponsorship of new enterprise CD services and CDSs to be placed on the CDS baseline list following a CD technology's verification and validation of functionality and compliance with security requirements.

(3) Manages a process for identifying enterprise CD services and CDSs to be placed on the CDS sunset list.

(4) Sends notification of changes to the CDS baseline list or CDS sunset lists to CD support elements (CDSEs).

p. Develops and maintains a CD roadmap that builds on the UCDSMO CD capabilities portfolio, validated CD capability requirements, capability gaps, and emerging CD technologies to establish necessary CDSs for enterprise CD services.

(1) Develops and conducts an outreach strategy to encourage development of innovative commercial CD technologies and enterprise CD services that satisfy DoD and IC common capability gaps, problem sets, and projected requirements.

(2) Coordinates research and development efforts for CD technologies, to include the development and implementation of enterprise CD services and provides information on CD research and development efforts to the Assistant Secretary of Defense for Research and Engineering as requested.

(3) Releases requests for information to vendors at least semi-annually to identify potential vendor solutions for identified capability gaps and associated capability requirements.

(4) Facilitates communications between commercial entities with new CD technologies and DoD Components that have capability gaps that could be met by vendor solutions.

q. Maintains a list of DoD and IC UCDSMO certified laboratories based on NSA certification recommendation that are available to conduct fee-for-service CD technology security control assessments and penetration testing in support of DoD Component requirements, and makes the list available through the UCDSMO website.

r. Schedules and oversees security control assessments accomplished by DoD laboratories for CD technologies, including new technologies, new CDS versions, and technologies determined by the CDTAB to require a new Target of Evaluation (TOE). Security control assessments will be conducted in accordance with DoD Components priorities. Any conflicts in scheduling or resources availability between DoD Components requirements will be brought to the DoD CIO for resolution.

s. UCDSMO maintains for information purposes a control list in support of Reference (p) and a frequently asked questions file about the release and export of CDSs at UCDSMO site at https://intelshare.intelink.sgov.gov/sites/ucdsmo/default1.aspx by accessing the Cross Domain Shared Docs link and then accessing the export and release folder.

t. Appoints representatives to the CDTAB as specified in Reference (t).

4. USD(P). The USD(P):

a. Coordinates with the DoD CIO and CJCS to establish a process for release of CDSs to foreign mission partners.

b. Provides advice to the DoD CIO and other DoD Components, as required, on foreign disclosure and export of CDSs and CD technologies.

5. USD (I). The USD(I):

a. Collaborates with the DoD CIO and CJCS on a strategy to implement enterprise CD services.

b. Coordinates with DoD CIO to establish a process for release of CDSs to foreign mission partners.

c. Provides interpretations of Information Security Program requirements as provided in Reference (i).

6. DIRNSA/CHCSS. In addition to the responsibilities in section 8 of this enclosure, and under the authority, direction, and control of the USD(I), the DIRNSA/CHCSS:

a. Advises the DoD CIO, DoD Component heads, and the Director, UCDSMO on the security features, practices and procedures, and architecture required for DoD CDSs to enforce security policy.

(1) Develops and maintains inspection, sanitization, and data transfer guidance documents for the file formats and protocols used by the DoD.

(2) Develops and maintains filter configuration standards.

b. Supports assessment and penetration testing of CD technologies.

(1) Assists the UCDSMO in developing standards to certify DoD laboratories to conduct security control assessments of CD technologies and penetration testing in order to verify and validate functionality and compliance with security requirements.

(2) Conducts certification assessments of DoD laboratories in accordance with UCDSMO-provided criteria and provides certification recommendation to the UCDSMO. NSA will provide a recommendation to revoke certification if DoD standards are not being met.

(3) Provides training to DoD Component personnel based on training requirements jointly identified by the DoD Components, the IC, DoD mission partners, and the UCDSMO (e.g., the risk assessment model or CD technology assessment).

(4) Conducts penetration testing or oversees the penetration testing by other organizations of new CD technologies or new CD technology versions, as required.

c. Conducts or oversees other DoD Component Red Team operations to emulate a potential adversary's attack or exploitation capabilities against DoD ECDSP sites or DoD Component sites hosting operational CDSs, as directed by Commander, U.S. Strategic Command (CDRUSSTRATCOM).

d. Assists the UCDSMO in developing a security control assessment guide and SAR template.

e. Evaluates DoD enterprise-wide CD vulnerabilities and provides recommendations on procedures and architecture to mitigate risk to CDRUSSTRATCOM and DoD CIO, as required.

7. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). In addition to the responsibilities in section 8 of this enclosure, and under the authority, direction, and control of the USD(I), the Director, DIA:

a. Provides enterprise CD services or enterprise-hosted CDS for Joint Worldwide Intelligence Communications System (JWICS) customers in coordination with collateral network service providers, as required.

b. Issues authorization for SCI enterprise CD services and enterprise-hosted CDSs deployed on JWICS in accordance with DNI guidance. If a CDS is physically deployed on a collateral DoD IS, then an assessment and approval is conducted in accordance with Enclosure 4 of this instruction for deployment.

c. Provides threat information for the transfer of information to or from foreign mission partners or foreign mission partner ISs, in support of the CD risk assessment and evaluation methodology.

8. DOD COMPONENT HEADS. The DoD Component heads:

a. Establish a CDSE to carry out CDSE responsibilities outlined in Enclosure 5 of this instruction for DoD Component current or planned CDSs.

(1) A DoD Component may execute a support agreement (e.g., a memorandum of agreement (MOA)) in accordance with DoDI 4000.19 (Reference (w)) with another DoD Component's CDSE to conduct specified CDSE duties and responsibilities on their behalf.

(2) A DoD Component CDSE will act as an oversight and coordination office for another DoD Component's CDSE when it is performing specified CDSE duties and responsibilities in accordance with a support agreement (e.g., an MOA).

b. Appoint representatives from the DoD Component to the CDTAB as specified in Reference (t).

c. Direct DoD Component organizations to coordinate with their servicing CDSE before contracting or obligating their organization to the acquisition of CDSs, CD technologies, or services. This includes coordinating with an external CDSE's providing CD support (e.g., a Combatant Command coordinating with Service CDSE providing CD support).

(1) Appoint CDSE individuals authorized to coordinate CD activities and manage DoD Component CD requirements in the designated centralized repository. Provide list of authorized individuals to UCDSMO and DoD ECDSPs.

(2) Select CDSs and new CD technologies following a selection decision in accordance with Pre-RMF Step 0 of Table 1 in Enclosure 4 this instruction.

(3) Ensure new CDS-related concepts and initiatives are coordinated with the UCDSMO and added to the CD capabilities portfolio.

d. Use the DoD CD process specified in Enclosure 4 to identify CD capability requirements and implement CDSs in support of DoD Component missions.

e. Use ECDSP's enterprise CD service or enterprise-hosted CDS when the solution satisfies a DoD Component's CD capability requirements. A list of operational and future services and the ECDSPs can be found at https://intelshare.intelink.sgov.gov/sites/ucdsmo/cap-port-2/CDServices/SitePages/Home.aspx.

f. If an enterprise CD service or enterprise-hosted CDS does not meet the CD capability requirements for the mission (e.g., exercises; research, development, test, and evaluation (RDT&E); modeling and simulation (M&S); tactical level unit operations; or sensor-to-weapon platform data transfer), then an exception for using a point to point, baseline list CDS, or new product may be required. When this case occurs, provide evaluation results during the CDS selection process establishing that the CD capability requirement cannot be satisfied by an enterprise capability.

(1) Develop a POA&M to transition a DoD Component CDS to an enterprise service or enterprise-hosted CDS as directed by the DoD ISRMC and DoD CIO Executive Board.

(2) Identify resource issues and courses of action for transition of DoD Component CDSs to enterprise service or enterprise-hosted CDS to the DoD CIO Executive Board, as required.

g. Document the CDS interconnection within both the IS's RMF assessment and authorization documentation in accordance with Reference (b) and the designated DoD repository in accordance with Reference (s).

h. Ensure the use of a CDS on the CDS sunset list, or a legacy CDS not on the CDS baseline list, is documented, reviewed by the DSAWG, and authorized either by the DoD ISRMC in accordance with section 5 of Enclosure 3 of this instruction.

(1) Upload to the designated centralized repository a POA&M detailing the plan to replace a CDS not on the CDS baseline list or a CDS operating beyond the CDS sunset list specified time with a baseline list CDS and notify the DSAWG and UCDSMO.

(2) Manage a POA&M to migrate to a CDS baseline list CDS and provide POA&M updates to reflect changes in migration status to UCDSMO and DoD CIO.

(3) When a CDS baseline list CDS cannot be used due to unique CD capability requirements, upload the DoD Component letter of exception with information required by section 5 of Enclosure 3 to the designated centralized repository and notify the DSAWG.

i. Inspect DoD Component ISs with DoD Component CDSs via a DoD Component directed cybersecurity inspection or approved U.S. Strategic Command (USSTRATCOM) directed cybersecurity inspection at least once during the first year of operation and thereafter once every 3 years to validate IS owner security self-assessment processes.

j. Oversee and monitor the life cycle management of DoD Component CDSs and CDS security configurations.

(1) Provide for life cycle management (i.e., pre-acquisition, acquisition, and sustainment) and operation of DoD Component enterprise CD services and operational CDSs under their control in accordance with DoDI 5000.02 (Reference (x)).

(2) Implement Committee on National Security Systems Instruction (CNSSI) No. 1253 (Reference (y)) required and CDSA specified security controls to enable the defense of the CDS and its operational environment in accordance with References (b), (c), and DoDI 8530.01 (Reference (z)).

(3) Designate an office or organization to track, maintain, and provide data on CD technology RDT&E, supporting laboratories, and deployed CDSs including system development life cycle (SDLC) phase.

(4) Ensure CDSs are designated as controlled inventory items and the associated CDS components and equipment are included in the Defense Property Accountability System for the purpose of accounting for their existence, location, custody, accountability, and disposition.

(5) Oversee DoD Component execution of funding for CDSs, including existing programs and new CDS-related concepts and initiatives, in accordance with Reference (x).

(6) Review, validate, and prioritize CD capability requirements and investments.

(7) Ensure IS owners manage and maintain the operation and security throughout the CDS's SDLC in accordance with References (b) and (c).

k. Maintain status on all CDSs, including those in operation, in the RMF process, or under research or development, in the designated centralized repository. If information is not in the designated centralized repository, the DoD Components will provide this information annually to the UCDSMO or as required by the DoD CIO.

l. Ensure both technical and managerial personnel involved in CDS management, administration, operation, maintenance, and assessment are trained and certified in accordance with DoD 8570.01-M (Reference (aa)).

m. Provide UCDSMO with CD personnel training requirements and associated DoD Component CD courses open to other organizations on a space available or fee-for-service basis.

n. Ensure DoD Component security control assessments and vulnerability assessments are conducted by security assessor personnel in accordance with published UCDSMO SCA guidance and baseline and CD overlay security controls for CDSs and deployed environments. Approved security control baselines and overlays are found in Reference (y).

o. Ensure DoD Component organizations with CDSs deployed within their IS authorization boundaries effectively implement required security controls for both the environment and deployed CDSs in accordance with References (b) and (y).

p. Notify Combatant Commands of any DoD Component CDS deployed and operating in a Combatant Command's area of responsibility.

q. Defend ISs and deployed CDSs, including sensors and boundary protection measures, as required by implemented security controls, AO, USSTRATCOM, and applicable DISA security technical implementation guides.

r. Ensure organizations conduct security self-assessments periodically to validate that the approved configurations of the CDS have not changed. Self-assessments must be submitted to the respective CDSEs, approved by the organization AO or designated representative, and uploaded to the designated centralized repository in accordance with Reference (s) and this instruction.

s. Update initially and as required the designated central repository with contact information, including e-mail, address, and phones numbers, for enclave and CDS points of contact (e.g., AO, IS owner, CDSE, information systems security manager (ISSM), information systems security officer (ISSO), information systems security engineer (ISSE), technical representative, administrative representative), and the required security and architecture documentation as specified in Reference (b) and the DoD Architecture Framework (Reference (ab)).

t. Follow guidance provided by DoD CIO before release of a CDS to a foreign mission partner as specified in section 9 of Enclosure 3 of this instruction.

u. Oversee DoD Component-managed ISs use of CDSs.

(1) Require the issuance of a DoD ISMRC or DSAWG CDSA before allowing a CDS to access or transfer information between different interconnected security domains. A CDSA is required for use of a CDS.

(2) Provide DoD Component guidance on the CDS authorization process for DoD Component-managed ISs that is compliant with the RMF procedures specified in Enclosure 4, consistent with Reference (s), and DoD Component issuance(s), as required.

v. Direct the individuals responsible for managing a CDS to report security incidents to the local or site information security manager in accordance with Volume 3 of Reference (i) and the ISSM or ISSO in accordance with Reference (c). Inform the CDSE. In accordance with Volume 3 of Reference (i), the information security manager has the overall responsibility for resolution of the incident.

w. Establish and document DoD Component program for the use of removable media to conduct CD data transfers to include policy, acquisition, operations, and disposal. This program will be updated in accordance with Committee on National Security Systems Policy (CNSSP) No. 26 (Reference (ac)), other DoD and USSTRATCOM orders, and other issuances, as required.

x. Ensure a reliable human review (RHR) process and procedures are implemented for opening and reviewing digital objects (e.g., files or images) to ensure that the digital object (e.g., data) may be transferred across a CDS in those cases where RHR is required due to the limitations of the specific CDS.

(1) Provide training to information originators on the RHR process and procedures requiring that information transferred must be in accordance with References (i), (n) and (q) for the designation, marking, protection, and dissemination of controlled unclassified information and classified information.

(2) Use CDS sanitization tools as directed by DoD or the DoD Component.

(3) Enforce a visual RHR as required using procedures and standards for RHR defined in DoD Component guidance, United States Cyber Command tasking orders, and specific CDS operating guidance.

(4) Ensure adequate audit capability for attribution back to the originator.

y. Report unauthorized or non-compliant CDSs through the appropriate reporting chain as an actual or potential compromise of classified information or as an actual or potential unauthorized disclosure of controlled unclassified information, including breach of personally identifiable information (PII), in accordance with Volumes 3 and 4 of Reference (i) and DoD 5400.11-R (Reference (ad), as appropriate for the sensitivity of the information processed.

9. CJCS. In addition to the responsibilities in section 8 of this enclosure, the CJCS will facilitate and advocate Combatant Command CD capability and operational requirements at the CDTAB, DSAWG, DoD ISRMC, and other Joint Staff operational requirements forums, as required.

10. CDRUSSTRATCOM. In addition to the responsibilities in section 8 of this enclosure, the CDRUSSTRATCOM:

a. Provides the DSAWG and DoD ISRMC with relevant risk data of a DoD Component's operational environment to support CDS selection or CDSA during the RMF process. Relevant data includes evidence such as past cybersecurity inspection results, assessments, and compliance with directives and orders (e.g., vulnerability alerts or tasking orders) to determine the DoD Component's ability to operate, manage, and defend the DoD Component's CDS implementation.

b. Directs the disconnection or removal of CDSs or CD technologies that are determined to pose an operational risk to DoD information networks or as determined by the DoD ISRMC in coordination with operational chain of command. These CDS risks would be those determined to be impacting the ability to execute DoD missions or cause exceptionally grave or serious damage to national security through the compromise of classified information.

c. Oversees CD capabilities regarding the Unified Command Plan (Reference (ae)) assigned supporting space, missile defense, and nuclear command and control missions.

d. Validates vulnerability self-assessment processes during cybersecurity inspections.

ENCLOSURE 3

CD ACTIVITIES

1. CD CAPABILITIES PORTFOLIO. The UCDSMO has created the CD capabilities portfolio to meet DoD and IC problem sets and projected CD capability requirements, available through the UCDSMO website "Capabilities Portfolio" tab at: http://intelshare.intelink.sgov.gov/sites/ucdsmo/default1.aspx, to provide a complete listing of CDSs and CD technologies.

a. Enterprise CD Services List. The CD enterprise services list identifies CD services available for delivery by the DoD and IC.

b. CDS Baseline List. The CDS baseline list is a starting point for leveraging identified and validated CDSs that support operational needs within the DoD and IC and are available for deployment. For more information on the CDS baseline list, refer to the UCDSMO Capabilities Portfolio tab at https://intelshare.intelink.sgov.gov/sites/ucdsmo/cap-port-2/default.aspx.

(1) Each solution on the CDS baseline list has successfully completed a security control assessment conducted by a SCA, who has provided a statement that comprehensive review, analysis, and testing were performed and confirms (i.e., verifies) that the requirements are correctly defined and that the CD technology correctly implements required functionality and security requirements in a non-operational environment using UCDSMO-published CDS test standards. Types of CDSs include CDSs providing access, data transfer, and multi-level solutions to meet CD requirements.

(2) The submitter confirms to the UCDSMO that the CDS has life cycle support and sustainment.

(3) The AO will direct an onsite operational security assessment (i.e., site security control assessment) of CDSs on the CDS baseline list before a DSAWG or DoD ISRMC CDSA granting authorization to transfer information between interconnected security domains is implemented.

c. CDS Sunset List. CDSs are placed on the CDS sunset list because:

(1) Components of the solution have reached end of life and are no longer supported;

(2) They were superseded by a newer version or significant security relevant configuration modification;

(3) They no longer satisfy a needed capability; or

(4) The solution has been deemed to have serious security problems and the DoD ISRMC or designated representative has agreed that immediate removal or replacement is necessary.

d. CD Technology Lists. The CD technology lists identify existing, emerging, and enabling CD-related technologies and supporting activities. Technologies identified may be in various stages of development and deployment, and may not have undergone security control assessment.

2. ACQUISITION AND USE OF A CDS

a. Acquisition. CDSs will be acquired in accordance with Reference (x).

b. Trusted CDSs. CDSs will be protected throughout the entire system lifecycle in accordance with DoDI 5200.44 (Reference (af)) to protect against vulnerabilities in system design, sabotage, or subversion of a system's critical functions or components by foreign intelligence, terrorists, or other hostile elements.

c. CDS Baseline List

(1) Assists the DoD Component CDSE and DoD Component customers in selecting an appropriate CDS.

(2) Identifies vendors that can provide a CD technology or CDS for the DoD Component CDSE.

d. New CD Technology Life Cycle Sustainment and RMF. Each item on the CDS baseline list will have a program management support structure to ensure the provision for life cycle and sustainment of CD technologies and services in accordance with Reference (b) and (x).

(1) Mission or business ownership, CD technology development and integration, and the CDS security management oversight responsibilities must comply with the policy and procedures of References (b), (c), and (x) for all CD technology acquisitions, CDSAs, and operations within the deployed environment (e.g., an enclave).

(2) New CD technologies will be added to the CDS baseline list in accordance with References (b) and (c) and this instruction.

(3) The CD capabilities portfolio is the entry point for identifying new commercial CD technologies to meet DoD and IC common problem sets and projected CD capability requirements.

(4) A DoD Component wishing to sponsor a new CD technology for placement on the CDS baseline list must contact their CDSE for assistance and guidance to ensure any new CD related technology development activities are coordinated with the UCDSMO before initiation.

e. Life Cycle Support and Sustainment. The DoD Component CDSE must provide the UCDSMO a written assertion from the CDS Program Management Office that funding is available to provide life-cycle support and sustainment for a CDS to be added to the CDS baseline list. In the case of commercial off-the-shelf hardware and software, the developer must either provide a statement that required support and sustainment are included in the acquisition costs or provide a cost schedule for service or maintenance. The DoD Component CDS Program Management Office must declare that, at a minimum, the CD technologies and service life cycle supports:

(1) Availability. The CDS is available and will be supported for both DoD and IC customers in accordance with DoD CIO, Assistant DNI, and IC Chief Information Officer (CIO) Memorandum (Reference (ag)). A CDS selected and approved for use will be supported in accordance with the support agreement (e.g., a MOA) between the CDS owner and customer.

(2) Configuration Management. The CDS security relevant configuration will be documented and managed throughout the development cycle and during operational use for the life of the CD technology.

(3) Distribution Control. Distribution control will be maintained for the life of the CDS.

(4) Product Support. To the greatest extent possible, the Program Management Office or developer must provide assurance that support for the hardware platform, operating system, application, and appropriate data rights will be available for the life of the product. This assurance should include a plan for POA&M development in the case of unforeseen software or hardware obsolescence.

(5) Software Maintenance. An outline or plan for how software updates, including patching, bug fixes, upgrades, and enhancements, will be provided.

(6) User Support. An outline or plan for how help desk, user documentation, administrative documentation, and training will be supplied.

f. Additional CDS Employment Guidance. The following additional guidance is provided on employing a CDS.

(1) Chaining. The use of direct or relayed connections from a higher accredited domain to a series of lower accredited domains **after passing through an isolated device** that implements the enforcement of all applicable approved policy decisions for each domain transfer is permitted.

(2) Cascading. The downward flow of information through a range of security levels greater than the accreditation range of a system, network, or component **without passing through an isolated device** that implements the enforcement of all applicable approved policy decisions for each domain transfer is prohibited.

(3) Diversity. To reduce the risk when accessing or transferring information between a range of security levels, the use of different CDSs should be considered if they are available and meet the mission requirements (e.g., using one CDS between unclassified to secret domains and using a second different CDS between secret to TS SCI security domains).

3. ENTERPRISE SERVICES

a. A DoD Component must use or transition to an enterprise service if the CD requirement can be met under the existing enterprise service CDSA criteria (e.g., classification level, data types, filters, or flows) in accordance with DoD ISRMC guidance.

b. Existing CD requirements not using an enterprise solution will be evaluated for transition to an enterprise service when:

(1) The existing CDS undergoes a security posture review due to the DoD ISRMC periodic CDSA review requirements, a CDSA revalidation, or a review required as a result of the downgrade in the CDS's security posture.

(2) The CDS is placed on the sunset list due to reaching end of life or the CDS requires a review of existing CDSA due to a major upgrade.

c. The addition of a new customer to an enterprise service does not require any further approval if there are no changes required to the enterprise service CDSA or the configuration of the CDS.

d. The DoD Component CDSE will coordinate with the ECDSP for enterprise service or enterprise-hosted CDS support.

e. Following the CDS selection the DSAWG will review any required changes to the enterprise service CDSA or the configuration of the CDS. The CDTAB and DSAWG will determine what actions are required to implement required changes in coordination with the ECDSP, the DoD Component, and the CDTAB in accordance with RMF Step 6, Table 8 of Enclosure 4 of this instruction.

f. The DoD Component through their CDSE will complete a service agreement with the ECDSP. The DoD Component and ECDSP documentation will be updated to reflect use of the enterprise service (e.g., the DoD Component information network authorization package and service provider subscriber list).

g. The UCDSMO, DSAWG, and user community will be notified at least 12 months before an enterprise service being terminated to ensure the transition of user community CD requirements to another CDS. The proposed schedule to change or terminate an enterprise service may require DoD ISRMC approval depending on operational impact to the DoD Component(s) dependent on the enterprise service.

4. MINIMAL IMPACT CDS AND REPEATABLE CDS INSTANTIATIONS

a. Minimal Impact CDS Authorization. Certain CDSs pose a minimal risk to DODIN. For example, a CDS with no DODIN connectivity, encrypted tunneling, or data flow isolation may have minimal impact.

(1) The determination that a CDS has minimal impact on the DoD is made during the pre-RMF Step 0 found in Table 1 in Enclosure 4 of this instruction.

(2) During the analysis of CDS alternatives in accordance with the pre-RMF Step 0 in Table 1 in Enclosure 4 of this instruction, a CDS selection recommendation will be made by the CDTAB. As applicable, this recommendation will also include the determination that the CDS has minimal impact on the DODIN.

(3) The DSAWG will approve CDS selection and an initial CDSA. If the DSAWG determines the CDS has minimal impact to the DODIN, the DSAWG will direct that the designated repository be updated to track additional instantiations from the initial registration of the first CDS.

(4) The DoD Component AO must submit a letter annually to his or her respective CDSE and the CDTAB stating there is still a need for the CDS and that there is no change to the CDS implementation or its impact on the DODIN.

(a) The CDSE will notify the DISA Enterprise Connection Division and ensure SGS is updated accordingly in accordance with Reference (s).

(b) If a DoD Component wants to change the CDS implementation, the requirement must be resubmitted for a CDSA as outlined in Enclosure 4 of this instruction.

b. Repeatable CDS Instantiation Authorization. For authorization of additional, repeatable instantiations of a CDS, the CDS must first complete the RMF process outlined in Enclosure 4 of this instruction, and then obtain an authorization to operate and a CDSA. For example, CDSs in mobile platforms or training systems may require multiple, repeatable CDS instantiations.

(1) The DSAWG will specify the criteria for obtaining authorization for repeatable instantiations of a CDS. At a minimum, the criteria will include: a specific mission; the same hardware, software, and configuration; identical data types, filters, and flows; the same classification levels and information networks, which may include different enclaves; a matching risk environment; a proliferation control plan; and a tracking methodology for instantiations.

(2) The requestor must prove to the DSAWG that instantiations are identical to include site security control assessments; master configuration disks, and disk cloning.

(3) The DSAWG will authorize the maximum number of instantiations in the CDSA.

(4) The DoD Component CDS owner must establish a tracking process approved by the CDSE and must track instantiations to include CDS number; unique CDS identifiers, such as hardware serial number or asset tag; location; deployment dates; local points of contact; and the Command Communications Service Designator. The DoD Component CDS owner or manager will forward this information to the CDSE monthly or when changes occur for uploading the information into the designated repository.

(5) An annual revalidation of the CDS instantiations is required as directed by the DSAWG or DoD ISRMC.

5. CDS EXCEPTIONS AND LEGACY CDS TRANSITION

a. All DoD Components must transition to use of the CDS baseline list.

b. Use of a CDS that is not on the CDS baseline list or is on the CDS sunset list requires a letter of exception and POA&M detailing the transition to a CDS baseline list CDS.

c. If the DoD Component determines that no available CDS baseline list CDS can be implemented due to operational need or unique technical requirements, a DoD Component CIO standard letter requesting an exception will be forwarded to the DSAWG. The letter must justify the exception, provide an analysis of CDS alternatives considered, and include an enclosure with available security test results from either a government or commercial SCA for the CDS.

(1) For a planned CDS, a POA&M or a documented and funded approach is required.

(2) A POA&M must include the transition to a CDS baseline list CDS, describing the risk mitigation strategy.

d. For a CDS on the CDS sunset list, the exception letter and POA&M must be submitted to the DSAWG for evaluation at least one year prior or as soon as the exception requirement is established to the published CDS sunset date.

e. The POA&M and exception letter is forwarded through the DSAWG to the DoD ISRMC for a CDSA. A CDSA for a legacy CDS or CDS not on the CDS baseline list is required to authorize its employment.

6. USE OF REMOVABLE MEDIA FOR CD DATA TRANSFER

a. The DoD Component authorizing official is the approval authority for authorizing the use of removable media for CD data transfers within their area of responsibility. Any alternate approving officials designated must be an O-6 or equivalent to act on behalf of the authorizing official.

b. The DoD Component will use their established and documented program to conduct CD data transfers to include policy, acquisition, operations, and disposal using removable media.

c. Only designated personnel will be authorized to conduct CD data transfers.

d. Removable media will be properly accounted for, marked, and securely managed in accordance with Volume 2 of Reference (i) and Reference (ac).

7. PROCESSING REQUEST FOR CD URGENT OPERATIONAL REQUIREMENT

a. In those cases where a DoD Component has an urgent, mission-critical CD requirement, the requesting organization will immediately contact their respective DSAWG representative to sponsor the request.

b. The respective DSAWG representative will review the requesting organization's request and supporting evidence. If the request is an Urgent Operational Requirement and cannot follow the normal CDS approval process, the DSAWG representative will contact the DSAWG Chair, via the DSAWG Secretariat to identify and lay out the specific urgent CD requirement and proposed CDS with supporting evidence.

c. The DSAWG Chair will evaluate the justification and submitted evidence, and consult with the applicable DoD Component CDSE(s) and DSAWG representative(s) impacted by the operational requirement. If the connection is deemed a "high risk" or outside the previously approved DSAWG risk acceptance decisions, then the DSAWG Chair will consult with the respective mission area principal authorizing official, DoD ISRMC representative, or the DoD ISRMC Chair.

d. Barring objections, the DSAWG Chair will approve an administrative interim CDSA to meet the urgent operational requirement and to provide sufficient time to get the requirement into the normal CDS approval process. The adjudication process has the flexibility and capability to manage and adjudicate urgent/time-sensitive, mission-critical CD requirements expeditiously, within 24-48 hours when necessary.

e. The DSAWG Secretariat will notify the DSAWG membership of the interim approval of a CDSA. The owning DoD Component CDSE will bring expeditiously the CD requirement to the DSAWG for a full community risk decision on CDS.

f. Questions regarding processing urgent operational CDS requirements should be directed to the DSAWG Secretariat at (301) 225-2905 or disa.meade.ns.mbx.dsawg@mail.mil. The DSAWG membership list can be found at: http://intelshare.intelink.sgov.gov/sites/dsawg/default.aspx.

8. RECIPROCITY

a. Reciprocity of CDS and CD technology body of evidence (BOE) will advance information sharing and reduce rework and cycle time to satisfy a CD capability requirement.

b. DoD and the IC will use a consistent BOE from the RMF process to support reciprocity.

(1) To support reciprocity for a CDS, the DoD BOE consists of:

(a) The security authorization package (i.e., the security plan (SP) including architecture documentation and network topology, SAR, POA&M, and authorization decision document) in accordance with Reference (b).

(b) System inventory and installation procedures.

(c) Security test procedures (e.g., site and CD technology security control assessment plans and procedures).

(d) Results of site and CD technology security test procedures.

(e) Artifacts labeled as "if available or highly desired" (e.g., two copies of the baseline software application).

(2) Only security controls required to be tested due to a CDS deployment into a different IS environment will be executed. Earlier test procedures will not be re-executed.

c. Requests for reciprocity documentation for CDS baseline list CDS will be forwarded to the point of contact listed in the CDS information sheet.

9. FOREIGN RELEASE OF CDS OR CD TECHNOLOGY

a. All requests for disclosing, releasing, or transferring of a DoD CDS, CD technology, or associated information to a foreign government or mission partner must be consistent with References (n), (o), (p), CNSSP No. 8 (Reference (ah)) and the procedures in CJCS Instruction 6510.06B (Reference (ai)).

b. Requests must meet the disclosure criteria, conditions, and limitations in accordance with Enclosure 3 of Reference (n).

c. DoD Component organizations with a requirement for a foreign release of information on a CDS or release of a CDS or CD technology will contact their DoD Component Foreign Disclosure Officer and CDSE before release to ensure compliance with References (n), (o), (p), (q), and (ai).

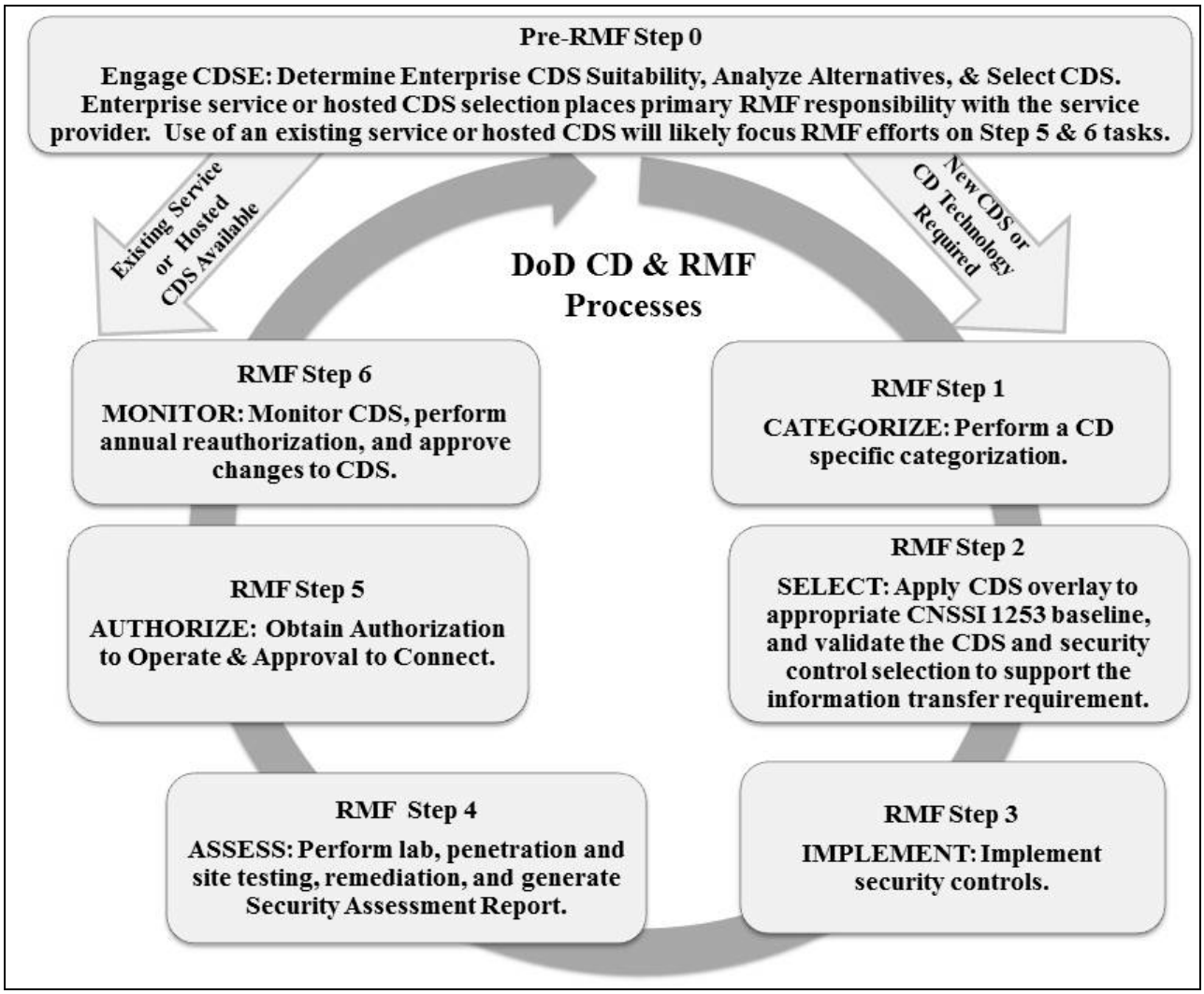
ENCLOSURE 4

CD PROCESS AND THE DOD RMF PROCESS

1. CD PROCESS AND THE DOD RMF PROCESS OVERVIEW

a. A CDS is assessed and approved as a component within an existing or a new IS's authorization boundary or authorized as a separate IS using the DoD RMF process in accordance with Reference (b) and as shown in the figure.

Figure. DoD CD and RMF Processes



b. The CDSE will be contacted before a DoD organization executes Step 1 of the DoD CD and RMF process for a CDS as a component of an IS or as a CDS with a separate authorization boundary as described in Reference (b) and this instruction. For simplicity, the text and tables in this enclosure use the term "IS" when addressing both situations.

c. This enclosure will discuss the RMF tasks, including risk decision points, required deliverables, and the organization or position primarily responsible for conducting RMF tasks. The level of effort to complete an RMF task will depend on the status of the IS with a CDS component or a CDS with a separate authorization boundary (e.g., changes to an existing or new CDS) and will be determined by the IS owner, information owner, AO, and supporting CDSE. For more details on the DoD RMF or the federal RMF guidance, see Reference (b) and NIST Special Publication 800-37 (Reference (aj)).

2. PRE-RMF STEP 0: ENGAGE CDSE. The first task by an organization with a CD requirement is to engage the CDSE and document the CD capability requirement, determine need for a CDS, and perform an initial analysis to identify a CDS. See Table 1.

Table 1. Pre-RMF Step 0: Engage CDSE

CD Supporting Tasks	Deliverable	Responsibility	Notes:
Pre-RMF Step 0: Task 0-1: Identify CDSE and establish contact to review CD capability needs.	Document the initial CD capability requirement.	**Primary**: IS owner and information owner. **Support:** CDSE.	Information required for review by CDSE includes the CD operational profile; channel flow functional and security requirements including information description; operational impact; networking environment; and quality of service (i.e., key performance parameters). The CDSE may determine there is no actual CD need and there may be alternate means to satisfy the mission requirement.
Task 0-2: Determine if an existing enterprise CD service or an enterprise-hosted CDS baseline list CDS can satisfy the CD capability requirements.	CDS suitability determination.	**Primary**: CDSE. **Support**: IS owner; information owner; CD service provider; and CDTAB.	An initial determination of suitability for enterprise CD services or enterprise-hosted CDS is required. The CDSE with the IS owner and information owner will determine if an enterprise service is suitable to meet the CD requirement. The CDSE will contact the ECDSP. If the ECDSP can meet the CD requirement within the CDSA for the enterprise CDS, then this alternative should be the primary alternative going into analysis of alternatives. Reasons for an enterprise CD service or enterprise-hosted CDS inability to satisfy the requirement will impact the selection decision and responsibilities for completion of the rest of the DoD RMF. For those instances where enterprise CD services or enterprise-hosted CDSs are not suitable, the determination of suitability will assist in completion of the analysis of CDS alternatives and CDS selection.

Table 1. Pre-RMF Task: Engage CDSE, Continued

CD Supporting Tasks	Deliverable	Responsibility	Notes:
Task 0-3: Analysis of CDS alternatives to satisfy information transfer, IS, and supported mission requirements.	CDS recommendation with analysis of alternatives.	**Primary:** IS owner; information owner; and CDSE. **Support:** CDTAB, ISSE; AO or designated representative; CD service provider; and USSTRATCOM.	The analysis of CDS alternatives is jointly conducted by the IS owner, information owner, and CDSE. Considerations in the analysis include, but are not limited to, funding and resources programmed for the life cycle management of the CDS; risk based on the CDS and its operating environment security controls; and use of an enterprise service or enterprise-hosted CDS. USSTRATCOM will provide relevant security data in support of analysis. The CDTAB reviews the analysis of alternatives to provide a CDS recommendation.
Task 0-4: CDS selection decision based on analysis of CD alternatives.	CDS selection decision.	**Primary:** DSAWG. **Support:** IS owner; information owner; CDSE; CDTAB; and USSTRATCOM.	Based on CDTAB recommendation and review of alternatives, a CDS is selected. The DSAWG will determine selection of an existing enterprise service, enterprise-hosted CDS, or operational CDS. The CD service provider with CDTAB would determine any tasks or DSAWG approval required within Task 6-1 of RMF Step 6 for implementation. Selection of a new CDS or CD technology selection requires entry into RMF Step 1.

a. The identification of a CD capability requirement should occur as early as possible in an IS's development life cycle or as soon as an organization determines the need for a requirement in an existing IS. As soon as such a need is identified the organization must contact their CDSE. If a DoD Component does not have a CDSE, the function may be provided via an agreement with another DoD Component's CDSE.

b. Next the CDSE, IS owner, and information owner conduct an initial analysis of CD capability requirements and available CDSs to determine the best CDS available to meet the requirements.

c. Table 2 identifies the available types of alternatives to meet CD capability requirements and who assumes the primary and the supporting roles for RMF actions on CDS selection.

Table 2. CDS Alternatives and Identification of Primary RMF Leads

Category	CDS Alternatives	IS Owner (Primary)	Information Owner (Supporting)	Notes
ENTERPRISE	1. Enterprise CD service	ECDSP	DoD Component (Requestor)	The CD capability requirement owner is the information owner in a supporting role and works with the CDSE to ensure that the requirement is met by the ECDSP in accordance with the support agreement. The ECDSP (e.g., DISA) is the lead for completing the RMF steps for the IS. The information owner's CDSE is responsible for providing the ECDSP with the risk related to access and transfer of the information.
	2. Existing enterprise-hosted CDS (additional point to point CDS or new information transfer flow)	ECDSP	DoD Component (Requestor)	The CD capability requirement owner is the information owner in a supporting role and works with the CDSE to ensure that the requirement is met by the enterprise-hosted CDS ECDSP in accordance with the support agreement. The enterprise-hosted CDS ECDSP is the lead for completing the RMF steps for IS. The CDSE is responsible for providing the ECDSP with the risk related to access and transfer of the information.
POINT TO POINT	3. Operational CDS baseline list CDS	CDS's IS system owner (internal or external to the DoD Component)	DoD Component (Requestor)	The CD capability requirement owner is the information owner in a supporting role and works with the CDSE to ensure that the CD requirement is met by the operational CDS's IS owner in accordance with the support agreement. The operational IS owner is the lead for completing the RMF steps for IS. The information owner's CDSE is responsible for providing the service provider the risk related to access or transfer of the information.
	4. Existing CDS baseline list CDS (used as previously tested)	DoD Component (Requestor)	DoD Component (Requestor)	The DoD Component is both the IS owner and information owner and is responsible for completing the RMF steps, ensuring the life cycle maintenance, and protecting and monitoring the IS.
	5. Modifying CDS baseline list CDS	DoD Component (Requestor)	DoD Component (Requestor)	The DoD Component is both the IS owner and information owner and is responsible for completing the RMF steps, ensuring the life cycle maintenance, and protecting and monitoring the IS.
NEW TECH	6. CD technology requiring development and full testing	DoD Component (Requestor)	DoD Component (Requestor)	In certain cases a CDS baseline list CDS may not meet the CD capability requirements for the mission and a new technology may be required. New development will be pursued only when options 1-5 cannot meet mission needs. The DoD Component is both the IS owner and information owner and is responsible for completing the RMF steps (including a CD technology security control assessment to verify and validate security requirements and the IS security control assessment), ensuring the life cycle maintenance, and protecting and monitoring the IS.

Table 2. CDS Alternatives and Identification of Primary RMF Leads, Continued

Category	CDS Alternatives	IS Owner (Primary)	Information Owner (Supporting)	Notes
CDS Not on the CDS baseline list	7. CDS not on the CDS baseline list or a CDS on CDS sunset list	DoD Component (Requestor)	DoD Component (Requestor)	Approval to use a CDS that is not in the CDS baseline list or is in the CDS sunset list will be handled on a case by case basis by the DoD ISRMC and requires a DoD Component CIO to submit a letter of exception justifying the request and a POA&M to DoD ISRMC. The POA&M must include a transition to a CDS baseline list CDS describing the risk mitigation strategy.

3. RMF STEP 1: CATEGORIZE IS. RMF Step 1 is completed by categorization of the IS with a CDS component or a CDS as an IS in accordance with Reference (y). See Table 3.

Table 3. RMF Step 1: Categorize IS

CD Supporting Tasks	Deliverable	Responsibility	Notes:
RMF Task 1-1: Categorize the IS.	Document results of the categorization in the SP.	**Primary:** IS owner or CD service provider. **Support:** CDSE; ISSM or ISSO; information owner; ISSE; AO or designated representative.	The security categorization determines the appropriate values for factors that definitively represent the protection security requirements of the information or the information system.
a. For a new IS with a CDS component.	a. Must perform a categorization on the IS and a CDS.		
b. For an existing IS adding a new CDS component.	b. Revisit or update the categorization.		
c. For a CDS as an IS.	c. The CD is the IS that is being deployed. Perform categorization in accordance with the RMF.		
RMF Task 1-2: Describe the CD capability requirements, CDS, and update SP.	Update SP and description of CDS in CD Appendix (CDA).	**Primary:** IS owner or CD service provider. **Support:** CDSE; ISSM or ISSO; information owner; ISSE; and AO or designated representative.	The DoD Component AO validates the CD capability requirement and provides DoD Component-level approval for the updated SP, as required in accordance with DoD Component guidance.
RMF Task 1-3: Register the CDS as a CD capability requirement through the CDSE.	CDS registered and relationship with IS established in designated tracking system.	**Primary:** CDSE. **Support:** IS owner; CD service provider; ISSM or ISSO; ISSE.	The registration process establishes the relationship between the IS, the CDS, and the IS owner that owns, manages, or controls the system. The confidentiality, integrity and availability levels are identified within the tracking system.

a. Determine the security impact of the IS with a CDS component or a CDS as an IS including the information processed, stored and transmitted. Additionally, the categorization for an IS with a CDS component must also consider the connected environment (e.g., connection

partners, environmental threats, DODIN compared with non-DODIN, or boundary protection requirements).

b. Categorization review of the IS with a CDS component is valuable to determine required controls for processed data that may be independent of the CDS such as the Information Security Program protection requirements in Volumes 3 and 4 of Reference (i). For example, availability requirements may be driven to a higher rating than what the CDS will impose due to handling of certain types of data (e.g., tactical data or space data).

c. Results of the system categorization are documented in Section 1 (Requirements) of the DoD Component's CDA, which will become part of the IS's SP as listed in Reference (b).

4. RMF STEP 2: SELECT SECURITY CONTROLS

a. Security controls are the safeguards or countermeasures employed to protect the confidentiality, integrity, and availability of the IS and its information and to properly manage mission, business, and system risks. More information on this step and tasks in Table 4 may be found in Reference (aj). The confidentiality, integrity, and availability levels determined in accordance with Reference (y) during Step 1 (Categorization) will establish the baseline set of security controls from NIST Special Publication 800-53 (Reference (ak)) to be used in conjunction with the CD Overlay. The CD Overlay can be found at the UCDSMO Governance and Policy link at https://intelshare.intelink.gov/sites/ucdsmo/SitePages/Home1.aspx.

Table 4. RMF Step 2: Select Security Controls

CD Supporting Tasks	Deliverable	Responsibility	Notes:
RMF Task 2-1: Identify the security controls provided by the organization as common controls for IS.	Document security controls in SP.	**Primary:** IS owner or CD service provider. **Support:** ISSM or ISSO; ISSE; information owner; AO or designated representative; and CDSE.	Task 2-1 and Task 2-2 may be performed in parallel. In those instances where an enterprise CD service or another CD service provider is selected, the CD service provider has primary responsibility for this step, supported by the information owner and supporting CDSE. The initial set of security controls will be identified from the categorization of the IS in accordance with Reference (y). Controls inherited will be influenced by the type of IS being implemented (as described in Task 1-1 in Table 3). Security controls required are typically traceable to the security requirements in federal and DoD-level issuances. For example, see cybersecurity requirements in Reference (c) for ISs and the Information Security Program protection requirements in Volumes 3 and 4 of References (i) for information.

Table 4. RMF Step 2: Select Security Controls, Continued

CD Supporting Tasks	Deliverable	Responsibility	Notes:
RMF Task 2-2: Select, modify, enhance or add security controls for the IS and document the selected security controls in the SP.	Document security controls in the SP.	**Primary:** IS owner or CD service provider. **Support:** ISSE; ISSM or ISSO; information owner; AO or designated representative; CDSE; and SCA.	The CD security control overlay will be utilized to identify CD-specific security controls. There may be other appropriate security control overlays (e.g. PII, tactical, or space) that need to be applied that may affect allocation of security controls. Identify CDS security control requirements based on the threats, the CD security control overlay for CDS baseline list CDS, and include review of previous SARs and security relevant configuration guidance. Tailoring of controls, as described in Reference (b), will be performed in this step. This tailoring will be influenced by the type of IS being implemented.
RMF Task 2-3: Develop or update a strategy for continuous monitoring of security control effectiveness and any proposed or actual changes to the IS and its operational environment in accordance with Reference (c) and additional guidance in NIST Special Publication 800-137 (Reference (al)).	New or updated continuous monitoring strategy.	**Primary:** IS owner or CD services provider. **Support:** Information owner; ISSM or ISSO; AO or designated representative; CDSE; and SCA.	The strategy identifies the security controls to be monitored, the frequency of monitoring, and the security control assessment approach, how changes will be monitored, how security impact analyses will be conducted, and the security status reporting process. If a CD service provider is engaged on behalf of an information owner, the CD service provider will perform this task.
RMF Task 2-4: Review and approve the SP for the IS.	Updated SP and continuous monitoring strategy.	**Primary:** AO or designated representative. **Support:** IS owner; information owner; ISSM or ISSO; and CDSE.	The SP and continuous monitoring strategy review, along with the review of the IS operational and planning documents (such as the information support plan) lead to RMF Step 3. Validate that the CDS and security controls support CD information transfer requirement.

b. The next step is to tailor the list of controls, as described in Reference (b), to account for the operating environment and other factors. The resulting set of controls may be satisfied by inherited controls or by controls implemented in the CDS. RMF Task 2-1 and Task 2-2 can be performed in parallel.

5. RMF STEP 3: IMPLEMENT SECURITY CONTROLS. For this step, the IS owner for the CDS will implement the security controls within the CDS and the operational environment in accordance with the DoD RMF tasks outlined in Reference (b). See Table 5.

Table 5. RMF Step 3: Implement Security Controls

CD Supporting Tasks	Deliverable	Responsibility	Notes:
RMF Task 3-1: Implement the security controls specified in the SP.	CDS and operating environment security controls implemented in accordance with security relevant configurations.	**Primary:** IS owner or CD service provider. **Support:** ISSE; ISSM or ISSO; and SCA.	In those instances where an enterprise CD service or another CD service provider is selected, the CD service provider has primary responsibility, supported by the information owner and CDSE for this step. The SCA is encouraged to be present at all design reviews. For cases where new development is required, any new CD-related technology development activities must be coordinated with the UCDSMO before initiation, and the DoD acquisition process found in Reference (x) and section 2 of Enclosure 3 of this instruction must be followed.
RMF Task 3-2: Document the security control implementation, as appropriate, in the SP, providing a functional description of control implementation.	Updated SP.	**Primary:** IS owner or CD service provider. **Support:** ISSM or ISSO; ISSE; and CDSE.	The IS owner for the CDS must document the selected controls for the CDS in accordance with the RMF tasks outlined in Reference (b). There are no unique CDS requirements associated with this task.

6. RMF STEP 4: ASSESS SECURITY CONTROLS

a. For this step, the implemented security controls for a CDS are independently evaluated. See Table 6. CDSs may be comprised of multiple components (e.g., hardware, software, or filters), may or may not operate as a component of a larger IS, and must always be independently evaluated. This step determines the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome in meeting security requirements. Guidance for assessments can be found in the UCDSMO CD Security Assessor's Guide including SAR template (Reference (am)).

Table 6. RMF Step 4: Assess Security Controls

CD Supporting Tasks	Deliverable	Responsibility	Notes:
RMF Task 4-1: Develop, review, and approve a plan to assess security controls for the IS.	Upload the completed security control assessment plan for the CD technology or site to the designated centralized repository (i.e., SGS).	**Primary:** SCA. **Support:** IS owner or CD service provider; ISSM or ISSO; information owner; CDSE; AO or designated representative; and senior information security officer (SISO).	In those instances where an enterprise CD service or another CD service provider is selected, the CD service provider has primary responsibility, supported by the information owner and CDSE for this step. For CDSs, a formal test readiness review is required that ensures that the SP and all associated documentation is available to support the assessment activities. The assessment plan should include how to perform both a CD technology security control assessment (if required) and the site security control assessment of CDS and its operational environment using UCDSMO assessment guidance. For a modified baseline solution, the CDTAB will evaluate the changes and the extent to which the CDS must be tested. The DSAWG will arbitrate disputes regarding the extent to which the CDS must be tested.
RMF Task 4-2: Assess the security controls in accordance with the assessment procedures defined in the security control assessment plan.	a. Completed CD technology security control assessment and penetration testing, if required.	a. **Primary:** SCA. **Support:** IS owner or CD service provider; information owner; and ISSM or ISSO.	Tasks 4-2 through 4-4 are iterative. a. The assessor will consider reusing previous security control assessment results, when reasonable and appropriate to support reciprocity.
	b. Authorization to issue an interim CDSA.	b. **Primary:** DoD ISRMC or DSAWG. **Support:** IS owner or CD service provider; CDTAB; information owner; ISSM or ISSO; SCA; and CDSE.	b. The CDTAB reviews updated CDA and security control assessment plan and provides risk assessment and recommendation to DSAWG. Before the site security control assessment, an interim CDSA for conducting site security control assessment for CDS is issued for the network service provided.
	c. Completed site security control assessment.	c. **Primary:** SCA. **Support:** IS owner or CD service provider; information owner; and ISSM or ISSO.	c. Before site security control assessment, all high risk findings from CD technology and penetration testing must be addressed. The site security control assessment is part of the original security control assessment for a new IS or updates an existing SAR based on the addition of a CDS or new CDS as a component of an existing IS.
RMF Task 4-3: Prepare the SAR documenting the issues, findings, and recommendations from the site security control assessment.	a. Initiate or update SAR after CDS security control assessment.	**Primary:** SCA. **Support:** IS owner or CD service provider; and ISSM or ISSO.	Tasks 4-2 through 4-4 are iterative. Guidance on the format to use for documenting the results of testing can be found using Reference (am).
	b. Final SAR updated after site security control assessment of CDS and operational environment.		

Table 6. RMF Step 4: Assess Security Controls, Continued

CD Supporting Tasks	Deliverable	Responsibility	Notes:
RMF Task 4-4: Conduct initial remediation actions on security controls based on the findings and recommendations of the SAR and reassess remediated controls, as appropriate.	Updated SAR and CDA. Uploaded SAR and CDA to designated centralized repository.	**Primary:** IS owner or CD service provider; and SCA. **Support:** AO or designated representative; SISO; Information Owner; ISSM or ISSO; and ISSE.	Tasks 4-2 through 4-4 are iterative. Remediation actions are performed during testing to reduce residual findings. The SP will be updated to reflect the system state after remediation. Remediation will not be deemed complete until all high risk findings are addressed.

b. Task 4-2 describes the type of assessments required for CDSs. After the completion of CD technology security control assessment, IS owners will request a CDSA for site security control assessment of the CDS in its operational environment. The differing primary and supporting roles for the security control assessment are shown in Table 6. There are three components to the security control assessment for an IS with a CDS component or a separate IS.

(1) CD Technology Security Control Assessment. A certified laboratory performs the security control assessment. This assessment step includes review of the implemented security controls and security relevant configuration of the CD technology; a CD technology security control assessment is required if a selected solution is a new technology, requires a new TOE, significant security relevant configuration changes are made, or a new filter is required. For a CD technology that has already been assessed (e.g., one requiring a new TOE or having significant configuration changes), only those security controls impacted require testing. The SCA verifies and validates the CD technology as meeting functionality and security requirements before placing the CD technology on the CDS baseline list.

(2) Site Security Control Assessment. The site security control assessment is performed within the operational environment of the IS to ensure proper system configuration; appropriate inheritance of common controls; adequate security within the deployed environment; and sufficient implementation of technical controls within the specific operational configuration. This includes Red Team operations for unknown vulnerabilities within the system when deployed in the operational environment, as required.

(3) Penetration Testing. NSA will conduct or oversee DoD organizations testing for unknown vulnerabilities and attempts to circumvent or defeat the security features of a new CD technology or new versions of current CD technology.

7. RMF STEP 5: AUTHORIZE IS. This step authorizes the IS for operation based on a determination of the risk to organizational operations and assets (including the risk of unauthorized disclosures of classified and controlled unclassified information), individuals, other organizations, and the nation resulting from the operation of the IS and the decision that this risk is acceptable. In the DoD, this step consists of the IS AO's authorization to operate and the DSAWG or DoD ISRMC's CDSA for access or transfer of information between different interconnected security domains. See Table 7.

Table 7. RMF Step 5: Authorize IS

CD Supporting Tasks	Deliverable	Responsibility	Notes:
RMF Task 5-1: Prepare the POA&M based on the findings and recommendations of the SAR, excluding any remediation actions taken.	POA&M.	**Primary:** IS owner or CD service provider. **Support:** Information owner; ISSM or ISSO; SCA; and CDSE.	In those instances where an enterprise CD service or another CD service provider is selected, the CD service provider has primary responsibility, supported by the information owner and CDSE for this step. The IS owner, with assistance from the organization's CDSE, must document the agreed on actions for ongoing mitigation of findings not addressed during testing, in accordance with the RMF tasks outlined in Reference (b). There are no unique CDS requirements associated with this task.
RMF Task 5-2: Assemble the security authorization package artifacts, and submit the artifacts to the AO for adjudication.	Updated SP, SAR and POA&M. Risk Assessment Report.	**Primary:** IS owner or CD service provider. **Support:** SCA; ISSM or ISSO; and CDSE.	The IS owner, with assistance from the organization's CDSE, must submit the security authorization package and risk assessment report to the AO for risk determination and risk acceptance in accordance with RMF tasks outlined in Reference (b). If the CDS is an update to a baseline product or a new development, the UCDSMO will be copied on the submission. CDSE must maintain a record of all submissions from their DoD Component (or supported DoD Component, if acting on behalf of another DoD Component).
RMF Task 5-3: Determine the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation.	Risk determination	**Primary:** AO for the IS and the DoD ISRMC or DSAWG if delegated for DoD enterprise **Support:** SISO; AO designated representative; CDSE; CDTAB; SCA; USSTRATCOM; and DIA.	The SAR artifacts and risk assessment report are reviewed and assessed for impact of the proposed CDS, to the IS and to the DoD enterprise in accordance with Reference (b). CDS risk determination should include evaluation of vulnerabilities, threats, and impacts from and to the information network or environment, the data traversing the CDS, and the CDS itself consistent with Reference (v).
	a. IS risk determination.		a. Risk determination for the IS by the AO.
	b. DoD enterprise risk determination.		b. Risk determination for the DoD enterprise by the DSAWG or DoD ISRMC.

Table 7. RMF Step 5: Authorize IS, Continued

CD Supporting Tasks	Deliverable	Responsibility	Notes:
RMF Task 5-4: Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.	a. Authorization (to operate) decision document for IS.	a. **Primary:** AO. **Support:** AO designated representative and SISO.	a. The AO will produce an authorization decision document for the implemented IS in accordance with Reference (b). For the DoD, it will be the AO's decision to issue an authorization to operate the IS based on the site security control assessment including the SCA's recommendation and the DoD Component risk assessment report.
	b. CDSA to authorize the use of a CDS to access and transfer information between different interconnected security domains.	b. **Primary:** DoD ISRMC or DSAWG. **Support:** AO or designated representative; SISO; CDTAB; DSAWG; and DoD information network provider.	b. Once an authorization to operate is issued by the appropriate AO, the DSAWG or DoD ISRMC reviews the CDTAB recommendations, the DoD Component risk assessment, and the DoD information network provider (e.g., DISA for the DISN) satisfactory security review of connected operational environment. Based on review the decision to issue a CDSA is made. The information network provider updates or issues an approval to connect.

8. RMF STEP 6: MONITOR SECURITY CONTROLS

a. Once a CDS is in operation, the IS's security state must be monitored in accordance with Reference (b). The security control monitoring step tracks changes to the CDS as an IS or the IS with a CDS as a component that may affect security controls and then assesses resultant security-control effectiveness in accordance with References (b) and (am). The IS owners or CD service providers may use References (u) and (al) to implement rigorous and comprehensive, ongoing monitoring programs. These ongoing monitoring activities are in addition to the periodic inspections identified in subparagraphs c through e of this section. If done correctly, these ongoing monitoring activities will streamline the periodic assessments. See Table 8.

b. Active defense of CDSs and the IS environment (e.g., an enclave) will be performed to enable management, modification, or enhancement of required security controls. This monitoring will be conducted by the site and CDS operator in coordination with their designated organizations providing cybersecurity.

c. At a minimum, once every 3 years, or as requested or directed, an on-site validation inspection (e.g., USSTRATCOM or DoD Component cybersecurity inspection) will be performed for the CDS and deployed environment. This inspection will use CDS focused expertise, analysis, and tools to validate CDS owner self-assessment and will be recorded in the designated centralized repository. In addition, a periodic vulnerability self-assessment of the CDS itself is required by the DSAWG for revalidation of the CDSA using References (b) and (am).

Table 8. RMF Step 6: Monitor Security Controls

CD Supporting Tasks	Deliverable	Responsibility	Notes:
Task 6-1: Determine the security impact of proposed or actual changes to the IS and its environment of operation.	Change Request.	**Primary:** IS owner or CD service provider. **Support:** AO or designated representative; information owner; ISSM or ISSO; CDSE; and CDTAB.	In those instances where an enterprise CD service or another CD service provider is selected, the CD service provider has primary responsibility, supported by the information owner and the CD service provider's CDSE for this step. This could be a new information flow for an existing enterprise service or the transition of a DoD Component CDS to an enterprise-hosted CDS site based on a Pre-RMF Step 0 selection decision. If changes are required to an operational CDS, the change will be documented by the IS owner or CD service provider, and presented to the AO. Changes to operational devices must be reviewed and approved by the CDTAB or DSAWG as applicable before the changes being made.
Task 6-2: Assess all security controls employed within and inherited by the CDS in accordance with the organization-defined monitoring strategy.	Periodic continuous monitoring reporting.	**Primary:** SCA. **Support:** IS owner or CD service provider; AO or designated representative; information owner; ISSM or ISSO; and CDSE.	Selection of security controls for ongoing vulnerability self-assessment will be done in a manner to ensure all controls are reviewed annually and testing conducted on those controls that had changes in compliance status (noncompliance) or require minimum annual testing based on security control implementation guidance. A defined periodic review of selected controls is required for all IS, in accordance with guidance established by the AO and the DSAWG. Some examples of CDS specific items to be evaluated are: operating system end of life, hardware warranty expiration, current patch level, connection approval, etc. Review will include the evaluation of open POA&M weaknesses that were created at authorization and ensure that corrective actions have either been completed or are on track for completion within the accepted schedule. The SCA is responsible for validating the completed POA&Ms under the direction of the AO and the DSAWG.
Task 6-3: Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M.	IS risk determination.	**Primary:** IS owner or CD service provider. **Support:** AO; AO designated representative; information owner; ISSM or ISSO; ISSE; and CDSE.	The IS owner or CD service provider for the CDS must update appropriate documents as a result of the ongoing monitoring of the CDS in accordance with the RMF tasks outlined in Reference (b). There are no unique CDS requirements associated with this task.

Table 8. RMF Step 6: Monitor Security Controls, Continued

CD Supporting Tasks	Deliverable	Responsibility	Notes:
Task 6-4: Update the SP, SAR, and POA&M based on the results of the continuous monitoring process.	Updated SP, SAR, and POA&M.	**Primary:** IS owner or CD service provider. **Support:** Information owner and the ISSM or ISSO.	The IS owner or CD service provider for the CDS must update appropriate documents as a result of the ongoing monitoring of the CDS in accordance with the RMF tasks outlined in Reference (b). There are no unique CDS requirements associated with this task.
Task 6-5: Report the security status of the IS to the AO and other appropriate organizational officials on an ongoing basis, in accordance with the monitoring strategy.	Periodic continuous monitoring reporting.	**Primary:** IS owner or CD service provider. **Support:** ISSM or ISSO; CDSE; and CDTAB.	The IS owner or CD service provider reports the security status of the IS with CDS to the AO, and CDTAB on an ongoing basis in accordance with the RMF tasks outlined in Reference (b). The security status should include the effectiveness of the security control implementations by the CDS and inherited from the IS.
Task 6-6: Review the reported security status of the IS and CDS (including the effectiveness of security controls employed within and inherited by the CDS) on an ongoing basis in accordance with the monitoring strategy. Determine whether the risk to organization operations, assets, individuals, other organizations, or the Nation remains acceptable.	Accept Risk.	**Primary:** AO for the IS and the DSAWG for CDSA. **Support:** AO designated representative; SISO; and USSTRATCOM.	The AO annually reviews the IS's security posture and authorization to operate to confirm security posture remains acceptable and validates CD requirement. The CDTAB will act on the security status and determine the updated risk, as required. The risk status will then be provided to the AO and the DSAWG to accept the risk as required. USSTRATCOM will provide relevant security data to CDTAB and DSAWG in support of risk recommendations and decision.
	a. Authorization or the acceptance decision for CDS.	a. The AO will authorize or accept risk for authorizing the CDS.	If an enterprise service or enterprise-hosted CDS is not currently employed, the AO must determine if the requirement can migrate to an enterprise service or enterprise-hosted site.
	b. CDSA.	b. The DSAWG will deny or grant a 1 year extension for the CDSA, as required or the DISA CDS Team may issue a CDSA as authorized by the DSAWG.	The DoD ISRMC can direct the use of an enterprise service or enterprise-hosted CDS. The DoD Component will submit a POA&M within 30 days for the transition. The POA&M must provide for transition within 12-18 months. Unresolved resource issues will be forwarded to the DoD CIO Executive Board for DoD CIO resolution.

Table 8. RMF Step 6: Monitor Security Controls, Continued

CD Supporting Tasks	Deliverable	Responsibility	Notes:
Task 6-7: Implement a CDS decommissioning strategy, when needed, which executes required actions when a CDS is removed from service.	Updated IS inventory.	**Primary:** IS owner or CD service provider. **Support:** AO designated representative; SISO; information owner; ISSM or ISSO; and CDSE.	As all CDSs process sensitive information and are export controlled, the disposal of the CDS must be in accordance with Reference (o) and any information security requirements in Volume 3 of Reference (i), and DoDI 2030.08 (Reference (an). In the decommissioning of the CDS or CDS flow, the IS owner or CD service provider should work with the CDSE to ensure all appropriate tracking systems are updated and in accordance with Reference (s). The IS owner with the CDSE, will monitor the CDS sunset list to plan for decommissioning.

d. To revalidate a CDSA the enclave must have a satisfactory security review by the governing DoD information network owner (e.g., DISA for the DISN). A revalidation memo will be submitted by the AO stating that the CDS is still required and that the CDS security relevant configurations have not changed. Supporting documentation can include a satisfactory vulnerability self-assessment or a cybersecurity inspection and the approved POA&M for the enclave. This documentation will be provided to the CDSE on completion of these actions. Exemptions (e.g., for mobile devices or platforms such as ships, vehicles, or aircraft) from specified requirements may be authorized by the DSAWG.

e. CDSAs issued by the DSAWG or DoD ISRMC will be valid for up to 3-years. The DSAWG and DoD ISRMC may issue CDSAs for less than 3 years based on assessment of risk or requirement.

ENCLOSURE 5

CD AND RMF ROLES

1. DOD ISRMC. The DoD ISRMC:

a. Provides governance approval for enterprise CD services, CDSs, and CD technologies with support from the DSAWG in accordance with Reference (c) as the DoD risk executive. The DoD ISRMC website can be found at https://intellipedia.intelink.sgov.gov/wiki/DISN/GIG_Flag_Panel.

b. Approves the risk model for DoD authorization of enterprise CD services, CDSs, and CD technologies.

c. Authorizes or delegates authority to the DSAWG for an enterprise CD service or CDS CDSA. The CDSA will be approved for 1 to 3 years based on current DoD ISRMC criteria.

d. Collaborates with the Committee on National Security System Enterprise Risk Management Board on common CDS risk governance and reciprocity processes.

e. Approves or delegates approval of DoD Component POA&Ms for replacing legacy CDSs not on CDS baseline list operating beyond specified time on CDS sunset list, and letters of exception for the operation of a CDS not on the CDS baseline list.

f. Oversees the CDSA process and provides guidance to the DSAWG and CDTAB.

g. Resolves issues brought forward from the DSAWG.

h. Directs DODIN connection authorities (e.g., the DISA Connection Approval Office) to implement CDS interconnection on meeting any CDSA conditions.

i. Instructs through USSTRATCOM and the DoD chain of command the disconnection or removal of CDSs that are found operating without approval or are non-compliant with this instruction or its approved security configuration.

j. Forwards unresolved resource issues through the DoD CIO Executive Board for DoD CIO resolution.

k. Approves or delegates approval authority for Reference (t).

2. DSAWG. Under the authority, direction, and control of the DoD ISRMC, the DSAWG:

a. Adjudicates CDTAB risk assessment and CDS recommendations.

b. Approves or disapproves a CDSA for a CDS as delegated by the DoD ISRMC (e.g., a previously approved CDS) or makes a CDSA recommendation to the DoD ISRMC.

c. Reviews and approves criteria for a CDSA after consultation with DoD ISRMC.

d. Reviews Reference (s).

e. Maintains a website at http://intelshare.intelink.sgov.gov/sites/dsawg/default.aspx.

3. CDTAB. Under the authority, direction, and control of the DoD ISRMC and DSAWG, the CDTAB:

a. Analyzes DoD Component CD capability requests and proposed CDS recommendations to:

(1) Identify CDS alternatives, including not using a CDS.

(2) Review analysis of CDS alternatives, and recommend use of an enterprise CD service, an enterprise-hosted CDS or a CDS baseline list point-to-point CDS, or leveraging another DoD Component's operational CDS, to meet DoD Component capability requirements.

b. Reviews a summary of security control assessment results in accordance with this instruction as a DoD risk assessor for a CDS or CD technology to:

(1) Concur or non-concur on proposed CDS risk assessment for a CDS or CD technology.

(2) Identify issues and recommend risk mitigations for any weaknesses or deficiencies in the security controls identified by the security control assessments.

(3) Forward the risk assessment, findings, and recommendations for security services providers to the DSAWG for review.

(4) Recommend changes to existing security control implementation or suggest supplemental security controls to be used.

c. Reviews new CD technology proposals to:

(1) Determine if new CD technologies will satisfy current CD capability requirements.

(2) Make recommendation for security control assessment of new CD technologies to UCDSMO.

(3) Evaluate the proposals in light of existing commercial and government-developed CDSs, as appropriate.

(4) Identify and recommend best-of-breed CDSs for implementation as enterprise CD services, to minimize development and redundant acquisition of equivalent CDSs.

d. Reviews periodic vulnerability self-assessment for revalidation of CDSA in accordance with DoD ISRMC-approved criteria to:

(1) Advise the DSAWG of the risk.

(2) Ensure submitted vulnerability self-assessment on the security status of CDS is completed as required by DoD ISRMC criteria.

(3) Provide a technical risk assessment and mitigation recommendations for the DoD Component's CDS and POA&M.

e. Determine that an enterprise service or enterprise-hosted site cannot technically support CD requirements based on DoD Component validation of CD requirements.

f. The CDTAB site is located at https://intelshare.intelink.sgov.gov/sites/cdtab/SitePages/Home.aspx.

4. CDSE. CDSE:

a. Manages the DoD Component's CD-related activities.

b. Maintains knowledge of CD capabilities provided by enterprise CD services, CDS baseline list, and CD technologies listed within the CD capabilities portfolio. The CDSE will identify enterprise CD services or CDS baseline list capability gaps to the UCDSMO.

c. Coordinates the DoD Component's CD related security control assessment and authorization activities.

d. Participates in applicable UCDSMO and DoD CD forums (e.g. CDTAB, tiger teams, working groups) to represent DoD Component CD needs.

e. Maintains awareness of the Component's CD capability requirements and deployed CDSs in support of operations, exercises, RDT&E, or M&S.

f. Provides supported organizations with documentation and guidance on procedures and documentation required to perform RMF processes.

g. Provides CD support to Combatant Commands and other organizations in accordance with support agreements. Support to Combatant Commands will be in accordance with DoDD 5100.03 (Reference (ao)) and Reference (w).

h. Supports DoD Component CD planning efforts.

(1) Coordinates modernization planning for CDS sunset list CDSs with CDS IS owners in accordance with Reference (x) and DoD Component processes.

(2) Supports DoD Component planning for use of CDSs in support of operations, exercises, and RDT&E including M&S.

i. Oversees the management of the DoD Component's CD capability requirements.

(1) Conducts analysis of DoD Component requirements, and advocates those requirements within the DoD Component's overall requirements process.

(2) Supports analysis of CDS alternatives for DoD Component requirements.

(3) Submits CDTAB agenda requests, as required.

(4) Tracks and assesses requirements that have not been met and revalidates those requirements as necessary.

(5) Prioritizes CD capability requirements in coordination with the IS owner and information owner. Priority will be based on the mission impact to the readiness and ability to execute specific assigned missions by the requesting organization if a CDS is not provided.

(6) Maintains a prioritized list of DoD Component unsatisfied CD requirements (e.g., unavailable technology).

(7) Ensures that new CD technologies are compatible with the DoD Component's overall enterprise architecture and existing DoD Component ISs, as appropriate.

j. Monitors the acquisition and life cycle management of DoD Component CDSs.

(1) Oversees DoD Component security testing, evaluation, and implementation of CDSs (e.g., CDS implementation of security relevant configurations and site assessment plan) in accordance with this instruction.

(2) Enters and updates, as required, CDSs operational data, to include updates and patches for CDSs, via the designated centralized repository, currently the SGS at https://giap.disa.smil.mil/.

(3) Ensures that any new CD-related technology acquisition program development activities are coordinated with the UCDSMO before initiation.

(4) Requests security control assessments of new CD technologies to verify and validate their functionality and compliance with the security requirements, as needed.

(5) Ensures new CD technologies that complete verification and validation of functionality and security requirements are proposed for listing in the CDS baseline list.

(6) Supports the IS owner in the development of software, detailed design documents, test plans and procedures, and user documentation, as required.

(7) Coordinates with UCDSMO to arrange for a certified laboratory to conduct a DoD Component CD technology security control assessment, as required.

k. Monitors CDS assessments and inspections.

(1) Monitors and tracks assessments, inspections, and resulting findings.

(2) Recommends courses of action in response to assessment and inspection results, if required.

(3) In coordination with the information owner and IS owner, performs the risk rating activities as defined in the risk assessment process to obtain a CDS connection decision.

(4) Coordinates annual CDS revalidation and vulnerability self-assessments with DoD Component IS owners. The revalidation memorandum must identify a continued mission requirement, confirm the security relevant configuration is unchanged, confirm that an enterprise service or enterprise-hosted CDS site cannot support the CD requirement based on the DoD Component's annual validation of the CD requirement, and provide a statement of security self-assessment.

5. CD SERVICE PROVIDER. The CD service provider:

a. Provides enterprise CD services listed in the UCDSMO capabilities portfolio for DoD Components. Some of these services may be on a fee-for-service basis.

(1) Identifies and publishes enterprise CD services available as part of basic information network subscription services at least annually or when changes occur.

(2) Identifies and provides DoD Components and UCDSMO with available additional levels of enterprise CD services and rates.

(3) Develops standard service level agreements (SLAs) or support agreements for enterprise CD services.

(4) Ensures enterprise CD services provided for use by multiple DoD Components are compliant with the CDS baseline and sunset lists, and other CD guidance.

b. Provides hosted CDSs to DoD Components in accordance with a support agreement or SLA.

c. Implements and maintains required security controls for operating CDSs and for the CDS environment in accordance with the CD security control overlay and direction from USSTRATCOM orders or directives (e.g., vulnerability alerts or tasking orders).

d. Incorporates new CD capability requirements into enterprise CD services or hosted CDSs, as required.

e. Conducts site security control assessments of enterprise CD services or enterprise-hosted CDS sites to assess implemented Reference (y) security controls, the Reference (y) CDS overlay, and Reference (am). Site security control assessment schedule must be coordinated with supporting CDSE.

6. SCA. There are three security control assessment roles related to CDSs.

a. CD technology SCA. This role is assigned to a DoD SCA organization conducting security control assessments of CD technologies, which must be evaluated by the NSA in accordance with UCDSMO established criteria. The CD technology SCA:

(1) Conducts CD technology security control assessments to test effectiveness of the CD technologies and verify and validate the CD technology implements required functionality and security requirements for placement on the CDS baseline list.

(2) Provides status to the UCDSMO on the capacity to conduct CD technology security control assessments in support of DoD test and evaluation requirements.

(3) Conducts or provides security control assessment support. The security assessment support may be provided to organizations within the DoD Component or to external organizations on a fee-for-service basis in accordance with the DoD Component's guidance and a support agreement (e.g., a MOA).

(4) Prepares the security control assessment package for the CD technology including:

(a) A SCA statement that comprehensive review, analysis, and tests were performed, and confirm (i.e., verify) that the requirements are correctly defined and that the CD technology correctly implements required functionality and security requirements.

(b) SAR.

(c) Inventory and installation procedures.

(d) Security test procedures.

(5) Documents the issues, findings, and recommendations.

(6) Ensures required security control assessment documentation is complete in accordance with Reference (am) and available for review by the CDTAB.

b. Penetration Tester. The penetration tester, in coordination with the CD technology SCA, conducts penetration testing of the CD technology, to search for vulnerabilities, examine source code for best practices, and attempt to subvert the protection mechanisms of the CD technology.

c. Site SCA. The site security control assessment is conducted in coordination with the CDSE. The site SCA:

(1) Uses the RMF process to validate selected security controls as part of the site security control assessment of CDSs and CD technologies in accordance with References (b), (y), and (am).

(2) Supports the DoD Component risk assessment by providing SAR in accordance with Reference (b).

7. AO. The AO:

a. Authorizes a CDS to operate, based on the implementation of an agreed set of security controls and acceptance of risk to organizational operations. This authorization is required before requesting a CDSA to access or transfer information between different interconnected security domains in accordance with Reference (b) and this instruction.

b. The AO or designated representative ensures RMF tasks and risk assessment tasks are completed by trained and qualified personnel with documentation in accordance with Reference (b).

c. The AO or AO designated representative is responsible for the oversight of the IS. Only an AO can authorize the operation of the IS.

8. IS OWNER. The IS owner:

a. Contacts their DoD Component CDSE before contacting or obligating their organization to the acquisition of CDSs, CD technologies, or services.

b. Provides information required by supporting SCAs conducting CD technology or site security control assessments.

c. Deploys an IS with a CDS component under their authority in accordance with Reference (b), this instruction, and their DoD Component's guidance.

d. Completes a CDA during the RMF process in coordination with the information owner and CDSE.

e. Operates the CDS in accordance with the CDSA in coordination with the network service provider.

f. Ensures that information that is not owned by DoD, but is hosted on DoD IS, complies with the Information Owner requirements in section 9 of this enclosure.

g. Conducts defensive actions and protective measures in coordination with the supporting cybersecurity service provider organization for the CDS and CDS environment in accordance with Reference (c) and USSTRATCOM orders and directives (e.g., alerts or tasking orders).

h. Ensures the CDSE has current and accurate information on ISs and CDS points of contact to enable the CDSE to update the designated repository.

i. Provides life cycle information in coordination with the information owner annually, or as required, to the DoD Component designated organization or in accordance with Reference (x).

j. Supports the DoD Component CDS risk assessment by providing the level of impact (i.e., harm) to the organization due to a threat event causing loss of CDS availability consistent with Reference (u).

k. Directs a periodic self-assessment be conducted to assess the protection mechanisms and security controls implemented to protect CD activities. The assessment will:

(1) Review the security relevant configuration, operation, and administration of the CDS in its operational environment.

(2) Verify that the CDS is utilized per the approved security relevant configuration and documentation requirements.

(3) Identify possible security vulnerabilities.

(4) Document findings in an assessment report and updated IS POA&M to support annual CDSA revalidation.

l. Validate CD requirements and, if operating a DoD Component point-to-point CDS, validate that an enterprise service or enterprise-hosted site cannot support CD requirements.

9. INFORMATION OWNER. The information owner:

a. Provides the information description for the CD capability requirement, to include data types, file extensions, and support of structured and unstructured data in the CDA.

b. Provides specification for data information flow in coordination with the IS owner to include source and destination IS classifications, data flow (e.g., high to low, low to high), data

structure and parameters, any CDS filtering of data, transfer protocol requirements, and throughput required.

c. Provides annual validation of mission needs through the appropriate AO to the CDSE.

d. Provides guidance to content originators on information required marking, dissemination, and metadata (e.g., binary, text, image, voice, or video) in accordance with DoDI 8320.02 (Reference (ap)) and Volume 2 of Reference (i).

e. Coordinates with the IS owner to support the DoD Component CDS risk assessment by providing the level of impact (i.e. harm) to the organization due to a threat event causing an unauthorized disclosure, unauthorized modification, unauthorized destruction, or the loss information in support of DoD Component CDS risk assessment consistent with Reference (u).

10. ISSM. The ISSM will carry out cybersecurity and RMF responsibilities in accordance with References (b) and (c).

11. ISSO. The ISSO will carry out cybersecurity and RMF responsibilities for the CDS in accordance with References (b) and (c).

12. ISSE. The ISSE:

a. Develops and implements IS security based on the selected security controls and security requirements.

b. Formulates security architecture recommendations, and designs security services.

c. Recommends and coordinates the application of fixes, patches, and disaster recovery procedures in the event of a security breach.

d. Researches emerging technologies to support security enhancement and development efforts.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AO	authorizing official
BOE	body of evidence
CD	cross domain
CDA	Cross Domain Appendix
CDRUSSTRATCOM	Commander, U.S. Strategic Command
CDS	cross domain solution
CDSA	Cross Domain Solution Authorization
CDSE	Cross Domain support element
CDTAB	Cross Domain Technical Advisory Board
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CNSSI	Committee on National Security Systems instruction
CNSSP	Committee on National Security Systems Policy
DIA	Defense Intelligence Agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DNI	Director of National Intelligence
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DODIN	DoD information networks
DSAWG	Defense/IA Security Accreditation Working Group
ECDSP	enterprise CD service provider
IA	information assurance
IC	Intelligence Community

IS	information system
ISRMC	Information Security Risk Management Committee
ISSE	information systems security engineer
ISSM	information systems security manager
ISSO	information systems security officer
JWICS	Joint Worldwide Intelligence Communications System
M&S	modeling and simulation
MOA	memorandum of agreement
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PII	personally identifiable information
POA&M	plan of action and milestones
RDT&E	research, development, test, and evaluation
RHR	reliable human review
RMF	Risk Management Framework
SAR	security assessment report
SCA	security control assessor
SCI	sensitive compartmented information
SDLC	system development life cycle
SGS	SECRET Internet Protocol Router Network Global Information Grid Interconnection Approval Process System
SISO	senior information security officer
SLA	service level agreement
SP	security plan
TOE	Target of Evaluation
TS	Top Secret
UCDSMO	Unified Cross Domain Services Management Office
USD(I)	Under Secretary of Defense for Intelligence

USD(P)	Under Secretary of Defense for Policy
USSTRATCOM	U.S. Strategic Command

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this instruction.

access CDS. A type of CDS that provides access to a computing platform, application, or data residing on different security domains from a single device without any transfer between the various domain.

adequate security. Defined in CNSSI No. 4009 (Reference (aq)).

AO. Defined in Reference (aq).

AO designated representative. Defined in Reference (aq).

authorization. Defined in Reference (aq).

authorization boundary. Defined in Reference (aq).

BOE. The set of artifacts that the DoD uses to support assessment and authorization of a CDS.

cascading. The downward flow of information through a range of security levels greater than the accreditation range of a system, network, or component without passing through an isolated device that implements the enforcement of all applicable approved policy decisions for each domain transfer.

CD capabilities. Defined in Reference (aq).

CD service. A service that provides access or transfer of information solutions between different security domains.

CD technology. Hardware or software used to provide a CDS.

CDS. Defined in Reference (aq).

CDS baseline list. A list managed by the UCDSMO that identifies CDSs that are available for deployment within the DoD and IC.

CDS filtering. The process of inspecting data as it traverses a CDS and determines if the data meets pre-defined policy.

CDS sunset list. A list managed by the UCDSMO that identifies CDSs that are or have been in operation, but are no longer available for additional deployment and need to be replaced within a specified period of time.

CDSA. A risk decision by the DoD risk executive to authorize the use of a CDS to access or transfer information between different interconnected security domains.

chaining. Direct or relayed connections from a higher accredited domain to a series of lower accredited domains after passing through an isolated device that implements the enforcement of all applicable approved policy decisions for each domain transfer.

common control. Defined in Reference (aq).

controlled interface. Defined in Reference (aq).

continuous monitoring. Defined in Reference (al).

controlling domain. The domain that assumes the greater risk and thus enforces the most restrictive policy.

countermeasures. Defined in Reference (aq).

cybersecurity. Defined in Reference (c).

data flow. The movement of data between source and destination and the path traversed.

data transfer solution. Interconnect networks or information systems that operate in different security domains and transfer data between them.

DISN. Integrated network centrally managed and configured to provide long-haul information transfer services for all DoD activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services.

ECDSP. An organization that establishes, manages, and maintains the overall infrastructure and security posture offering automated capabilities to users and applications within an enterprise environment for information sharing across and among security domains.

enterprise CD service. Automated capabilities available to end users and hosted mission applications within an enterprise environment for information sharing across and among security domains utilizing one or more CDSs.

enterprise hosted CDS. A point-to-point CDS that is managed by an ECDSP that may be available to additional users within the enterprise with little or no modifications.

information owner. Defined in Reference (aq).

IS. Defined in Reference (aq).

IS owner. Defined in Reference (aq).

ISSE. Defined in Reference (aq).

ISSM. Defined in Reference (aq).

ISSO. Defined in Reference (aq).

memorandum of agreement. Defined in Reference (aq).

mission partner. Defined in Reference (l).

multi-level solution. A technical implementation of multilevel security.

multilevel security. Defined in Reference (aq).

network. Defined in Reference (aq).

overlay. Defined in Reference (y).

penetration testing. Defined in Reference (aq).

PII. Defined in Reference (aq).

POA&M. Defined in Reference (aq).

reciprocity. Defined in Reference (aq).

Red Team. Defined in Reference (aq).

removable media. Defined in Reference (aq).

RHR. A review of information/data intended for transfer (high to low) across security domains that is performed by an individual with knowledge of the subject matter. The goal is to validate that the information/data being transferred meets criteria set forth by the relevant security policy.

risk. Defined in Reference (aq).

risk assessment. Defined in Reference (aq).

risk assessment methodology. A risk assessment process, together with a risk model, assessment approach, and analysis approach.

risk executive. Defined in Reference (aq).

risk management. Defined in Reference (aq).

risk mitigation. Defined in Reference (aq).

risk model. The component of a risk methodology that defines key terms and assessable risk factors.

RMF. Defined in Reference (aq).

safeguards. Defined in Reference (aj).

SAR. A documents assessment that results in sufficient detail to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements.

security control assessment. Defined in Reference (aq).

security control assessor. Defined in Reference (aj).

security control enhancements. Defined in Reference (aq).

security controls. Defined in Reference (aq).

security domain. Defined in Reference (aq).

security plan. Defined in Reference (aj).

security posture. Defined in Reference (aq).

security policy. Defined in Reference (aq).

security requirements. Defined in Reference (aq).

senior information security officer. Defined in Reference (aq).

service level agreement. Defined in Reference (aq).

service provider. Organization that provides some types of communications, storage, processing, or content service or any combination thereof.

special access program. Defined in Reference (aq).

tailoring. Defined in Reference (aj).

Target of Evaluation. Defined in Reference (aq).

threat. Defined in Reference (aq).

threat event. Event or situation that has the potential for causing undesirable consequences or impact.

transfer CDS. A type of CDS that enforces security policy for the movement of data between information systems operating in different security domains.

tunneling. Defined in Reference (aq).

unauthorized disclosure. Defined in Reference (aq).

user. Defined in Reference (aq).

validation. Defined in Reference (aq).

verification. Defined in Reference (aq).

vulnerability. Defined in Reference (aq).

vulnerability assessment. Defined in Reference (aq).