Department of the Army
Pamphlet 25–2–1

Information Management: Army Cybersecurity

Army Cross Domain Solution and Data Transfer Management

Headquarters
Department of the Army
Washington, DC
12 April 2019

UNCLASSIFIED

SUMMARY

DA PAM 25–2–1
Army Cross Domain Solution and Data Transfer Management

This administrative revision, dated 31 May 2019—

- Corrects the e-mail address (title page).

This new publication, dated 12 April 2019--

- Provides guidance on cross domain approval processes and procedures, relating to the connection of a cross domain solution between differing security domains, for Army cross domain solution customers (chaps 1, 2, and 5).

- Contains instructions for Army organizations to effectively acquire cross domain solution capabilities (chap 3).

- Provides the procedures required for manual data transfers across security domains, when access to a cross domain solution is not available and using removable media is required for the mission (chap 4 and para 5–4).

Headquarters
Department of the Army
Washington, DC
12 April 2019

Department of the Army Pamphlet 25–2–1

Information Management: Army Cybersecurity

Army Cross Domain Solution and Data Transfer Management

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is a new Department of the Army pamphlet.

Summary. This pamphlet provides guidance for assessing, approving, acquiring, and using cross domain solutions within the Department of the Army. It supports AR 25–2 and Army cybersecurity. This pamphlet provides amplifying procedures and guidance for AR 25–2.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent for this pamphlet is the Army Chief Information Officer/G–6. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Office of the Army Chief Information Officer/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107 (email: usarmy.pentagon.hqda-cio-g-6.mbx.policy-inbox@mail.mil).

Distribution. This pamphlet is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Contents—Continued

Chapter 1
Introduction

1–1. Purpose
The Army Cross Domain Management Office (CDMO), within the Cybersecurity Directorate of the Chief Information Officer (CIO)/G–6, Army, sets the guidance for this Department of the Army (DA) pamphlet (Pam). The Army CDMO is the cross domain support element (CDSE) for the Army, and provides cross domain solution (CDS) oversight at the Headquarters, Department of the Army (HQDA) level. This DA Pam provides guidance on cross domain approval processes, and procedures, on how to connect a CDS between differing security domains. It also helps Army organizations to obtain CDS capabilities effectively and efficiently, and to steer manual data transfers across security domains, when a CDS is not available.

1–2. References
See appendix A.

1–3. Explanation of abbreviations and terms
See the glossary.

1–4. Applicability
a. The procedures in this DA Pam will help protect classified and sensitive Army information from unauthorized disclosure–inadvertent or intentional–caused by improper methods of conducting data transfers across security domains. It also provides cybersecurity CDS guidance to protect classified networks from potential malicious intent by use of a CDS. Further, it applies to all Army secret and below interoperability (SABI) CDSs governed by the Department of Defense (DOD) connection approval process, and managed by the Army HQDA CIO/G–6 Cybersecurity Directorate. The HQDA CIO/G–6 Special Access Programs (SAP) Office processes CDS connections involving SAPs. (See contact information for the Army SAP office in para 5–1.)

b. This document does not authorize declassification or downgrading the classification of information, but reduces the inherent technical risks of data transfer. The original classification authority conducts information declassification and downgrading. This document is not applicable for the Joint Worldwide Intelligence Communications System (JWICS) or for top secret–sensitive compartmented information (TS–SCI). (See contact information for Army CDS involving JWICS or TS–SCI data in para 5–1.)

c. This document does not address the specific procedures required while handling removable media. Find additional information and guidance for specific processes and procedures regarding removable media in DA Pam 25–2–4.

Chapter 2
Cross Domain Solution Overview

2–1. Background
a. A security domain is a system or network, operating at a particular sensitivity level, which implements a security policy and is administered by a single authority.

b. A CDS is a form of controlled interface that provides the ability to manually or automatically access or transfer information between different security domains.

(1) *Access cross domain solution.* A type of CDS that gives users access to a computing platform, application, or data residing in different security domains from a single device, without any transfer between the various domains.

(2) *Transfer cross domain solution.* A type of CDS that enforces security policy when moving data between information systems that operate in different security domains.

(3) *Multi-level cross domain solution.* A type of CDS that uses trusted labeling to store data at different classifications and allows users to access the data based upon their security domain and credentials.

(4) *Cross domain service.* A cross domain (CD) service provides access, or transfer of information solutions, between different security domains.

c. Figure 2–1 represents an Army CDS and security domain structure. Security domain "A" represents an unclassified network such as the Non-Classified Internet Protocol Router Network (NIPRNet), and "B" represents a classified network such as the Secret Internet Protocol Router Network (SIPRNet).

d. The act of manually or automatically accessing and transferring information between different security domains requires the use of specific procedures and processes to mitigate the risks involved with the activity. Malware can be inadvertently transferred between systems when connecting two security domains. Another risk during data transfer from classified systems is unauthorized disclosure of classified information (UDCI). Follow data transfer procedures to mitigate these risks to ensure data integrity and to prevent data UDCI incidents.

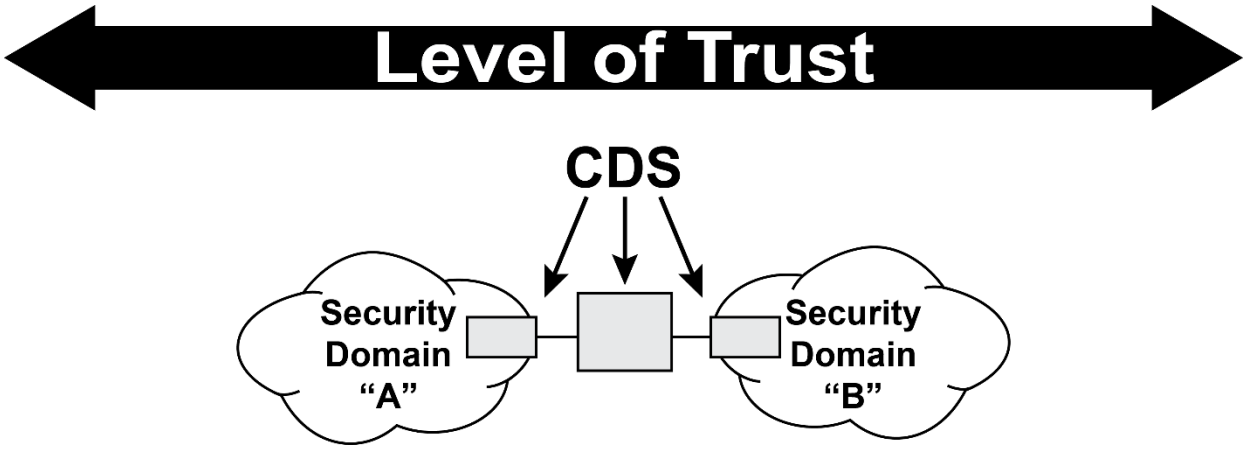

Figure 2–1. Army Cross Domain Solution and Security Domain Structure

Chapter 3
Cross Domain Solution Approval Process

3–1. Cross domain management

a. Information system owners (ISOs) must contact the Army CDMO as soon as a cross domain requirement is identified. The ISO will submit CDS requirements, or will designate a representative to submit CDS requirements, through their respective organization and program information system security managers (ISSMs), to the Army CDMO. (See contact information for the Army CDMO in para 5–1*a*.)

b. Organizations must not commit any resources, neither funding nor technical, prior to beginning CDS coordination with the Army CDMO. Early engagement is essential to meet schedule requirements. The Army CDMO is the focal point for implementing all Army SABI CDSs.

c. Organizations requiring a CDS must not acquire or procure CDS technology until their connection requirement is approved by the Defense Security/Cybersecurity Authorization Working Group (DSAWG).

d. The Army CDMO provides the following support related to the DOD connection approval process for SABI CDSs:

(1) Requirements validation.

(2) CDS technology identification.

(3) Review of authorization documentation and requirements.

(4) Coordination with DOD agencies.

(5) Army sponsorship at CDS approval boards and/or panels.

e. Do not procure CDS technology before DOD-level validation of the cross domain requirement, coordinated by the Army CDMO. The Army CDMO, in coordination with the Cross Domain Technical Advisory Board and DSAWG, will determine if the requirement can be met by the Defense Information Systems Agency (DISA) Cross Domain Enterprise Service (CDES). When applicable, the DISA CDES is the preferred method of implementing a CDS within a network.

f. If the requirement cannot be met by the DISA CDES, the capability requirement must be met by a technology listed on the Unified Cross Domain Services Management Office (UCDSMO) Baseline.

g. If the designated CDS is not listed on the UCDSMO Baseline, or if approved technologies do not meet the capability requirements for a mission, a modified CDS or new technology will be developed to meet mission requirements in accordance with DOD Instruction (DODI) 8540.01. The modified or new technology will be required to undergo a lab-based security assessment (previously known as certification test and evaluation (CT&E)), and will be assessed by the security control assessor for functionality and security requirements.

3–2. Cross domain solution approval process

The DOD Global Information Grid Inter-connection Approval Process was created to provide a consistent way to simplify and consolidate the various connection approval processes. When connecting networks of different security domains all DOD Services and agencies must comply with the policies and processes in accordance with DODI 8540.01, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02D, and Appendix H of the Defense Information Systems Network (DISN) Connection Process Guide (CPG) 5.1. The CDS process provides an integrated, comprehensive, and consistent approach to addressing the shared-risk associated with the connection of networks of different security domains. The step-by-step connection approval process for SABI CDS is documented in the DISN CPG 5.1 Appendix H.

a. The Army Communications-Electronics Research, Development, and Engineering Center (CERDEC) will perform CDS risk assessments and develop risk ratings on a fee-for-service basis in accordance with the CIO/G–6 memorandum, dated 9 June 2014 (Notification of Change in Service of SABI CDS Risk Assessments). Contact the Army CDMO for coordination with CERDEC regarding pricing information.

b. All Army organizations that maintain connections between networks of different security domains must revalidate their CD connections annually in accordance with DODI 8540.01, CJCSI 6211.02D, and DISN CPG 5.1 Appendix H. Army CDMO will provide the necessary templates and documentation when an annual review is required.

3–3. Supporting documentation

Each supporting CD document should be developed by the appropriate owner as identified and defined by the roles and responsibilities outlined in DODI 8540.01 and the DISN CPG 5.1. With guidance from the Army CDMO, the following documentation will be developed throughout the SABI CDS process.

a. A cross domain validation and approval request identifies the CDS mission and cross domain requirements.

b. The cross domain appendix (CDA) is the source of technical information for risk analysis with a detailed description of the requirement, data types, proposed solution, and interconnected partners. It is updated and expanded throughout the CDS approval process and signed by the authorizing official (AO). The completed CDA may be classified, and must be uploaded to the classified DOD CDS database by the Army CDMO.

c. The site-based security assessment plan (previously known as security test and evaluation (ST&E plan)) provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment.

d. The security assessment report (SAR) provides 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. The SAR associated with CDSs may include results from both site- and lab-based security assessments.

e. Each CDS technology has its own unique list of configuration and security policy files, which CERDEC must evaluate to determine a risk rating. Each new or updated version of a CDS technology may be required to undergo a lab-based security assessment (previously known as CT&E) prior to gaining UCDSMO baseline approval.

f. The cross domain solution authorization (CDSA), issued by DISA, is a risk decision by the DOD risk executive (such as DOD Information Security Risk Management Committee or DSAWG on its behalf) to authorize the use of a CDS to access or transfer information between different interconnected security domains.

g. The CDS annual review memorandum revalidates the operational requirement and approved configuration of CDS.

Chapter 4
Data Transfers Across Security Domains

4–1. Manual data transfer requirements

a. The intent of data transfer guidance is to balance the risk of inadvertent data exposure with the need to move redacted or sanitized information quickly from one domain to another. Trained personnel and the use of automated tools to review and redact information are critical to minimize the amount of time and effort required, and increase the level of confidence in the releasable product.

b. All removable media are prohibited from use on all SIPRNet servers, systems, and stand-alone workstations unless specifically authorized by the AO. However, individuals within an organization may be approved, due to a critical mission need, to perform manual data transfers across security domains, using approved removable media, due to the unavailability of an automated CDS. Note: This DA pamphlet does not address the specific procedures required while handling removable media. Additional information and guidance for specific processes and procedures regarding removable media are found in DA Pam 25–2–4.

c. The AO will determine the acceptable use and approval process for the use of removable media devices to be included in Network User Training programs.

d. The ISSM will issue a data transfer agent (DTA) authorization only after the user(s) have demonstrated hands-on performance in hidden data removal, data transfer, and UDCI incident procedures appropriate for their environment. The AO will provide a written authorization to the unit's ISSM for each authorized user appointed to use removable media on SIPRNet infrastructure, which includes the full name, rank/grade, and Social Security number or personal identification number of the authorized individual. The AO will also provide a written authorization for each server, system, and stand-alone workstation approved to use removable media.

e. The DTA is an inherently privileged user who is authorized to perform security-relevant functions and who maintains special access to transferring information. The DTA is therefore required to comply with the appointed information assurance training certification-level requirements in accordance with DOD 8570.01–M, USARCYBER OPORD 2016–033, and DA Pam 25–2–7.

f. The DTA must comply with the site AO's user agreement rules for conducting data transfers on SIPRNet and must have written approval from the AO prior to conducting any data transfer on SIPRNet. DTAs must provide physical protection of removable media devices.

g. All approved DTAs must maintain data transfer records (as evidence) for all data removed from a SIPRNet machine and must report these records monthly to the ISSM.

h. The DTA must only use removable media in compliance with the processes and procedures provided by the AO.

i. The AO will develop procedures to conduct semi-annual random and periodic inspections of data transfers and sites authorized to use removable media devices to ensure transfers comply with the proper procedures. In addition, the AO must maintain and retain logs as evidence that inspections occurred and report findings up the chain of command. Reviews must be integrated into Command Inspection Programs.

j. All data being transferred from top secret networks or non-DOD networks to SIPRNet are scanned using the National Security Agency's File Sanitization Tool (FiST), later dubbed "XD-Air."

k. Data transfer across security domains at contractor facilities is prohibited. Any contracting agency requiring data transfer across security domains must do so through a government controlled and DTA-authorized facility.

4–2. Required documentation

a. Following any violation of the acceptable use policy implemented by the AO, the processes and procedures employed must be investigated.

b. All DTAs must complete and sign a nondisclosure agreement and privileged access agreement, which must also be signed by the ISSM. User agreements and proof of mandatory training requirements must be uploaded to the Army Training and Certification Tracking System (ATCTS). The data transfer privileges of each individual DTA will be reviewed quarterly to ensure privileges are still necessary and up to date.

c. Commanders, ISSMs, and DTAs must ensure a UDCI incident response plan is prepared and rehearsed in all areas where data transfer solutions are permitted, and that all users are aware of incident handling and reporting requirements. Timely response and notification is critical to minimize the effects of any incidental UDCI.

d. The AO and ISSM must maintain a record of all personnel and systems that are authorized to use removable media devices on SIPRNet within their environment. The AO and ISSM must state that individuals are trained and are proficient in accomplishing the transfer process in a memorandum or equivalent documentation.

e. Each time a transfer is accomplished, accountability and nonrepudiation are critical. DTAs must request a read receipt verifying only the intended recipient has received the transferred data, and DTAs must send a read receipt to the data owner when files are received from top secret network sources.

f. Each individual data transfer using removable media in lieu of a CDS must be formally authorized, documented, and logged by the AO. Data transfer events will be documented by the AO or DTA in a memorandum or log entry that identifies the transfer. Log and include the following information in an enclosure with the memorandum or log entry, and include two person integrity procedures to reduce the potential for insider threat:

(1) Identification of the authority and reason for the release of the information.

(2) Time and date of redaction and method of transmission.

(3) Destination network or resource to which the information was intended.

(4) The point of contact (POC) information of the DTA executing the procedures and verifying results.

(5) File-specific information for each file transferred must be captured to include the file size and file name and extension.

g. Every data transfer that is performed must be recorded and the status be reported to the ISSM and AO every 30 days.

h. The redacted or converted files will include an enclosure citing the redaction or cleansing action in the format of the native file. A new text file will be added with the redaction or sanitization enclosure and will identify the appropriate authority POC if the enclosure cannot be included in the native format.

4–3. Transition guidelines

a. After the transfer of the redacted data to the removable media is complete, review the contents on a stand-alone machine that has up-to-date virus definition files and is cleared for the classification level of the originating security domain that designates where the data is transferred from.

b. Use standard media colors or labels that match the classification level of the data transferred per the existing classification marking schema, in accordance with the proper Standard Form (SF). Removable media that are pre-authorized and approved by the ISSM will be used when transferring data.

c. Destroy removable media in accordance with the highest classification of the system the media was inserted into. The supplemental Army instructions and official rules for use of removable media on DOD systems can be found in DA Pam 25–2–4.

4–4. Automated services available for data transfer across security domains

a. The following is a list of automated cross-domain services that are available for manual cross-domain transfers across the DOD. Further information regarding each of these services are available on the listed website for each service provider.

b. Pair the following tools with reliable human review (RHR), which is the practice of examining a file's content, ensuring it contains only the appropriate information, and determining whether the file is properly classified.

(1) The Intelshare SharePoint Assured File Exchange (SAFE) provides one-way transfer capability between unclassified networks to SIPRNet via SharePoint. https://intelshare.intelink.gov/sites/u-safesource/. (Note: Intelshare SAFE should not be confused with the U.S. Army Aviation and Missile Research Development and Engineering Center SAFE application, which provides encrypted file drop and pick up service on NIPRNet only.)

(2) The Intelink Global Information Data Exchange (Glide) One-Way Transfer (OWT) provides one-way transfer capability between networks of lower classification to higher classification via the Glide user interface. It transfers from unclassified to SIPRNet, from unclassified to top secret, and from secret to top secret (https://glide.intelink.gov).

(3) The Defense Intelligence Agency's Department of Defense Intelligence Information System (DODIIS) One Way Transfer Service (DOTS) provides one-way transfer of documents between networks of lower classification to higher classification. It transfers from unclassified to SIPRNet, from unclassified to top secret, and from secret to top secret (https://dots.dodiis.mil).

4–5. Manual data transfer services across security domains

a. The products named in paragraphs 4–5*b*(1) through 4–5*b*(5) are used within the DOD and the intelligence community, and are the authorized tools for the Army to use when conducting manual secure data transfers. The user guides, product support, and POC information is listed on the individual product websites.

b. These tools do not determine if a file is properly classified. The authors and reviewers in the RHR process are ultimately responsible for determining whether a file is appropriately classified. Users are required to follow the site security policy, regarding RHR processes for reviewing files, and cross-domain transfer policy and procedures for transferring files.

(1) The File Sanitation Tool (FiST), later dubbed "XD Air," is a laptop kiosk that reads content from removable media. It also scans for viruses, performs a deep content inspection, clean/dirty word search, and scans for hidden content. Only "known good" files that pass inspection are written to clean media, while files that do not pass the security scan are omitted to avoid data leakage or infection. Visit http://www.tresys.com/products/xd-air.php.

(2) The COMPUSEC Toolbox suite of security applications is maintained by the 25th Air Force for manually transferring data between different security domains. Obtain support information from the Joint voice over Internet Protocol (JVOIP)/Defense Information Systems Network Satellite Transmission Services-Global (DSTS–G) at 977–6035, afisra.a6se@us.af.mil.

(3) The Department of the Army Intelligence Information Services (DAIIS) File Transfer Service provides 24-hour multidirectional, cross domain file transfer service. This service supports defined Joint Task Force intelligence mission requirements. This service also supports high-to-low and low-to-high transfers on NIPRNet, SIPRNet, JWICS, NSANet, CENTRIXS–SWA/ISAF, CENTRIXS–KOREA, Battlefield Information Collection and Exploitation System (BICES), and Stone Ghost networks. Contact the DAIIS Intelligence Support Center for more information at (703) 706–2430, DSN (312) 235–2430, SVOIP (302) 235–431–2430, or JVOIP/NSTS 964–2430.

(4) The Army data auditing manager (ADAM) tracks and audits the request and approval of all authorized data transfers from and to the Army Military Intelligence SIPRNet domain and Army JWICS/DODIIS non-cryptologic systems. Additionally, ADAM is used to request and approve data transfer agents, data transfer workstations, and approving authorities. ADAM is hosted and maintained by DAIIS, and mandated by the Deputy Chief of Staff, G–2. Contact the DAIIS Intelligence Support Center for more information at (703) 706–2430, DSN (312) 235–2430, SVOIP (302) 235–431–2430, or JVOIP/NSTS 964–2430, email address: usarmy.belvoir.inscom.mbx.portal-feedback@mail.smil.mil.

Chapter 5
Additional Cross Domain Solution Resources

5–1. Points of Contact

a. HQDA CIO/G–6 Cybersecurity Directorate:
Army Cross Domain Management Office
NIPRNet: usarmy.pentagon.hqda.list.cio-g6-cdmo@mail.mil
SIPRNet: usarmy.pentagon.hqda-cio-g-6.mbx.cdmo@mail.smil.mil
Telephone: (703) 545–4239; DSN 865
https://informationassurance.us.army.mil

b. HQDA CIO/G–6 Special Access Programs Office:
Telephone: (703) 545–1877; DSN 865

c. HQDA Office of the Deputy Chief of Staff G–2 Cybersecurity Division, DAMI–IM:
NIPRNet: usarmy.pentagon.hqda-dcs-g-2.mbx.ia-division@mail.mil
SIPRNet: usarmy.pentagon.hqda-dcs-g-2.mbx.ia-division@mail.smil.mil
Telephone: (703) 695–0893/2271/0609; DSN 865

5–2. Online resources

a. DISA Enterprise Connections webpage: http://www.disa.mil/network-services/enterprise-connections/mission-partner-training-program/cds-101/.

b. CDS 101 training for CDS computer based training: http://www.disa.mil/_flash_files/cds101.swf/.

5–3. Technical assistance

Technical assistance in the following areas may be available to Army CDS customers on a fee-for-service basis from CERDEC (contact Army CDMO for coordination):

a. Technology selection.

b. Documentation preparation.

c. Accreditation support.

5–4. Computer-based training

Computer-based training is required for authorized personnel that perform and oversee automatic and manual transfers across security domains. The following training courses provide guidance for protecting sensitive information in government systems:.

a. Identifying and Safeguarding Personally Identifiable Information (PII) training is available at http://iatraining.disa.mil/eta/piiv2/launchpage.htm/.

b. Portable Electronic Devices/Removable Storage Media training is available at http://iatraining.disa.mil/eta/pedrm_v2/pedrm_v2/launchpage.htm/.

Appendix A

References

Section I

Required Publications

AR 25–2
Army Cybersecurity (Cited in the title page.)

CIO/G–6 Memorandum
Notification of Change in Service of Secret and Below Interoperability (SABI) Cross Domain Solution (CDS) Risk Assessments (Cited in para 3–2*a*.) (Available at https://www.milsuite.mil/.)

CJCSI 6211.02D
Defense Information Systems Network (DISN) Responsibilities (Cited in para 3–2.) (Available at http://www.jcs.mil/.)

DA Pam 25–2–4
Removable Media (Cited in para 1–4*c*.)

DA Pam 25–2–7
Army Information System Privileged Access Agreement and Non-Disclosure Agreement (Cited in para 4–1*e*.)

DISN CPG 5.1
Connection Process Guide (Cited in para 3–2.) (Available at http://disa.mil/.)

DODI 8540.01
Cross Domain (CD) Policy (Cited in para 3–1*g*.)

DOD 8570.01–M
Information Assurance Workforce Improvement Program (Cited in para 4–1*e*.)

USARCYBER OPORD 2016–033
Implementation of Updated Policy for the Documentation of Privileged Users (Cited in para 4–1*e*.) (Available at https://atc.us.army.mil/iastar/.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. DOD publications are available at https://www.esd.whs.mil/. USC material is available at http://uscode.house.gov/.

AR 25–1
Army Information Technology

AR 25–30
Army Publishing Program

AR 380–5
Department of the Army Information Security Program

CJCSI 6510.01F
Information Assurance (IA) and Support to Computer Network Defense (CND)

CNSSI 4009
National Information Assurance (IA) Glossary (Available at https://www. dni.gov/.)

CNSSP 15
National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information among National Security Systems (Available at https://www.cnss.gov/.)

DODI 8500.01
Cybersecurity

DODM 5200.01 Vol. 1
DOD Information Security Program: Overview, Classification, and Declassification

HQDA CIO/G–6 Memorandum
Privileged Access to Army Information Systems, Networks and Data (Available at https://atc.us.army.mil/iastar/.)

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) website (https://armypubs.army.mil).

DA Form 2028
Recommended changes to Publication and Blank Forms

Glossary

Section I

Abbreviations

ADAM
Army data auditing manager

AO
authorizing official

AR
Army regulation

ATCTS
Army Training and Certification Tracking System

BICESCBT
Battlefield Information Collection and Exploitation System

CBT
computer-based training

CD
cross domain

CDA
cross domain appendix

CDES
Cross Domain Enterprise Service

CDMO
Cross Domain Management Office

CDS
cross domain solution

CDSA
cross domain solution authorization

CDSE
cross domain support element

CERDEC
Communications-Electronics Research Development and Engineering Center

CIO
chief information officer

CJCSI
Chairman of the Joint Chiefs of Staff Instruction

CLEAR
Content Locator Examination Analysis and Reporting

CND
computer network defense

CPG
connection process guide

CT&E
certification test and evaluation

DA
Department of the Army

DAIIS
Department of the Army Intelligence Information Services

DISA
Defense Information Systems Agency

DISN
Defense Information Systems Network

DOD
Department of Defense

DODI
Department of Defense Instruction

DOTS
Department of Defense Intelligence Information System (DoDIIS) One Way Transfer Service

DSAWG
Defense Security/Cybersecurity Authorization Working Group

DSN
Defense Switched Network

DSTS–G
Defense Information Systems Network Satellite Transmission Services-Global

DTA
data transfer agent

FiST
File Sanitization Tool

Glide OWT
global information data exchange one-way transfer

HQDA
Headquarters, Department of the Army

IA
information assurance

ISO
information system owner

ISRMC
Information Security Risk Management Committee

ISSM
information system security manager

JVOIP
Joint voice over Internet Protocol

JWICS
Joint Worldwide Intelligence Communications System

NIPRNet
Non-classified Internet Protocol Router Network

OPORD
operational order

OWT
one-way transfer

Pam
pamphlet

POC
point of contact

RHR
reliable human review

SABI
secret and below interoperability

SAFE
SharePoint assured file exchange

SAP
special access program

SAR
security assessment report

SF
Standard Form

SIPRNet
Secret Internet Protocol Router Network

ST&E
security test and evaluation

TS–SCI
top secret/sensitive compartmented information

UCDSMO
Unified Cross Domain Services Management Office

UDCI
unauthorized disclosure of classified information

USARCYBER
U.S. Army Cyber Command

Section II

Terms

Access Cross Domain Solution
A type of cross domain solution that provides user access to a computing platform, application, or data residing of different security domains from a single device without any transfer between the various domains.

Authorizing official
A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Authorizing official designated representative
An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.

Cross domain
The act of manually and/or automatically accessing and/or transferring information between different security domains.

Cross domain appendix
The CDS document serving as a source of technical information for risk analysis with a detailed description of the requirement, data types and proposed solution. It is updated and expanded at each of the four phases of the CDA approval process and signed by the AO.

Cross domain baseline
A list managed by the unified cross domain services management office (UCDSMO) that identifies CDSs available for deployment within the DOD and Intelligence Community.

Cross domain capabilities
Set of functions that enable the transfer of information between security domains in accordance with the policies of the security domains involved.

Cross domain service
Services that provide access and/or transfer of information between different security domains.

Cross domain solution
Form of controlled interface that provides the ability to manually or automatically access or transfer information between different security domains.

Cross domain solution authorization
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.

Cross Domain Technical Advisory Board
Provides technological risk assessments of CDSs and inter-domain demilitarized zone security architectures to the DSAWG.

Cross Domain Validation and Approval Request
A document that identifies the CDS mission and data requirements, signed by the program's AO.

Data transfer agent
An individual that is authorized, trained, and appointed by authorized personnel to perform the data transfer process.

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

Defense Security/Cybersecurity Authorization Working Group
The community forum for reviewing and resolving access and authorization issues related to the sharing of community cybersecurity risk.

Domain
An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

Enterprise cross domain 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.

Information systems security manager
Individual responsible for the information assurance of a program, organization, system, or enclave.

Lab-based security assessment (previously known as certification test & evaluation (CT&E))
Software and hardware security tests conducted during development of an information system component.

Multi-level cross domain solution
A type of CDS that uses trusted labeling to store data at different classifications and allows users to access the data based upon their security domain and credentials

Privileged user
A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Reliable human review
A review of information/data intended for transfer 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.

Removable media
Portable data storage medium that can be added to or removed from a computer device or network.

Security assessment plan
Provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. A CDS Security Assessment Plan can contain a Site-Based Security Assessment and a Lab-Based Security Assessment.

Security assessment report
An assessment which 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. A CDS SAR can contain a Site-Based Security Assessment and a Lab-Based Security Assessment.

Security domain
A domain that implements a security policy and is administered by a single authority.

Site-based security assessment (previously known as security test & evaluation (ST&E))
Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of the system.

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

Section III

Special Abbreviations and Terms

CAO
connection approval office

CDTAB
Cross Domain Technical Advisory Board

CDVAR
Cross Domain Validation and Approval Request

CENTRIX
Combined Enterprise Regional Information Exchange System
(top secret sensitive compartmented information and below interoperability)

GIAP
Global Information Grid Inter-connection Approval Process