USD(R&E)

Fundamentals of Cross Domain Solutions (CDS)

US Department of Defense Perspective

Mr. Burhan Adam
Director, Systems Security Policy, Standards, and Guidance
Science and Technology, Program Protection
Office of the Under Secretary of Defense for Research and Engineering

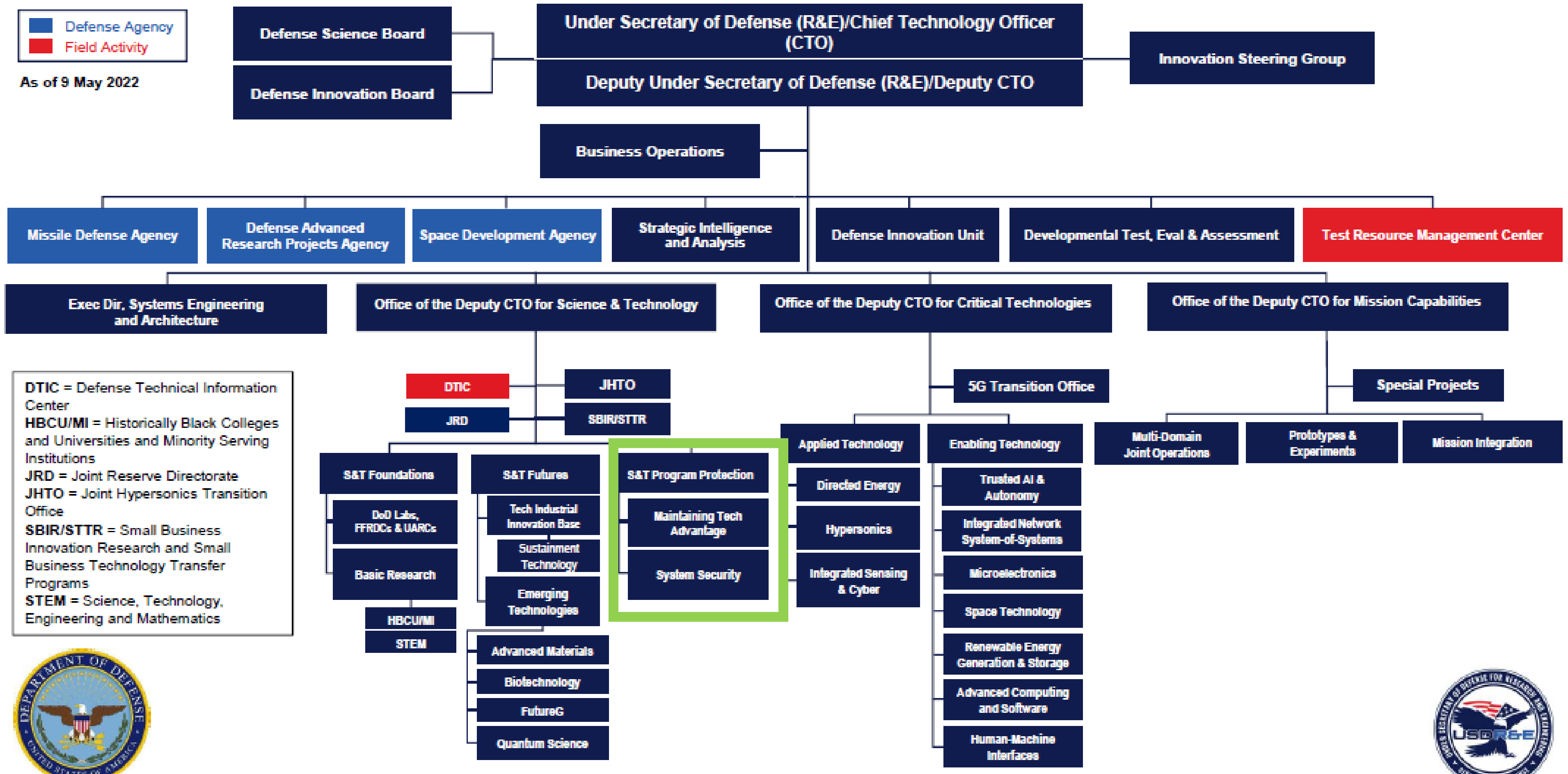
Cybersecurity & Information Systems Information Analysis Center (CSIAC)
14 February 2024

Agenda

- Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E))
- Department of Defense Instruction (DoDI) 5000.83
- Problem Statement
- CDS Polices
- CDS Key Concepts
- CDS Acquisition Process
- Summary
- Points of Contact
- Q&A

Source: Getty Images

Office of USD(R&E) Organization



🟦 Defense Agency
🟥 Field Activity
As of 9 May 2022
Defense Science Board
Defense Innovation Board
Under Secretary of Defense (R&E)/Chief Technology Officer (CTO)
Deputy Under Secretary of Defense (R&E)/Deputy CTO
Innovation Steering Group
Business Operations
Missile Defense Agency
Defense Advanced Research Projects Agency
Space Development Agency
Strategic Intelligence and Analysis
Defense Innovation Unit
Developmental Test, Eval & Assessment
Test Resource Management Center
Exec Dir, Systems Engineering and Architecture
Office of the Deputy CTO for Science & Technology
Office of the Deputy CTO for Critical Technologies
Office of the Deputy CTO for Mission Capabilities
DTIC
JRD
JHTO
SBIR/STTR
S&T Foundations
DoD Labs, FFRDCs & UARCs
Basic Research
HBCU/MI
STEM
S&T Futures
Tech Industrial Innovation Base
Sustainment Technology
Emerging Technologies
Advanced Materials
Biotechnology
FutureG
Quantum Science
S&T Program Protection
Maintaining Tech Advantage
System Security
5G Transition Office
Applied Technology
Directed Energy
Hypersonics
Integrated Sensing & Cyber
Enabling Technology
Trusted AI & Autonomy
Integrated Network System-of-Systems
Microelectronics
Space Technology
Renewable Energy Generation & Storage
Advanced Computing and Software
Human-Machine Interfaces
Special Projects
Multi-Domain Joint Operations
Prototypes & Experiments
Mission Integration

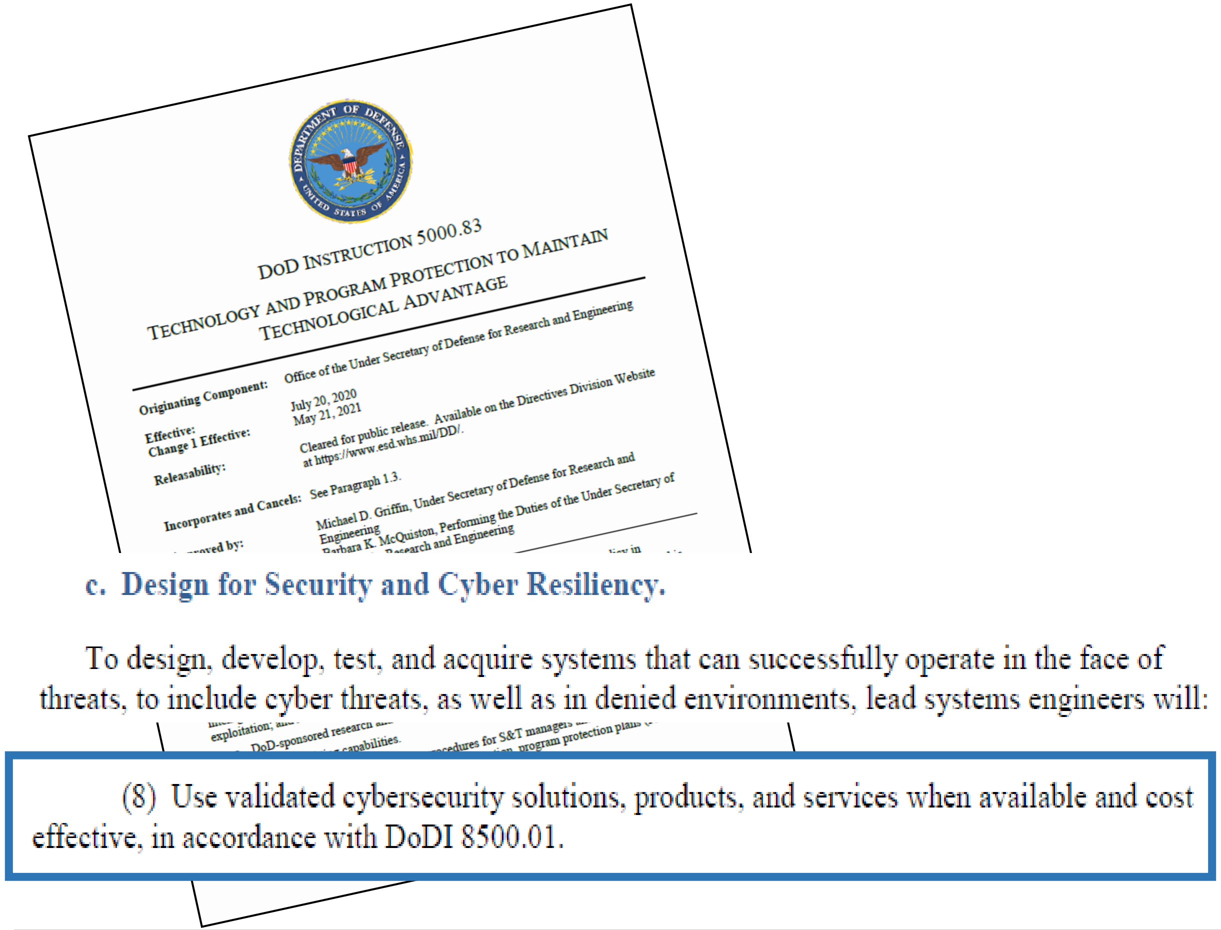
DTIC = Defense Technical Information Center
HBCU/MI = Historically Black Colleges and Universities and Minority Serving Institutions
JRD = Joint Reserve Directorate
JHTO = Joint Hypersonics Transition Office
SBIR/STTR = Small Business Innovation Research and Small Business Technology Transfer Programs
STEM = Science, Technology, Engineering and Mathematics

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

S&T Program Protection MISSION: Protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through superior, ***assured, secure and resilient systems***

Distribution Statement A: Approved for public release. DOPSR case #23-S-1103 applies. Distribution is unlimited.

DoDI 5000.83, Technology and Program Protection to Maintain Technological Advantage



DoD INSTRUCTION 5000.83

TECHNOLOGY AND PROGRAM PROTECTION TO MAINTAIN TECHNOLOGICAL ADVANTAGE

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Effective: Change 1 Effective:	July 20, 2020 May 21, 2021
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	See Paragraph 1.3.
…proved by:	Michael D. Griffin, Under Secretary of Defense for Research and Engineering Barbara K. McQuiston, Performing the Duties of the Under Secretary of … Research and Engineering

c. Design for Security and Cyber Resiliency.

To design, develop, test, and acquire systems that can successfully operate in the face of threats, to include cyber threats, as well as in denied environments, lead systems engineers will:

(8) Use validated cybersecurity solutions, products, and services when available and cost effective, in accordance with DoDI 8500.01.

- **Establishes responsibilities and procedures for *S&T managers and engineers* to manage system security and cybersecurity technical risks to:**
  - DoD-sponsored research and technology
  - DoD warfighting capabilities
- **System security and cybersecurity technical risks include:**
  - Hardware, software, supply chain exploitation
  - Cyber vulnerabilities
  - Reverse engineering, anti-tamper
  - Controlled technical information / data exfiltration
- **Design for security and cyber resiliency**
  - Secure Cyber Resilient Engineering (SCRE)

Establishes responsibilities for S&T managers and engineers on technology and program protection, includes pre- and post-acquisition protection activities

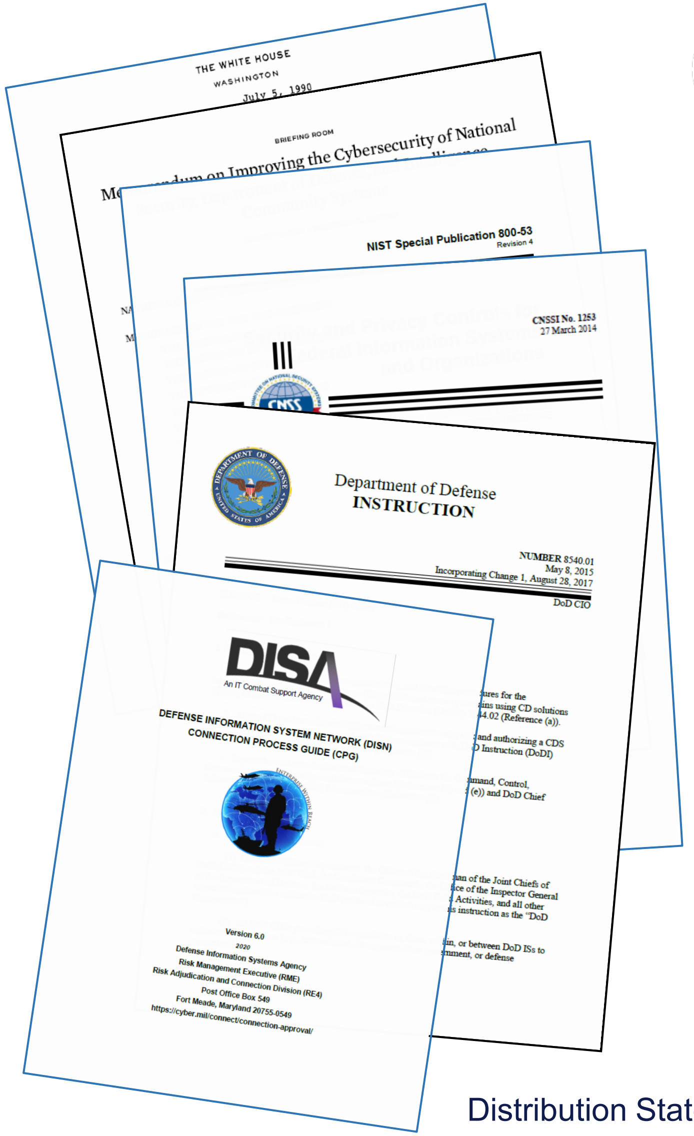
Problem Statement

- **Todays warfighting requires secure information sharing and collaboration across all types of boundaries including international, coalition partners, inter-governmental, non-governmental agencies**
  - Require technologies that enable warfighting communities and mission partners to share information across physically, logically, and administratively separated networks (known as security domains) in a reliable, secure and interoperable manner
  - Warfighters increasingly need to expand information sharing capabilities without introducing security vulnerabilities to their most sensitive systems and data/information
  - Interconnecting systems increase complexity in support of Joint All-Domain Command and Control (JADC2)

Source: Getty Images

CDS Technologies Address this Problem…

CDS Policy



THE WHITE HOUSE
WASHINGTON
July 5, 1990

BRIEFING ROOM
Memorandum on Improving the Cybersecurity of National

NIST Special Publication 800-53
Revision 4

CNSSI No. 1253
27 March 2014

Department of Defense
INSTRUCTION

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

DISA
An IT Combat Support Agency

DEFENSE INFORMATION SYSTEM NETWORK (DISN) CONNECTION PROCESS GUIDE (CPG)

Version 6.0
2020
Defense Information Systems Agency
Risk Management Executive (RME)
Risk Adjudication and Connection Division (RE4)
Post Office Box 549
Fort Meade, Maryland 20755-0549
https://cyber.mil/connect/connection-approval/

- **White House:**
  - *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, National Security Memorandum 8 (NSM-8), White House, 19 January 2022
    - Assigns National Cross Domain Strategy and Management Office (NCDSMO) its CDS authorities at a national level
  - National Security Directive 42 (NSD 42)
    - Assigns the National Security Agency (NSA) its information assurance authorities and designates NSA as the National Manager for National Security Systems (NSS). Document is confidential
- **DoD:**
  - DoDI 8540.01, Cross Domain Policy, Change 1, dated August 28, 2017
    - The DoD policy governing how to authorize and deploy CDS
  - Defense Information System Network (DISN) Connection Process Guide (CPG), Version 6.0, dated 2020, Defense Information Systems Agency (DISA)
    - Defines the process for connecting a CDS to DoD networks
- **National Institute of Standards and Technology (NIST):**
  - NIST SP 800-53 Revision Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated September, 2022
    - Defines the security controls used by the U.S. Government (USG) to assess IT systems.
- **Committee on National Security Systems (CNSS):**
  - CNSS Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems*, dated March 27, 2014
    - Applies the NIST-800 53 Security controls to NSS
  - CNSSI No. 1253, Appendix E, Attachment 3, *Cross Domain Solution Overlay*, dated February 08, 2023
    - Applies the CNSSI No. 1253 controls to CDS

National Cross Domain Strategy and Management Office (NCDSMO)

- **Formally stood up on 15 February 2019 by a joint DOD and IC CIO memorandum**
  - Replaces the Unified Cross Domain Services Management Office (UCDSMO)
  - Has been operating since 2017 and operates under the NSA's National Security Directive (NSD) 42 authorities

- **National Security Memo 8 (NSM-8) clarifies the authorities of Director, NSA (DIRNSA) as the National Manager, and designates NCDSMO to:**
  - Serve as the principal advisor to National Security System (NSS) owners for cross domain capabilities
  - Develop and maintain community outreach programs and forums
  - Develop and establish improved security solutions, remote management and monitoring, cyber defense, filtering requirements, and standards and technologies for CDS
  - Operate the USG CDS security testing program to ensure uniform comprehensive testing

Distribution Statement A: Approved for public release. DOPSR case #23-S-1103 applies. Distribution is unlimited.

NSA Guidance and Documents

- ***CDS 101: An Introduction to Cross Domain Solutions*, v1.0, NCDSMO Doc ID: NCDSMO-G-00032-001_00**
  - Describes CDS concepts, terminology, and the authorization process
- ***Cross Domain Solution (CDS) Design and Implementation Requirements: 2021 Raise the Bar (RTB) Baseline Release*, v4.1, July 11, 2022, NCDSMO Doc ID: NCDSMO-R-00008-004_01**
  - Establishes the requirements for the design, implementation and deployment of CDS
- ***Security Assessment of Cross Domain Solutions (CDS): Process and Requirements*, v4.1, NCDSMO Doc ID: NCDSMO-R-00003-004_01**
  - Describes key concepts and terminology related to the assessment (e.g., security testing) of CDS
- ***Cyber One-Way Taps Technical Requirements*, v1.0, NCDSMO Doc ID: NCDSMO-R-00016-001_01**
  - Describes the requirements for the design, implementation, and testing requirements of one-way taps and diodes
- ***CDSE 101: Guidance and Requirements*, v1.0, NCDSMO Doc ID: NCDSMO-R-00015-001_00**
  - Describes the certification process for Cross Domain Support Office/Elements and their functions
- ***Cross Domain Solution (CDS) Development and Testing Environment Security Requirements*, v1.1, 12 January 2022, NCDSMO Doc ID: NCDSMO-R-00011-001_01**
  - Defines the isolation and security requirements for networks used to development, test, evaluate and integrate CDS

NCDSMO Documentation can be obtained from Intelink-U at https://intelshare.intelink.gov/sites/ncdsmo

CDS Design and Implementation Requirements (Raise the Bar)

- Raise the Bar (RTB) is the NCDSMO's security requirements for the design, development, assessment, and deployment of CDS to improve the security and capabilities for the protection of NSS
- RTB is updated annually to address new threats, new technologies, new knowledge and any issues/vulnerabilities found
- Applies to all USG-operated CDS
- Applies to all CDS developed for sale as part of a Foreign Military Sales (FMS) activity
- NCDSMO Documentation and Requirements can be obtained from Intelink-U at:
  - https://intelshare.intelink.gov/sites/ncdsmo

Cross Domain Support Office/Element (CDSO/E)

- **Each USG agency has an associated CDSO/E**
  - The list of CDSO/Es is available on the NCDSMO NIPRnet Portal
- **CDSO/E certification and responsibilities are described in the NCDSMO publication *CDSE 101: Guidance and Requirements***
- **CDSO/E responsibilities include:**
  - Provides the primary interface between the agency and the NCDSMO
  - Works with agency personnel on the Buy, Modify, and Build (BMB) process for selecting a CDS
  - Provides support on the authorization process for the agency's CDS deployments

What is a Security Domain?

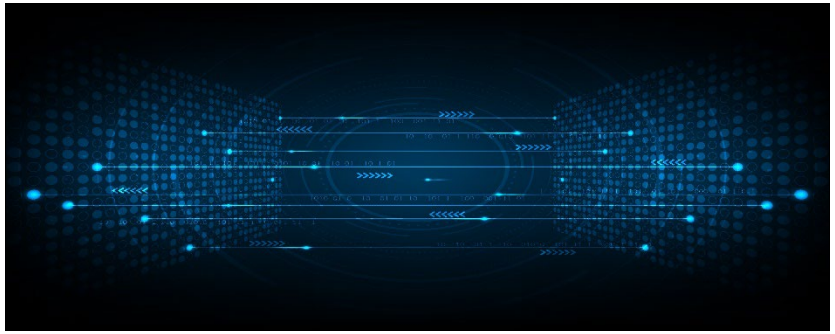
"A domain operating at a single security level (which includes a unique combination of classification, releasabilities, and dissemination controls) that implements a security policy and is administered by a single authority." – Committee on National Security Systems Instruction 4009

- **Security domains are identified by their security marking**
  - A security marking is a combination of a classification level in combination with any stated releasabilities, dissemination controls, compartments/Special Access Programs (SAPs), and some handling caveats
  - Examples of security domains in the US include:
    - NIPRnet, SIPRnet, JWICS, any of the Secret Releasable CENTRIXs networks
    - Controller Area Network Bus (CANbus) in a vehicle

Cross Domain Solutions

What is a CDS?

- "A form of controlled interface (a boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems) that provides the ability to manually and/or automatically access and/or transfer information between different security domains." - National Institute of Standards and Technology (NIST)
- A Controlled Interface is "A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems." - NIST SP 800-37 Rev. 1



Source: Getty Images

Why use a CDS?

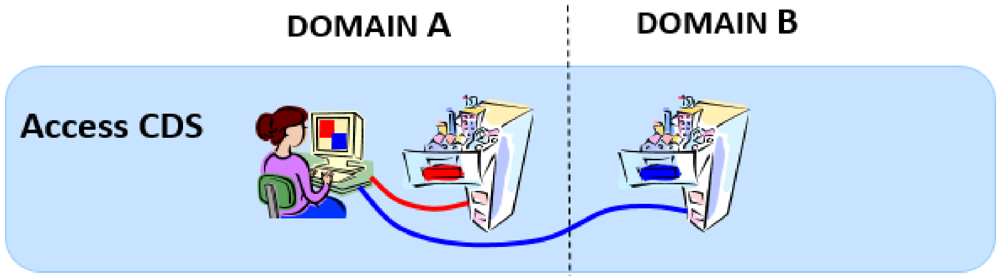
- Transfer data between different systems operating in different system domains
- Reduce accidental release of information from classified networks
- Enable Command & Control (C2) and status communications between components of a weapon system
- Desktop Reduction
  - Reduce the number of networks and PCs of different classification levels on users' desks
- Increased Information Sharing
  - Enhance exchange of information with coalition and external partners
- Reduction in Data Spills, Malware Infection/C2, and Data Exfiltration from use of removable media to transfer data

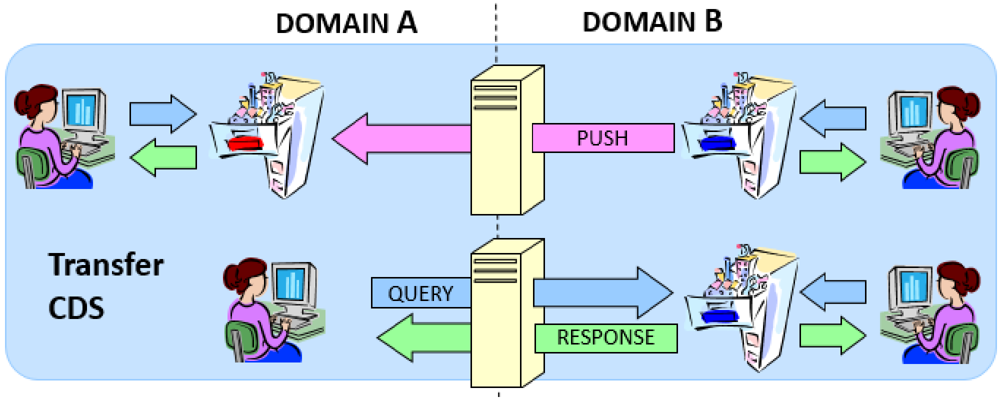
Cross Domain Solutions Types

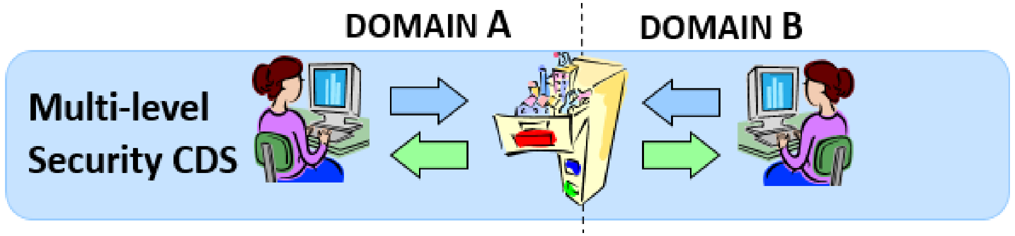
- **Access CDS**
  - Provides access to computing platforms residing in lower security domains without transfer of user data between the domains. The access function is implemented by transferring keyboard and mouse data down to the lower security domain and sending video/image data up to the higher security domain
  - Largest number of units deployed
  - Two sub-types:
    - Virtual machine-based
    - Remote Virtual Desktop Infrastructure (VDI)-based

- **Transfer CDS**
  - One-way or bidirectional data transfers
  - Transfers data between systems operating in different security domains Filters the data being transferred to remove malicious content and reduce data spills
  - Used in Human2Human, Human2Machine, and Machine2Machine data transfers

- **Multi-Level Security (MLS) CDS**
  - Stores and provides access to labeled data
  - Primarily used for multi-level database or file storage
  - Usually integrated with a transfer CDS to change the label on the data (e.g., a regrade operation)







Distribution Statement A: Approved for public release. DOPSR case #23-S-0053 applies. Distribution is unlimited.

CDS Applicable Environments

- **Enterprise**
  - CDS operated by specially designated General Purpose Enterprise Cross Domain Service Providers (GP-ECDSP) or Mission Specific Cross Domain Service Providers (MS-ECDSP)
  - List of ECDSPs are on the NCDSMO Portal
    - USG-contracted Cloud Service Providers are operating ECDSP capabilities
    - DISA
- **Point 2 Point (P2P)**
  - Local installation of a CDS in a non-tactical environment
  - Strong push by USG authorizing officials to transition P2P CDS deployments to ECDSPs to reduce long-term security and sustainment costs
- **Tactical**
  - CDS operating in communications and Size, Weight, Power, and Cooling (SWaP-C) constrained environment
  - Typical deployments include satellites, human-wearable, aircraft, ground vehicles, and naval vessels
  - Requires active anti-tamper and TEMPEST
  - Can be integrated with NSA-approved encryption devices

Source: Getty Images

Source: Getty Images

Distribution Statement A: Approved for public release. DOPSR case #23-S-0053 applies. Distribution is unlimited.

CDS Acquisition Process

- **Evaluate if your project or system needs any of the following:**
  - The need to transfer data between different security domains or systems operating at different security levels?
    - If so, do you have the specifications for your protocols and data formats?
  - The need to combine data from multiple sources at different levels into a single system for analysis and visualization?
  - The need to access low security domains from a high security domain?
  - Does the system have a red/black separation problem that is not related to encryption?
- **Contact your CDSO/E and the NCDSMO as early in the process as possible**
- **Conduct a Requirements Analysis**
  - Functional / Security
- **Conduct Analysis of Alternatives (AoA)**
  - Includes BMB determination for the CDS or changing the system to eliminate the need for a CDS
  - Consider technology listed in NCDSMO CDS Baselines
- **Selection and procurement of a solution**
  - May include development and testing of a new CDS or modification of an existing CDS
- **Executing the DOD CDS Approval Process**
  - Request for authorization to deploy
  - Installation and accreditation testing
- **Managing, monitoring, and maintaining your CDS**

Source: Getty Images

Buy vs. Modify vs. Build

- Engage with your CDSO/E and the NCDSMO *before you start and throughout the selection* and, if applicable, development lifecycle
- **Buy**
  - There are many Government-Off-The-Shelf (GOTS) and Commercial-Off-The-Shelf (COTS) options for CDS technology on the NCDSMO CDS Baseline
  - Most likely, one already exists that can be used out-of-the-box or with new rule sets or schemas
  - This approach is usually the lowest technical and approval risk, most cost-effective, and fastest solution to get deployed
- **Buy and Modify**
  - An existing CDS can be modified to support unique mission specific protocols, data formats, or Space, Weight, Power, and Cooling (SWaP-C) requirements
  - Generally, it is cheaper and faster and with lower schedule, technical, and security risks to fund modifications to an existing CDS than to start from scratch
  - Modifications to the CDS will require testing in an NCDSMO certified lab

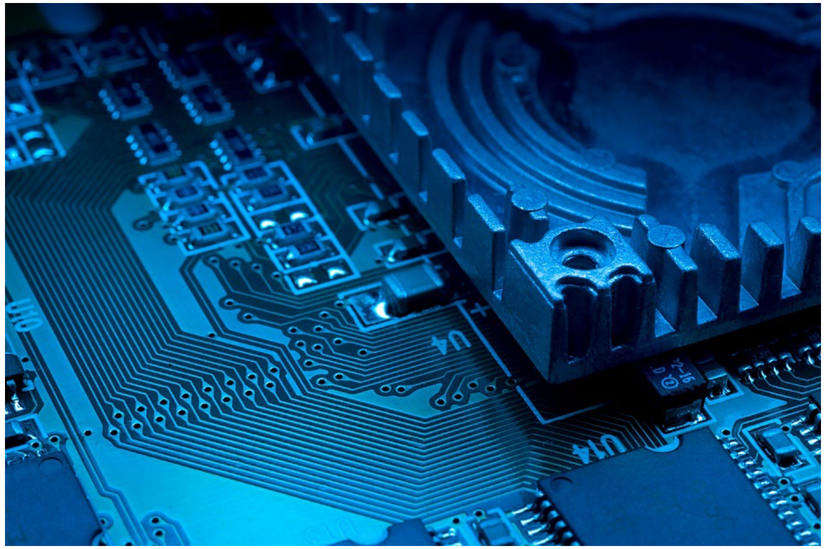
Distribution Statement A: Approved for public release. DOPSR case #23-S-1103 applies. Distribution is unlimited.

Buy vs. Modify vs. Build (cont.)

- **Build**
  - Used only when an existing CDS cannot be used or modified to meet mission requirements
  - It has high technical, security, programmatic, and schedule risks
  - A development program can expect building a new CDS to take at least 2-5 years and cost in the millions of dollars
  - NCDSMO lab testing is required for new CDS
  - This approach is the most expensive, has the highest technical and authorization risk, and has the longest timeline to deployment
- **CDS Testing**
  - **Security Assessment:** Changes to a CDS **must** go through NCDSMO's Lab-Based Security Assessment (LBSA) Process
    - The LBSA process and requirements are described in the NCDSMO document *Security Assessment of Cross Domain Solutions (CDS): Process and Requirements*
  - **Interoperability Testing:** Testing to confirm the interoperability between the CDS and the system(s) with which it is being integrated (e.g., Joint Interoperability Test Command testing) may be required
    - This is common for CDS that are integrated into weapon and C4ISR systems
  - **Flight/Vehicle Safety Testing:** Testing of the CDS system to confirm it meets safety requirements may be required
    - This is common for CDS integrated in military vehicles

Testing Requirements for CDS

- **Full Lab-Based Security Assessment (FLBSA)**
  - All features of the CDS are tested with a focus on the new or changed functionality regardless of what functionality the customer plans to use
- **Delta Lab-Based Security Assessment (DLBSA)**
  - All changes to the CDS since the previous test event are tested
- **Regression Lab-Based Security Assessment (RLBSA)**
  - Changes made to fix issues from a Full or Delta LBSA are tested
- **Modular Pipeline Component Testing (MPCT)**
- **Ruleset Testing (RST)**
- **Site-Based Security Assessment (SBSA)**
  - Testing is conducted at locations where a CDS is operated, staging site or depot site where CDS are configured prior to being deployed or integrated into a weapon system or sensor
- **Extended Site-Based Security Assessment (ESBSA)**
- **Developer Conducted Testing (DCT)**



Source: Getty Images

Refer to the *Security Assessment of Cross Domain Solutions (CDS): Process and Requirements, v4.0 for details*

Distribution Statement A: Approved for public release. DOPSR case #23-S-1103 applies. Distribution is unlimited.

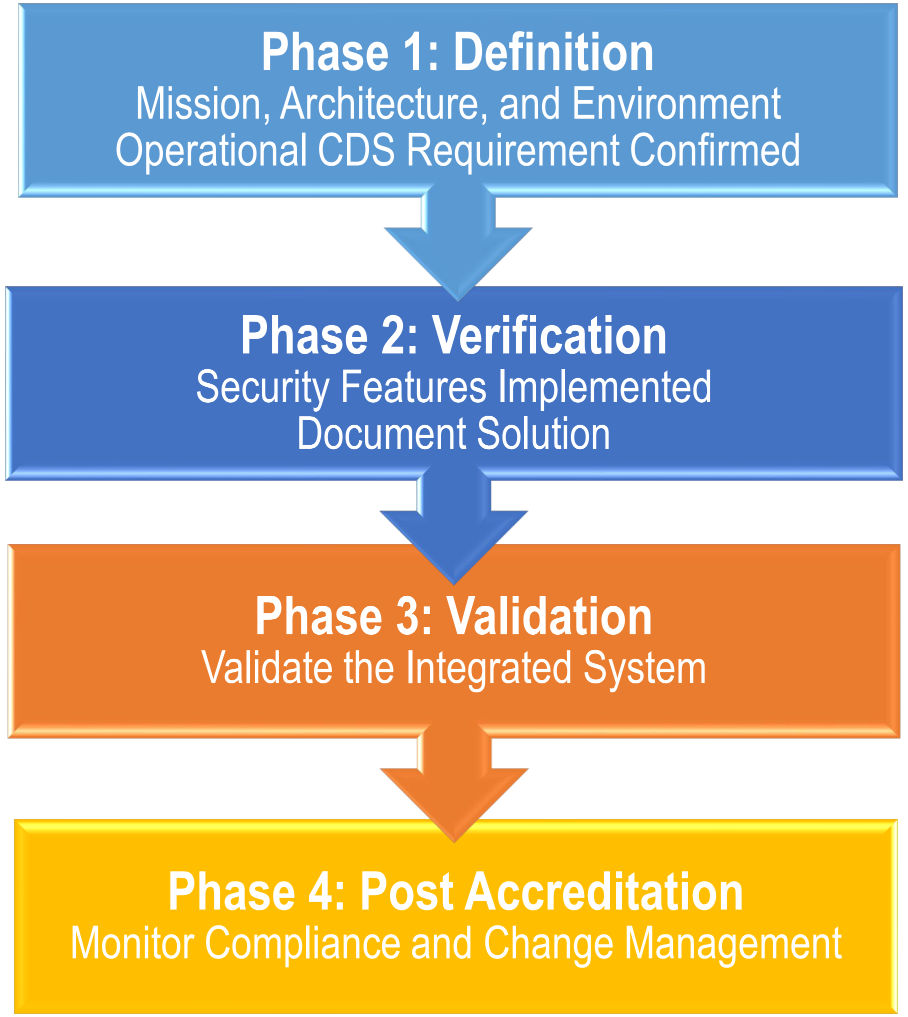
DoD CDS Connection Approval Process

- **<u>All</u> CDS connections to DoD classified networks must be in accordance with DoDI 8540**
  - The required connection process is described in detail in the DISN Connection Process Guide (CPG) v6.0
- **A CDS must be on the NCDSMO USG baseline to be deployed**
- **CDS connected to TS/SCI or Special Access Program (SAP) networks/systems may use a different approval process (see your CDSO/E for details)**
- **If a USG organization is deploying a CDS with a Commercial Solutions for Classified (CSfC), then agencies <u>must</u> contact their CDSO/E to coordinate the CDS approval in addition to registering the CSfC solution with the NSA CSfC Program Management Office (PMO). In CSfC, CDS are typically used:**
  - As an End User Device via an Access CDS
  - To support management and monitoring of a CSfC solution via a Transfer CDS

Source: Getty Images

Distribution Statement A: Approved for public release. DOPSR case #23-S-1103 applies. Distribution is unlimited.

CDS Connection Approval Process Overview



Phase 1: Definition
Mission, Architecture, and Environment
Operational CDS Requirement Confirmed

Phase 2: Verification
Security Features Implemented
Document Solution

Phase 3: Validation
Validate the Integrated System

Phase 4: Post Accreditation
Monitor Compliance and Change Management

What's Happening at Each Phase

- Solidification of the need for a CDS
- Selection of a technology "path", the BMB decision

- Design of the actual solution including its technology, configuration, data policy, and operational CONOPs
- Lab-based Security Assessment conducted (if applicable)

- Anticipated Risk Assessed
- Site integration and Site-based Security Assessment (SBSA) execution
- Actual deployed Risk Assessed

- Site compliance visits usually during a Command Cyber Operational Readiness Inspection (CCORI)
- Routine patching
- Annual re-accreditation

CDS Operations, Maintenance, and Lifecycle

- **CDS are not a black box**
  - Agencies can not install it and forget about it
- **CDS <u>must be patched regularly for the lifetime</u> of the weapon system, sensor, platform, or IT system in which it has been integrated**
  - All CDS software updates and patches are provided by the CDS vendor
  - For many weapon systems, implementing a CDS in hardware (e.g., Field Programmable Gate Arrays (FPGA)) can substantially reduce long term lifecycle costs
- **CDS <u>must be actively maintained and enhanced</u> to address new cyber threats and component obsolescence until the CDS or the system it is embedded in is decommissioned**
  - Operating systems and CDS components go to end of life and need to be periodically upgraded or replaced to ensure the CDS is secure and supportable
- Like all IT systems, a CDS **<u>must be monitored and defended</u>** with an active Defensive Cyberspace Operations capability

CDS Challenges and Risks

- May involve multiple security domains
- Approval for CDS deployments may involve multiple authorizing officials depending on the networks/systems involved
- Requires robust risk management strategy
- Requires robust sustainment strategy
- Requires individuals with specialty skillsets

- High value target for threats
  - Supply Chain threats
  - Data exfiltration threats
  - High side / low side domain(s) threats
  - Malicious insider (user / admin) threats
  - Facility access threats
  - Accidental release of sensitive information

Requires proactive engagement with CDSO/CDSE and NCDSMO

Summary

- **This presentation has addressed the basic concepts and key topics to help gain a foundational understanding of CDS**
- **The need to interconnect complex and critical weapons systems/systems of systems (SoS) and their security domains often necessitates the deployment of CDS**
  - CDS are required to support connections between different security domains
  - A CDS will enforce a security policy, developed to meet an organization's information sharing requirements, whilst upholding the security and risk acceptance assumptions of the security domains involved
- **The DoD acquisition engineering and technical community need to master how to define requirements for CDS; develop CDS architecture and design; and integrate, test, and deploy CDS**
  - Understand governing policies and processes

Points of Contact

If you believe you may have a CDS requirement or intend to buy, modify, or build a CDS contact your Cross Domain Support Element or the NCDSMO

NCDSMO can be reached at:

- Email: ncdsmo@nsa.gov
- NIPRnet: https://intelshare.intelink.gov/sites/ncdsmo (CAC/PIV required)

Further questions about the training courses:

- Mr. Burhan Adam
  burhan.y.adam.civ@mail.mil
- Ms. Singi De Silva
  singithi.n.desilva.ctr@mail.mil

Source: Getty Images

Distribution Statement A: Approved for public release. DOPSR case #23-S-0053 applies. Distribution is unlimited.

BACKUP

Isn’t CDS Just a Firewall?

No, there are substantial differences between the two.

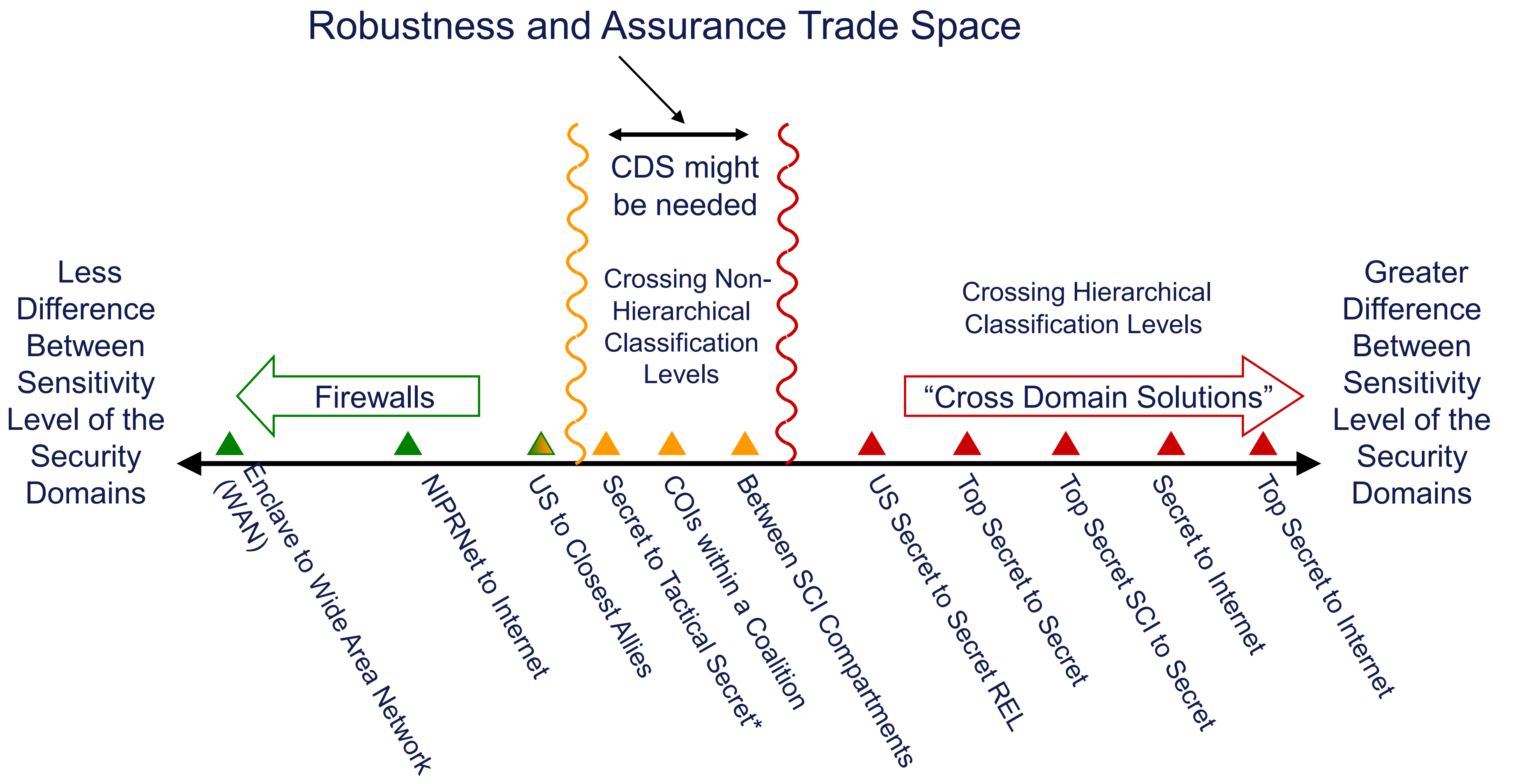
CDS

- Implemented on trusted platform
- Connects domains at **different** levels
- Opens doors that are normally closed
- Robust filtering of data at application level
- Prevents data leakage
- Few services allowed through (e.g., e-mail, messages, file transfer)
- No IP forwarding
- Performs regrading of data
- Requires special USG-run testing and authorization processes

Firewall

- Not generally implemented on trusted platform
- Connects domains at **same** level
- Closes doors that are normally open
- Controls network services
- Filters packets at protocol level; may proxy packets at application level
- More services allowed through (e.g., file transfer, e-mail, TELNET, HTTP)
- Most offer IP forwarding
- No regrading of data
- Commercial or NIAP testing is sufficient

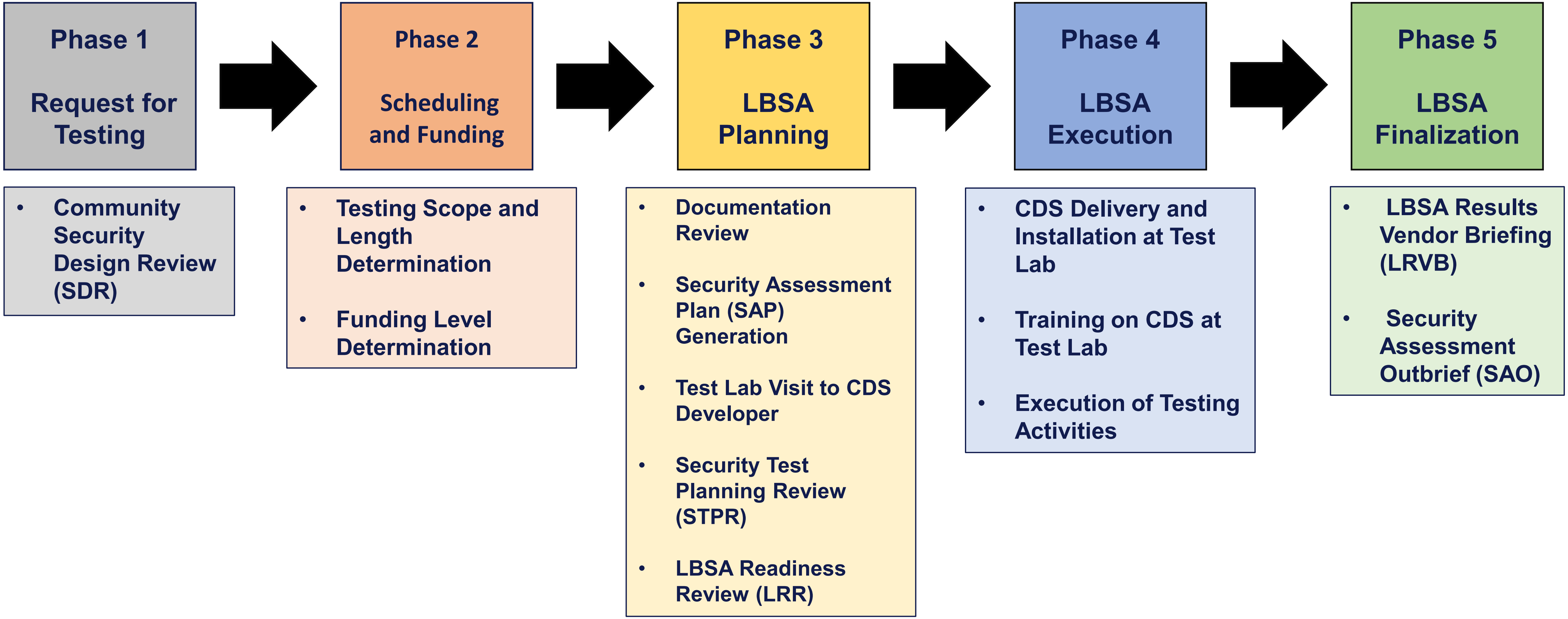
Controlled Interface Spectrum


Robustness and Assurance Trade Space
CDS might be needed
Crossing Non-Hierarchical Classification Levels
Crossing Hierarchical Classification Levels
Less Difference Between Sensitivity Level of the Security Domains
Greater Difference Between Sensitivity Level of the Security Domains
Firewalls
"Cross Domain Solutions"
Enclave to Wide Area Network (WAN)
NIPRNet to Internet
US to Closest Allies
Secret to Tactical Secret*
COIs within a Coalition
Between SCI Compartments
US Secret to Secret REL
Top Secret to Secret
Top Secret SCI to Secret
Secret to Internet
Top Secret to Internet

*Sometimes called Combat Sensitive Data

Distribution Statement A: Approved for public release. DOPSR case #23-S-1103 applies. Distribution is unlimited.

Lab-Based Security Assessment Process



Phase 1

Request for Testing

- Community Security Design Review (SDR)

Phase 2

Scheduling and Funding

- Testing Scope and Length Determination
- Funding Level Determination

Phase 3

LBSA Planning

- Documentation Review
- Security Assessment Plan (SAP) Generation
- Test Lab Visit to CDS Developer
- Security Test Planning Review (STPR)
- LBSA Readiness Review (LRR)

Phase 4

LBSA Execution

- CDS Delivery and Installation at Test Lab
- Training on CDS at Test Lab
- Execution of Testing Activities

Phase 5

LBSA Finalization

- LBSA Results Vendor Briefing (LRVB)
- Security Assessment Outbrief (SAO)

Contact your CDSO/E to request more information from the NCDSMO LBSA team on testing schedules and status