USD(R&E)

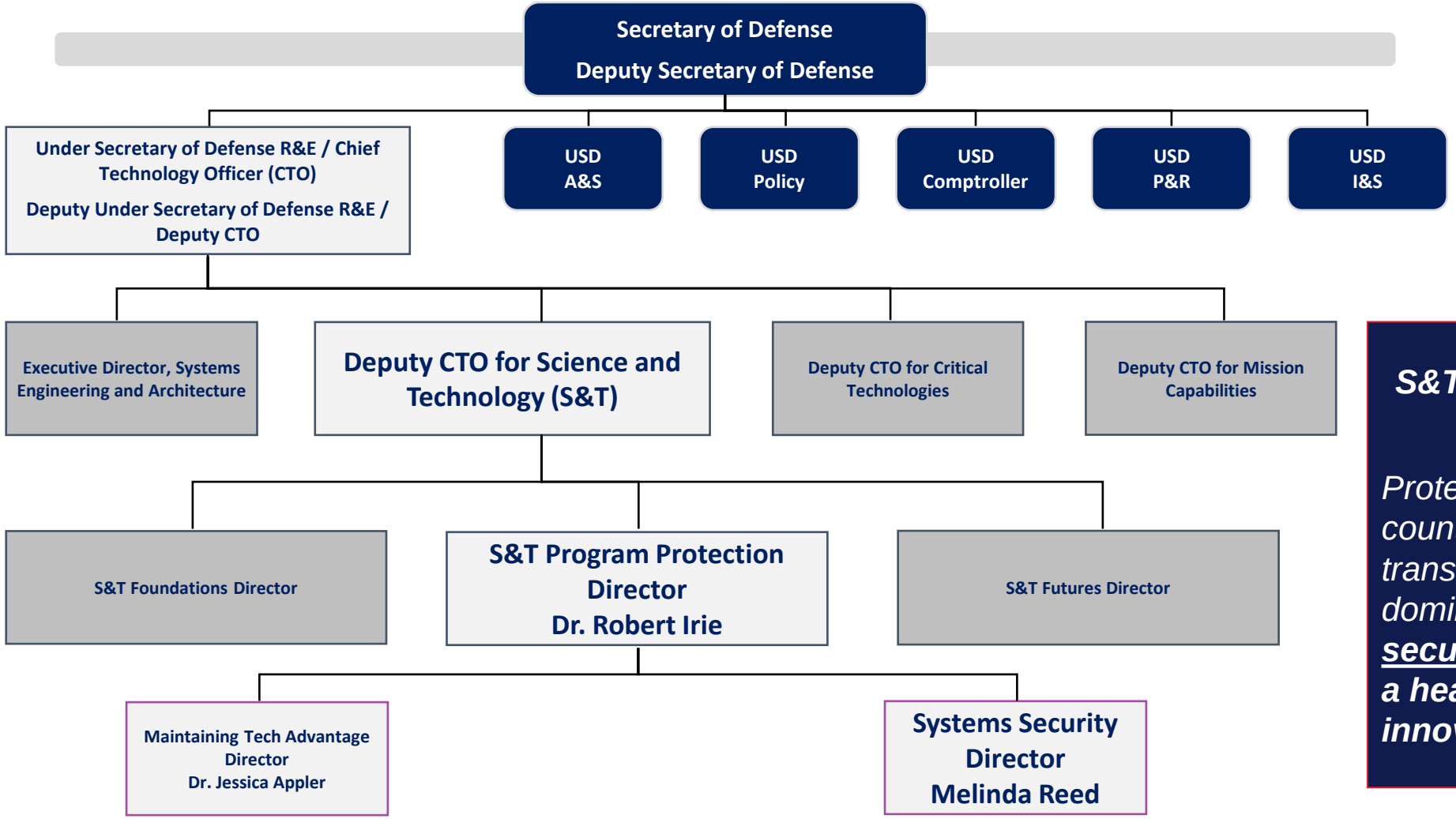
Cross Domain Solutions Tutorial

Mr. Burhan Adam
Director, Systems Security Policy, Standards, and Guidance
Office of the Under Secretary of Defense for Research and Engineering
National Defense Industrial Association Systems and Mission Engineering Conference
November 1-3, 2022

Agenda

- Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E))
- Department of Defense Instruction (DoDI) 5000.83
- Cross Domain Solutions (CDS) Problem Statement
- CDS Governing Policies
- Definition, Types, and Applications of CDS
- CDS Training Objectives and Plans
- Summary
- Points of Contact

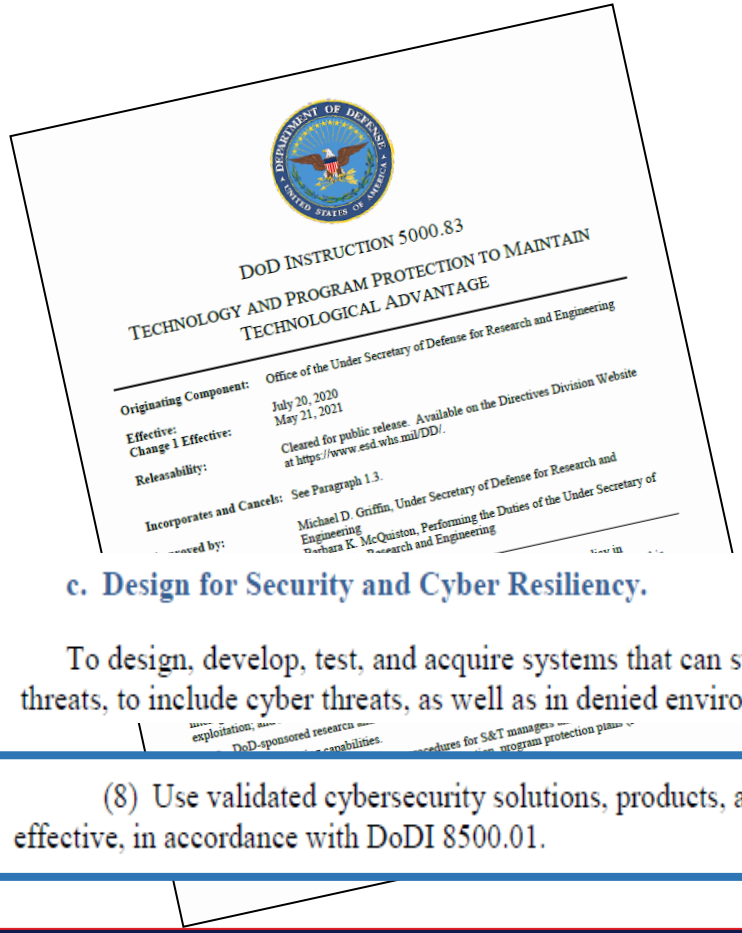
OUSD(R&E) Organization



S&T Program Protection (STPP) MISSION:

Protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through ***assured, secure and resilient systems*** *and a healthy, viable national security innovation base.*

DoDI 5000.83



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: July 20, 2020
Change 1 Effective: 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.

Approved 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.

DoDI 5000.83, *Technology and Program Protection to Maintain Technological Advantage*, May 2021

- **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, and cyberspace vulnerabilities
  - Reverse engineering, anti-tamper
  - Controlled technical information / data exfiltration

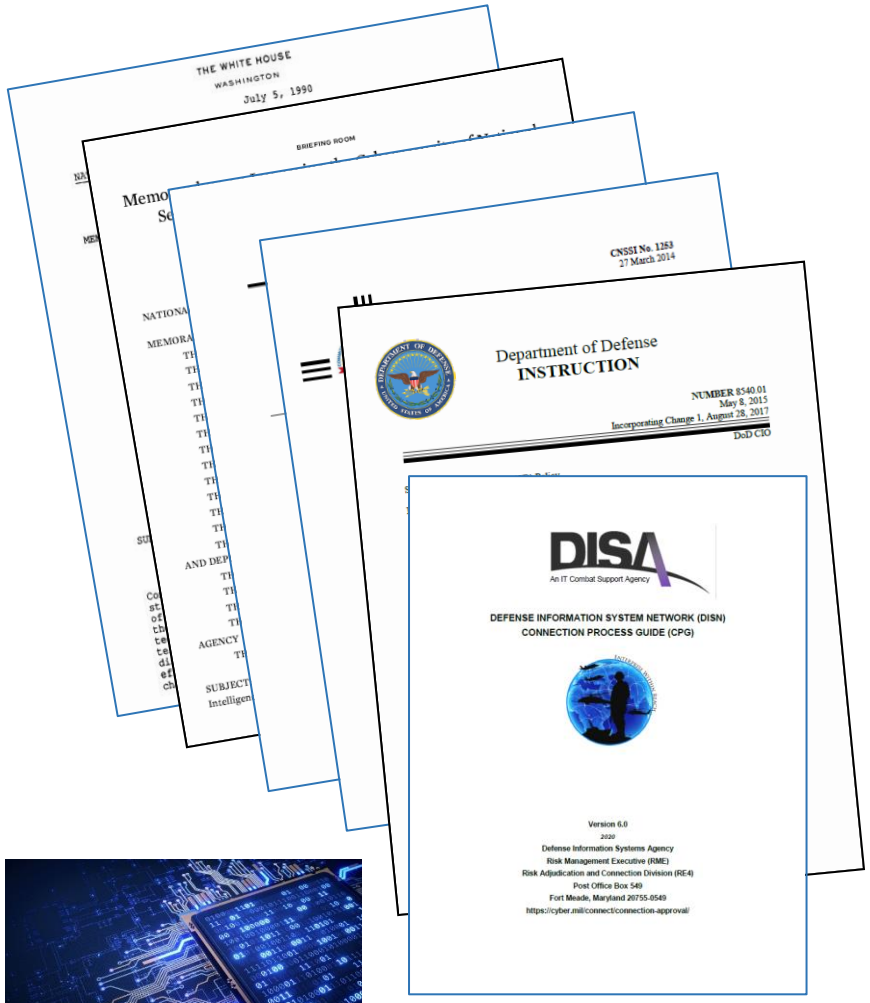
Establishes responsibilities for technology and program protection, includes pre- and post- acquisition protection activities

Problem Statement

- **Future and contemporary warfighting requires secure information sharing and collaboration across all types of boundaries including international, governmental, federal, agency, state, local, and security.**
  - Warfighters increasingly need to expand information sharing capabilities without introducing security vulnerabilities to their most sensitive systems and data/information.

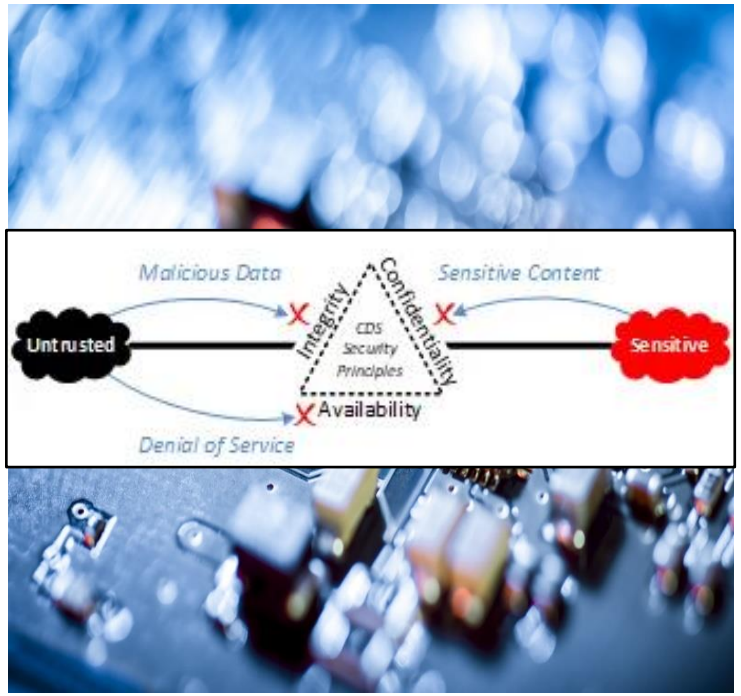
- **CDS technologies address this requirement by enabling warfighting communities and coalition partners to share information across physically, logically, and administratively separated networks (known as security domains) in a reliable, secure and interoperable manner.**

Cross Domain Solutions Policy



- **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 F, Attachment 3, *Cross Domain Solution Overlay*, dated September 12, 2017 or later
    - Applies the CNSSI No. 1253 controls to CDS

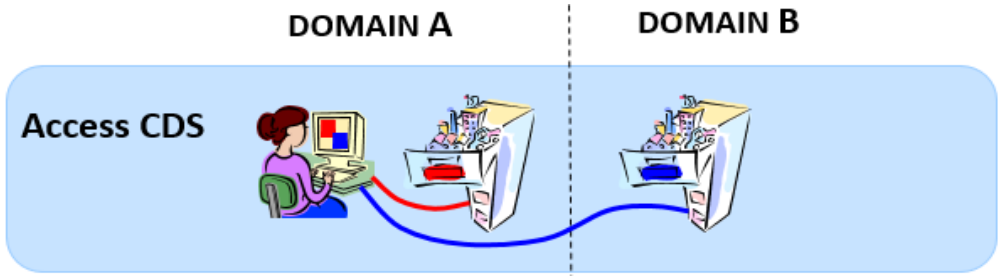
Cross Domain Solutions



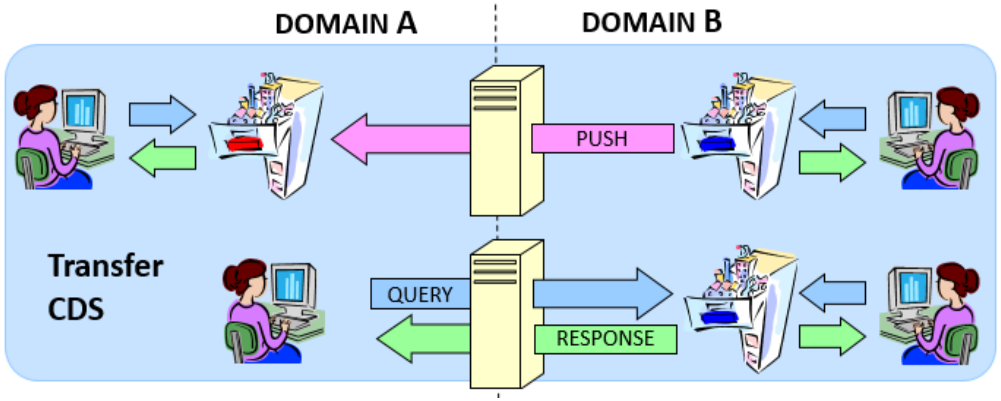
- **What is a CDS?**
  - "A form of controlled interface (a boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems) that provides the ability to manually and/or automatically access and/or transfer information between different security domains." - 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
- **Why are CDS needed?**
  - CDS are needed to enable secure information sharing
  - Must be implemented securely in order to maintain the necessary data characteristics of confidentiality, integrity and availability
  - Large enterprise data centers with many different networks and security enclaves with a different classification and or releasability requirements often need a CDS

Cross Domain Solutions Types

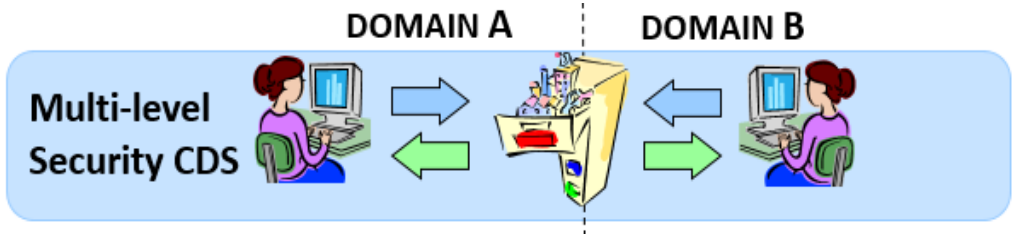
- **Access CDS**
  - Provides access to a computing platforms residing in lower security domains without transfer of user data between the domains. The access function is implemented by transferring keyboard and mouse data down to the lower security domain and sending video/image data up to the higher 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)



Cross Domain Solutions – Applicable Environments

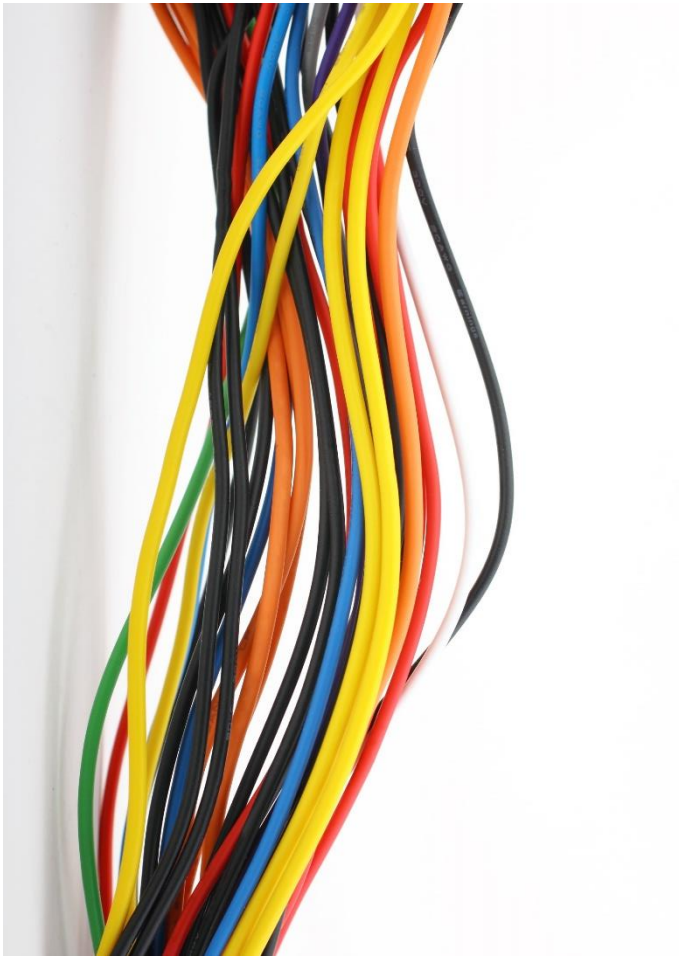
- **Enterprise**
  - CDS operated by specially designated General Purpose Enterprise Cross Domain Service Providers (GP-ECDSP) or Mission Specific Cross Domain Service Providers (MS-ECDSP)
  - List of ECDSPs are on the NCDSMO Portal
    - USG-contracted Cloud Service Providers are operating ECDSP capabilities
    - 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

Cross Domain Solutions Training

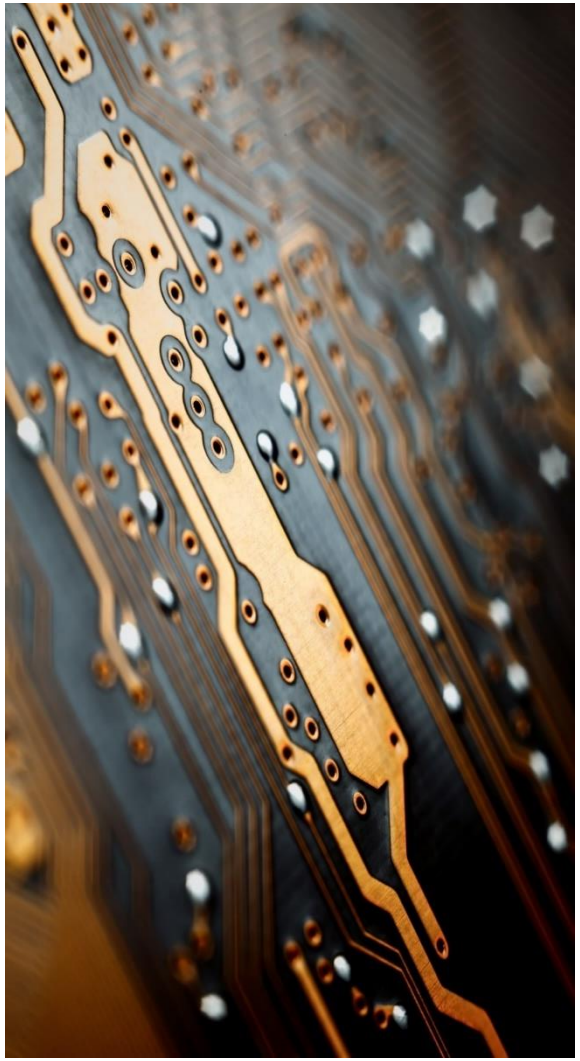
- **Provide training material to better support and educate the engineering workforce and their supporting technical staff on introductory, basic CDS concepts and key topics to help establish a foundation for understanding CDS technology and the associated policies, processes, challenges and risks**
- **Collaborative effort between NSA's National Cross Domain Strategy and Management Office (NCDSMO) and OUSD(R&E)**
- **Deliver two products in collaboration with Defense Acquisition University (DAU), National Defense University (NDU), and NCDSMO**
  - CDS Fundamentals Webinar (CDS 101)
    - Virtual webinar
  - CDS Practitioner Tutorial
    - Use-case and scenario building-based
    - In-person training course designed in-depth for the engineering community
- **Long-term: provide formal education and training**
  - Formal training courses
  - Standardizing CDS as a secure cyber resilient engineering (SCRE) design pattern for the community

Cross Domain Solutions Fundamentals Webinar (CDS 101) Objectives

- Understand CDS terminology and the CDS types
- What is the NCDSMO and its role?
- Understand USG and DoD CDS policies
- Understand the functions of CDS
- Understand how to identify a cross domain problem in system architecture
- Understand how to determine if you need a CDS
- Making a “buy, modify, or build” decision
- Overview of the CDS testing process
- Overview of the CDS accreditation and authorization process
- CDS lifecycle issues



Cross Domain Solutions Practitioner Training Objectives



- How to define/capture, analyze, and decompose cross domain security requirements
- Cross domain security principles
- Security domains and their connectivity considerations and requirements
- Understand how to develop, assess, and balance between information security requirements, operational objectives, threats, and business objectives
- Key considerations for secure CDS architecture and design development
- Integration and deployment considerations
- CDS testing requirements and process
- CDS accreditation and authorization process, requirements, and considerations
- CDS lifecycle/sustainment Issues and how to develop a strategy for them
- Management of technical risks
- CDS governing policies and guides

Summary

- **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
  - Secure Cyber Resilient Engineering (SCRE) solution
- **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

- **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