The Unified Cross Domain Management Office: Bridging Security Domains and Cultures

Marianne Bailey
OASD(IIA)

The Unified Cross Domain (CD) Management Office (UCDMO) was established July 2006 to address the needs of the DoD and the IC to share information and bridge disparate networks. Information sharing is a requirement that spans both departments and requires the ability to share information from the most highly classified networks to the most open coalition networks. The UCDMO was created to address the duplication, inefficiencies and resulting ineffectiveness resulting from years of uncoordinated activities in the CD arena.

The UCDMO was established on July 10, 2006, by the Assistant Secretary of Defense for Networks and Information Integration and Department of Defense Chief Information Officer (ASD(NII)/ DoD CIO), the Honorable John Grimes, and the Associate Director of National Intelligence and CIO, the Honorable Dale Meyerrose (ADNI & CIO). As the necessity to share information between the DoD, the IC, and U.S. foreign allies has continuously increased, the ability to bridge disparate networks (security domains) has become critical. Information sharing is a requirement that spans both departments and requires the ability to share information from the most highly classified networks to the most open coalition networks. In the past, these bridges or CD mechanisms were developed behind the doors of each organization for their specific applications. The result from years of doing business in this way has led to many CD stovepipes with independent sustainment tails, a tremendous number of interconnections, inconsistent security and risk-mitigation practices, and inadequate policies.

In addition, customers looking for a solution to enable them to share information across security domains had nowhere to go to seek help and often would develop another stovepiped solution. In the DoD, this flood of components into the current certification process resulted in a wait time anywhere from one to two years before approval to operate was granted. In the IC, there was less consistency among the agencies resulting in varying security practices. In an arena wrought with a lack of standards and excessive duplication, the worst part was that even for those who endured a two-year wait the customer's requirement for sharing information was not being met. In short, the lack of adequate CD mechanisms and common standards, policies and processes were significantly impacting the ability of the United States to ensure critical information was available when and where it was needed. The CIOs realized the need to join forces to solve the CD problem and created the UCDMO to address the duplication, inefficiencies and ineffectiveness resulting from years of uncoordinated activities in the CD arena.

The UCDMO faced two initial challenges: staffing the office, and tackling the initial tasking given to them by the CIOs to clean up the state of CD in the DoD and IC. Specifically, they were charged with getting the list of current operational mechanisms down to 24 specific mechanisms. Meyerrose and Grimes felt that 24 was a reasonable number of discrete CD mechanisms for the community. They wanted to make sure there were enough to fill the requirements of the DoD and IC, but not so many as to cause significant redundancy. With a staff of five, the UCDMO knew they would have to draw upon the community to tackle this task. To obtain support for both the staffing and the initial task, the UCDMO leadership began a series of meetings with all major agency CIOs to request full-time staff as well as participation in all tiger team[1] initiatives.

To address the current state of CD, the UCDMO led a community tiger team to determine a process for vetting the current operational solutions and eventually develop a CD baseline. The team quickly realized the need for a common CD taxonomy to ensure that all communities would speak the same language. First on the list was defining CD. The following definition was developed, vetted through the DoD and IC, and approved:

> A CD mechanism is defined as a form of controlled interface that provides the ability to manually and/or automatically access and/ or transfer information between differing security domains. [1]

The CD taxonomy was released in January 2007 and can be found on the UCDMO Web site[1]. Beginning with an initial list of more than 800 items believed to be CD products, the tiger team developed a fairly simple set of criteria and over the course of three months whittled the list of acceptable CD solutions down to 15 discrete items.

Products on the baseline are determined to meet the community standards and are available for reuse as a point solution or as an enterprise service. Each of these products is approved for a specific implementation such as bridging a top secret to secret domain or bridging a secret to unclassified domain. To make the list more useful to the customer, the UCDMO categorized CD mechanisms as *transfer*, *access*, and *multilevel*. A *transfer* device permits the movement of data from one domain to another. An *access* device allows a user to sit on one workstation and access multiple domains but not move data between them. A *multilevel* device stores and processes information of different security levels in a common repository but only allows a user to view appropriate information based on his/her credentials. CD baseline mechanisms are identified based on these three categories. An updated version of the list is released whenever there is a change to the baseline. The UCDMO Web site[2] contains the latest version of the CD baseline (see Table 1, next page) with descriptions and points of contact for each mechanism. Those items that did not make the baseline were placed in other categories such as research, development, legacy devices, or CD tools and were put into a queue to be handled by a follow-on UCDMO effort. New products are added to the baseline if they meet the following three criteria:

- **Capability.** Address a capability gap or extend current capabilities in a significant manner or lower cost.
- **Certification.** Complete certification testing with no findings of concern.
- **Lifecycle.** Lifecycle support and sustainment for at least three years.

By September 2007, UCDMO staff had grown to 30 individuals. The UCDMO management re-addressed their charter and goals and established four key initiatives to bring the communities together and solve the CD problem:

1. Strategic outreach and communication.

CD Baseline versus 2.1 (Released July 2007)		
Transfer	**Access**	**Multi-Level**
DSG 2.1	HP NetTop 1.3	ML Chat 1.0
DTW 3.4/3.4 N5	DTW 3.4/3.5 N5	TNE 9.0.1
ISSE 3.5B2	Janus 5.1	
MDDS 3.1	MDDS 3.1	
Radiant Mercury 4.0.5 P3	MLTC 3.0	
Smart.neXt 3.0	Secure Office Thin Client v1.1	
TDX 2.3		
TGS 2.1 P1		
TSABI OWT		

Table 1: *CD Baseline*

CD Capabilities	
Push Data	Subscribe/Distribute Information Feeds
	Post Data to Repositories
	Delivery to Specified Recipients
	Import Data
	Export Data
	Transfer Streaming Data
	Perform CD I&A and Attribute Management
Collaboration	Exchange E-mail
	Single Electronic Inbox
	Conduct Instant Messaging and Text Chat
	Shared Workspaces
	Audio Conferencing
	Video Conferencing
Centralized IT Management	Centralized IT Services (DNS, DHCP)
	Centralized Backup and Restore
	CD-Required Capabilities
	Centralized CD Audit
	Centralized Monitoring
	Remote CDS Administration
	Remote IT Administration
	Error Notification
Content Inspection and Release	Enforce Reliable Human Review
	Malicious Content Prevention
	Perform Attribute-Based Access Control
	Hidden Content Identification
	Enforce Content Policy
	Allow Policy Override
	Rules Management
Remote Access Centralized Repository and Other	Application Sharing
	Multilevel Data Repositories
	Network Reduction
	Desktop Reduction

Table 2: *CD Capabilities*

2. Transition to baseline and enterprise services.
3. Align DoD/IC policies and processes.
4. Manage a CD investment strategy.

These initiatives were developed to complement one another as well as address the lack of a single DoD/IC point of contact for CD activities, the disparate and inefficient policies and process, the duplication in research, development and testing, the excessive costs and security risk of managing point CD solutions, and the lack of a focused effort to meet the community's requirements.

The main focus of Initiative 1 is to provide one voice to all organizations involved in the CD space, whether it be customers, policy makers, or vendors. As part of the outreach element, the UCDMO leadership visits the combatant commanders, services, and agencies to provide information and solicit feedback on their recent initiatives and their long-term strategy. The UCDMO holds three types of official forums: customer, developer, and a yearly conference. The customer forum is held on a periodic basis to roll out major deliverables. The October 2007 customer forum was held at the Army Research Lab in Adelphi, Maryland, and was attended by approximately 250 individuals. The forum involved three days of interactive sessions describing the new implementation process and the associated DNI/DoD C&A transformation.

In November, the UCDMO held its first developer forum, known as Developer Days, to begin parsing through all CD research programs. In these sessions, a CD R&D program office provides CD program reviews to a community SME panel. During these reviews, the vendor and their associated government sponsor spend one hour providing information specific to their program, such as CD requirements being addressed, program milestones, status, funding profiles, and program risks. The UCDMO held successive Developer Days in February, March, and April. The recommendations from the SME panel will feed into the CD investment strategy discussed in Initiative 2. Additionally, the UCDMO will hold a yearly CD conference. The first conference was held in May 2007 in San Diego, California. More than 600 customers and developers attended the conference. The Honorable John J. Grimes, the Honorable Dale Meyerrose, and Vice Admiral Brown, JSJ6, were among the keynote speakers. This year's conference is being planned for October 2008. Information will be posted to the UCDMO Web site.

Initiative 2 will ensure that the commu-

nity moves from legacy point CD solutions to available baseline or enterprise CD services. Every CD connection introduces a risk to the networks and the data. CD solutions are complex and require lifecycle support such as installing security patches and updating malicious code software inspection mechanisms. Since the health of the CD mechanism is so critical to ensuring the security of the device, it is imperative that these devices be rigorously maintained. In the operational world, experience has shown that these devices are not being adequately maintained. The customer does not want the responsibility of deploying and maintaining the CD mechanism; what they want is the capability to share information across domains. Establishing CD enterprise services will solve this issue. Initial CD implementations at the enterprise will provide current CD baseline products in an enterprise capacity. To begin this transition, the UCDMO and enterprise service providers will partner with the customer to roll out CD enterprise services for customers requiring new or replacing legacy CD capabilities. In the DoD, Teresa White leads the DoD CD Enterprise service organization, and for the IC, Dan Nichols at Defense Information Agency is standing up CD services at regional service centers. The focus towards CD enterprise services provides users the required information sharing capabilities without the headaches of acquiring, certifying, accrediting and maintaining point CD mechanisms. Additionally, enterprise CD services will be the avenue for achieving global awareness of enterprise connectivity and greatly improve the security of our networks.

Initiative 3 is critical in ensuring common implementations throughout the community. The UCDMO is linked into the new DNI-led DoD/IC C&A transformation. One of the initial tasks was to develop a common set of security controls that will be recognized and accepted throughout both communities. This is the cornerstone to reciprocity in implementation, reusability, and efficiency. Additionally, the UCDMO has drafted a single CD implementation process that will eliminate the need for duplicative testing, promote sharing bodies of evidence, and provide accelerated approval for CD enterprise or baseline solutions. Both the security controls and the implementation process are available on the UCDMO Web site. The UCDMO is currently developing a series of CD profiles which will identify the minimum security controls required for a transfer, access, or multilevel mechanism. These profiles will assist the development organizations and can be used by vendors as build-to guidance as well as aid the testing organizations in ensuring a common and thorough set of standards. Implementing a common set of policies and procedures across these communities is more of a cultural challenge than a technical challenge. In the past, each community had separate standards and policies in addition to individual accreditation authorities. This may have made sense before our networks were so interconnected, but we must realize that every interconnection, every implementation of a CD solution puts our networks at risk. Many of the current connections were made based solely on mission need without sufficient consideration for protecting the networks and data. There is no arguing that success in moving to a centralized approach for implementing approved CD solutions will require a major cultural change. As the CIOs for the DoD and IC, John Grimes and Dale Meyerrose are committed to ensuring adequate protection of DoD and IC networks and are the catalyst for this change.

The 4th UCDMO initiative is developing a community-wide CD investment strategy. This initiative began almost immediately upon establishment of the UCDMO by consolidating the community CD requirements into a comprehensive list of 31 CD capabilities (Table 2).

Additionally, the UCDMO began to compile a list of all CD R&D efforts throughout the DoD and IC. Today, there is tremendous duplication among these efforts. Most of these programs are targeting the same five or six requirements. There is no coordination or even centralized tracking. It is very difficult for a customer to determine what other similar activities are occurring in the community. The UCDMO mapped the 31 capabilities to the currently available baseline mechanisms and to the known R&D activities resulting in a CD gap analysis. The UCDMO released Version 1.0 of the CD investment summary in March 2008. Additionally, they will provide CD investment recommendations to the CIOs. Some programs will be recommended for termination, others recommended for consolidation, and new programs will be suggested to target CD requirements gaps. The goal of Initiative 4 is to provide a focused, intentional, and targeted CD R&D program.

The UCDMO will also deliver an overall CD strategy for both the DoD and the IC in the CD Roadmap. Building on all four initiatives, this plan will lay the framework to ensure that CD will support both current and future information sharing.

CD is a critical enabler for implementing the President's National Security Strategy goal of information sharing[2]. The work of the UCDMO, coupled with support from the community, will make great strides in reaching that goal. Since its inception, the UCDMO has produced a CD baseline of products available for reuse, a list of known CD mechanisms in R&D, and a list of products that will need to be replaced in the next few years. In addition, a common DoD and IC process for CD implementation has been developed. The UCDMO has also made significant contributions to policies throughout the DoD and IC and will continue to have influence in the future. Success of the UCDMO requires a cultural change in which all partners work toward a common goal of enhancing our information sharing capabilities by fully supporting the UCDMO initiatives.◆

Reference

1. UCDMO. "Committee for National Security Systems Instruction 4009: National Information Assurance Glossary (CNSSI4009)."

Notes

1. A *tiger team* is a group of experts assembled for a set time to accomplish a specific task.
2. <www.intelink.gov/mypage/ucdmo>.
3. <www.whitehouse.gov/nsc/nss.html>.

About the Author

Marianne Bailey is the director of the UCDMO. She has been an employee of the federal government for 23 years and has recently finished a three-year leadership development program while holding positions in DISA and various other federal government organizations. Bailey has extensive IA experience and has provided IA guidance to a multitude of customers from the DoD, IC, and federal government sectors.

UCDMO
Phone: (240) 373-0796
Fax: (240) 373-0807
E-mail: ucdmo_outreach@nsa.gov

Acronym Key for This Issue

AIS: Assured Information Sharing
C&A: Certification and Accreditation
CIO: Chief Information Officer
CNSS: Committee on National Security Systems
DASD(IIA): Deputy Assistant Secretary of Defense for Information and Identity Assurance
DIACAP: DoD Information Assurance Certification and Accreditation Process
DIAP: Defense Information Assurance Program
DISA: Defense Information Systems Agency
DNI: Director of National Intelligence
DoD: Department of Defense
GIAP: GIG IA Portfolio (Management)
GIG: Global Information Grid
IA: Information Assurance
IC: Intelligence Community
INFOSEC: Information Security
IT: Information Technology
NII: Networks and Information Integration
NSA: National Security Agency
NSS: National Security Strategy
R&D: Research and Development
SME: Subject Matter Expert
UCDMO: Unified Cross Domain Management Office
USG: United States Government