# Distributed Mission Operations Cross Domain Solution Remote Management in Practice

**Bonnie Page Danner, CISSP**
**Northrop Grumman Information Systems**
**Orlando, Florida**
**Bonnie.Danner@ngc.com**

## ABSTRACT

The Distributed Mission Operations (DMO) Network operates Cross Domain Solutions (CDS) allowing warfighters in different simulation security domains to train together in daily events. The DMO Network requirement for remote CDS management led to a practical implementation meeting the needs of the warfighters, security implementers, and operators. Obtaining security approvals to remotely manage CDS in the classified environment is extremely challenging. DMO Network accreditation guidance states "Remote administration of the Controlled Interface is discouraged." Consequently, there are few remotely managed CDS applications operating today. Convincing the DMO Network Designated Approving Authority that trustworthy management systems operated from the DMO Network Operations Center would provide a higher level of assurance was achieved through evolving integration of Information Assurance requirements and capabilities into the developing Distributed Mission Operations Network Cross Domain Solutions (DCDS) architectures. The Certification and Accreditation demonstrated how the DCDS would contribute to the protection of the Controlled Interfaces located at remote mission training centers. This paper describes the drivers and requirements for remote management of the DCDS Systems that support the distributed training needs of the Combat Air Force.

Three versions of the DCDS implementation with remote management capability evolved over the past five years incorporating security and technology improvement with each new architecture. This paper discusses the need for the evolution and describes the most recent application and use of security capabilities in the DCDS remote management system. The paper provides an overview of accreditation achievement for the DCDS with remote management. In addition, the paper illustrates how the remote management solutions have enhanced the information assurance of the DCDS and how the capabilities work. The paper offers practical experiences with CDS remote management applications in the simulation and training world. Finally, this paper concludes with future considerations for CDS remote management and how it will help address emergent Combat Air Force DMO training needs.

## ABOUT THE AUTHOR

**Bonnie Page Danner, CISSP**, has more than 25 years of information technology experience in systems engineering, software development, and information assurance (IA). She has technical and project management experience on Department of Defense and civil federal programs, including leadership of DARPA, Navy, FAA, NASA, and Air Force Research & Development (R&D) programs and was Principle Investigator for Northrop Grumman IA Internal R&D projects. Bonnie's technical specialty is high assurance systems. Her technical experience includes multi-level security, formal methods, CDS, certification and accreditation, communications security, software safety, and independent verification and validation. Her modeling and simulation program experience includes JSIMS Security Lead and, currently, Northrop Grumman Security Engineering Lead for the Distributed Mission Training Program. She is the controlling authority for the DMO Network. Bonnie is Specialty Engineering Manager overseeing cyber security and network engineering and is currently managing DCDS Services tasking. Bonnie has published numerous articles in journals and conference proceedings on information assurance, software engineering, and field theory. She received a BS degree from Virginia Tech and a MS degree in mathematical sciences from Virginia Commonwealth University.

# Distributed Mission Operations Cross Domain Solution Remote Management in Practice

**Bonnie Page Danner, CISSP**
**Northrop Grumman Information Systems**
**Orlando, Florida**
**Bonnie.Danner@ngc.com**

## OVERVIEW

This paper describes an accredited and operational solution to a recognized Cross Domain Solution (CDS) need for remote management and administration. With the concept of emerging enterprise systems requiring communication between distinct security domains, the need for a centralized management solution has received growing attention from the security community in recent years.

At the start of the Distributed Mission Operations (DMO) Program, the United States Air Force Air Combat Command defined the need for multi-level security and CDS for recurring team training to support the war fighters. The DMO System Program Office, ASC/WNS tasked the Distributed Mission Training Operations and Integration contractor to implement a DMO Network CDS (DCDS) services capability for daily team training between war fighter communities with a requirement for communities to train together while operating at different security domains.

More than five years ago, the first implementation of the DCDS system provided a remote management capability for Combat Air Force DMO cross domain training. While the DCDS system meets a specific security need in the simulation and training environment, the overall remote management solution provides an example of viable risk reduction of unauthorized access for the Controlled Interfaces residing at remote mission training centers. The DCDS also offers the benefits of management and administration of remote assets from a centralized operations center where the security expertise resides.

### CDS Remote Management Challenge

Traditionally, CDS systems have been implemented on a single platform where local, privileged users manage and administer the overall system including controlled interface functions. Most all CDS systems approved for operation for Department of Defense applications are locally managed. Security guidance documentation and approval authorities are not favorably inclined toward remote management of controlled interfaces based on historical risk concerns. The perception is that remote management may create new and significant vulnerabilities to CDS systems with the introduction of an additional communications channel that is external to the controlled interface.

CDS systems require substantial security assurance evidence that the controlled interface polices/rules will perform as expected. Obtaining security approvals for remote management of CDS systems becomes a major challenge in any classified environment. Consequently, there are very few remotely managed CDS applications operating today. One example of accreditor reluctance is noted in the Joint, Air Force, Army Navy (JAFAN) 6/3 security accreditation guidance which states, “Remote administration of the Controlled Interface is discouraged.” The JAFAN 6/3 guidance specifies the security requirements for the DCDS system.

To achieve security approval for remote management the DCDS implementation and assurance activities provided evidence of strong access controls, successful performance of all security functions including those performed remotely, and a highly protected communications path between the Management System and the Controlled Interface.

### Meeting the CDS Remote Management Challenge

The DCDS design defines role based access controls for users (all privileged) to ensure only authorized users can perform their specified roles both locally on the Management System and remotely on the Controlled Interface. The security functions involving remote Controlled Interface management and monitoring are implemented with a secure operating system foundation. For example, the remote deployment of the Controlled Interface security policies/rules is restricted only to users specifically authorized to deploy the rules through mandatory access controls performed under the constraints of the trusted operating system policies.
The DMO Network operates in a closed environment with separate, National Security Agency (NSA) Type 1

crypto-nets. These crypto-nets are established for specific events where the security associations are set up for each event and taken down at the conclusion of the event. The specific communications channel between the DCDS Management System and the Controlled Interface is a partitioned, high domain crypto-net dedicated only for remote Management System communication with the Controlled Interface.

The DCDS protected environment, mandatory access controls, trusted operating system foundation and dedicated management crypto-net combine to meet the remote management challenge.

## BACKGROUND

Today, USAF distributed simulation training for Combat Air Force flight and mission crews occurs under the Distributed Mission Training Operations and Integration Contract. The DMO Network provides a contractor-owned infrastructure for CAF warfighter persistent, distributed training. The DMO Network enables both single domain and cross domain training events.

### Single Domain Events

The DMO Network includes Wide Area Network devices (Portals) located at each participant site and the Orlando-based Distributed Mission Training Operations Center (DOC). The DMO Network provides a secure environment that allows two or more simulation mission training centers to participate in a pre-scheduled training event. The DMO Network Portal translates mission training center message traffic allowing interoperability between different simulation protocols and does not distribute mission training center data used only for local training.

From the DOC the contractor manages multiple, concurrent mission training center DMO Network enclaves in support of the training events. An enclave consists of two or more DMO Network participant sites in the same security domain interacting in a training event on a single crypto-net. A crypto-net manager workstation in the DOC manages all DMO Network encryptors locally and at the mission training center sites. Only accredited, authorized sites with pre-signed security interconnectivity agreements are allowed to connect to the DMO Network. Personnel at each participant site perform their local support activities in accordance with DMO Network common security operating instructions and site internal security procedures.

### Cross Domain Events

The DCDS Protection Level 3 (PL3) (as described in JAFAN 6/3) conceptual architecture for cross domain event operation is illustrated in Figure 1. The PL3 DCDS consists of two main subsystems, the Controlled Interface located at each DCDS site, and the Management System located at the DOC. Figure 1 shows the PL3 Controlled Interface located at the high security domain site and managed through a dedicated crypto-net by the PL3 Management System resident in the DOC. A high security domain contains information that at least one participant in the low security domain is not authorized to access. Cross domain events may be conducted between high security domain enclaves and low security domain enclaves as depicted in Figure 1 with blue representing the high domain and red representing the low domain. The Controlled Interface performs all the security relevant decisions that govern the information flow between security domains. The deployed rule set/policy on the Controlled Interface determines whether or not information will be passed without alteration, modified and passed, or blocked between the security domains.

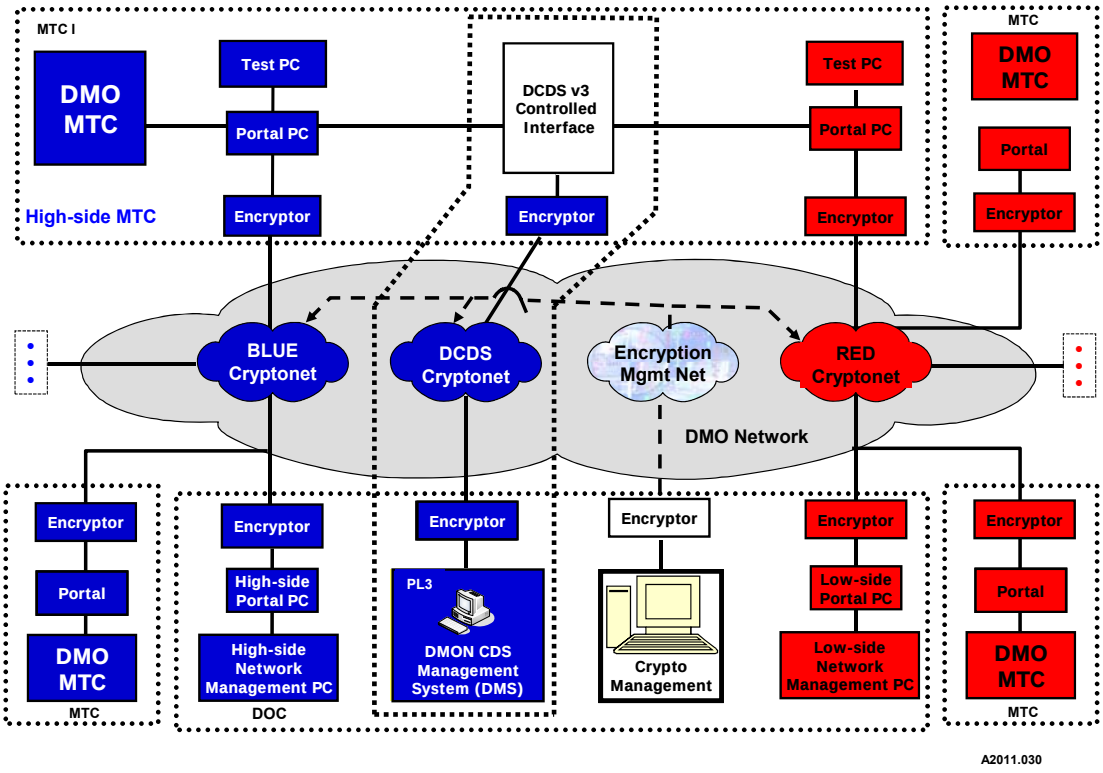


**Figure 1. DCDSv3 (PL3) Conceptual Operational Architecture**

## REMOTE MANAGEMENT DRIVERS

### DCDS Site Considerations

One of the paramount reasons for choosing to employ remote management of the DCDS was the existing DMO Network concept of operations. The current DMO Network event management process operates remotely. The DOC event managers in Orlando FL set up network security components and allow network connections to enable Distributed, Interactive Simulation (DIS) traffic to be exchanged by participating mission training centers. The historical precedence for remote management of DMO Network activities set the stage for using remote management of the DCDS. The DCDS matches the DMO Network from a network operational concept. Current DMO Network remote management activities, such as audit collection or Portal software update and control are similar actions needed to remotely manage the DCDS. Other considerations for management of the DCDS included issues that supported the rationale for remote management of the DMO Network. The security certification and accreditation boundary for the controlled DMO Network is situated between the mission training center and the DMO Network Portal. Because the DCDS Controlled Interface is deployed at a remote location, remote management solves a number of issues related to privileged user knowledge and access. One of the most obvious issues was cost to operate and maintain; the number of people who would have to be trained to manage the DCDS Controlled Interface is significantly less with remote management. DCDS management operations follow the existing DMO Network concept of operations. The DCDS Management System hosts the control and management applications that enable cross domain operations. DCDS Controlled Interface filtering rule/policy management is accomplished by operators located in the DOC; a process that is conceptually similar to the control of the DMO Network communications security or the setting up secure routes for training events. The DCDS Management System provides for segregation of operator roles, a capability which would be feasible but not economical if the equipment were managed at the remote locations.

### DCDS DOC Considerations

The DCDS requirements for local, secure, remote management and administration capabilities over the DMO Network led to the current DCDS security architecture. The DCDS architecture was devised to allow the Management System located at the DOC to

remotely manage and monitor the components of the Controlled Interface at a designated mission training center site.

The DOC-based Management System allows only privileged users the ability to remotely monitor and manage the Controlled Interface through the following:

- Separation and protection of management traffic and simulation data
- Direct monitoring and control of DCDS components
- Host-base firewall protections and alerts
- Implementation of NSA Type I encryption and Secure shell end-to-end privileged user access protections
- Password protected Basic Input-Output System (BIOS) settings for the controlled interface
- Operating system configurations that disable media drives
- Strict security policy enforcement.

**Trustworthy CDS Remote Management**

The individual components of the DCDS Controlled Interface and Management System are assembled and tested before the equipment is either shipped to the remote mission training center or installed in the DOC. The installation procedures and the associated configuration and functional tests ensure the DCDS is properly prepared for installation at the remote mission training center. The installation procedures ensure the authorized configuration is properly setup and the systems are secured via approved operating system hardening procedures.

Because the DCDS is remotely managed, the DCDS Controlled Interface is less susceptible to unauthorized alteration or tampering. Access to the DCDS Controlled Interface is controlled through a number of physical and automated access control features. The mission training center site agent controls access to the physical hardware needed to operate the DCDS Controlled Interface, but he does not control network operations. The DCDS Controlled Interface cannot be routinely accessed by mission training center personnel because they are not authorized to login to the Controlled Interface. In the case of the firewall Controlled Interface component, there is no operator interface at the mission training center. The other two DCDS Controlled Interface components are accessible at the site, but mission training center personnel are not authorized access, and access attempts are monitored through the DCDS access control and audit processes.

## THE DCDS REMOTE MANAGEMENT EVOLVING SOLUTION AND IMPLEMENTATIONS

Over the past five years, the DCDS has achieved eighteen different site accreditations at specified Combat Air Force DMO mission training centers. Two more approvals are pending with an additional two in the operational testing phase. All of the solutions implement remote management and administration of the Controlled Interface.

Over time, the DCDS system has evolved to the current version 3 architecture to meet changing requirements and address new constraints. Through the version evolution, remote management capabilities continue to be a significant strength of the solution providing a means to monitor and administer cross domain events from the DOC in Orlando.

**DCDSv1**

The DCDSv1 Management System supported the operational concept for cross domain mission training capability through the use of a trusted operating system to impose role based access control on the DCDS. DCDSv1 remote management capabilities maintained control over the use and application of filtering rules/policies. The DCDSv1 was capable of maintaining access control over the principal components and operation of those components, but audit limitations restricted logging of individual transactions of the Controlled Interface during cross domain operations. The DCDSv1 Controlled Interface and Management System were capable of monitoring the numerical count of the DIS Protocol Data Unit (PDU) operations within the Controlled Interface.

The DCDSv1 limitations when monitoring and recording individual PDU transactions resulted in a need to employ test tools that evaluated the DCDS to support mission training operations (See Figure 2, DCDSv1, Remote Management Architecture, below).

The test tools provided additional confidence that the statistics reported by the DCDSv1 Management System were representative of the cross domain activity. The DCDSv1 Management System also has limited maintenance capabilities for the remote DCDSv1 Controlled Interface. These limited remote maintenance capabilities were partially the result of deliberate vendor design restrictions related to the major component of the DCDSv1 Controlled Interface.

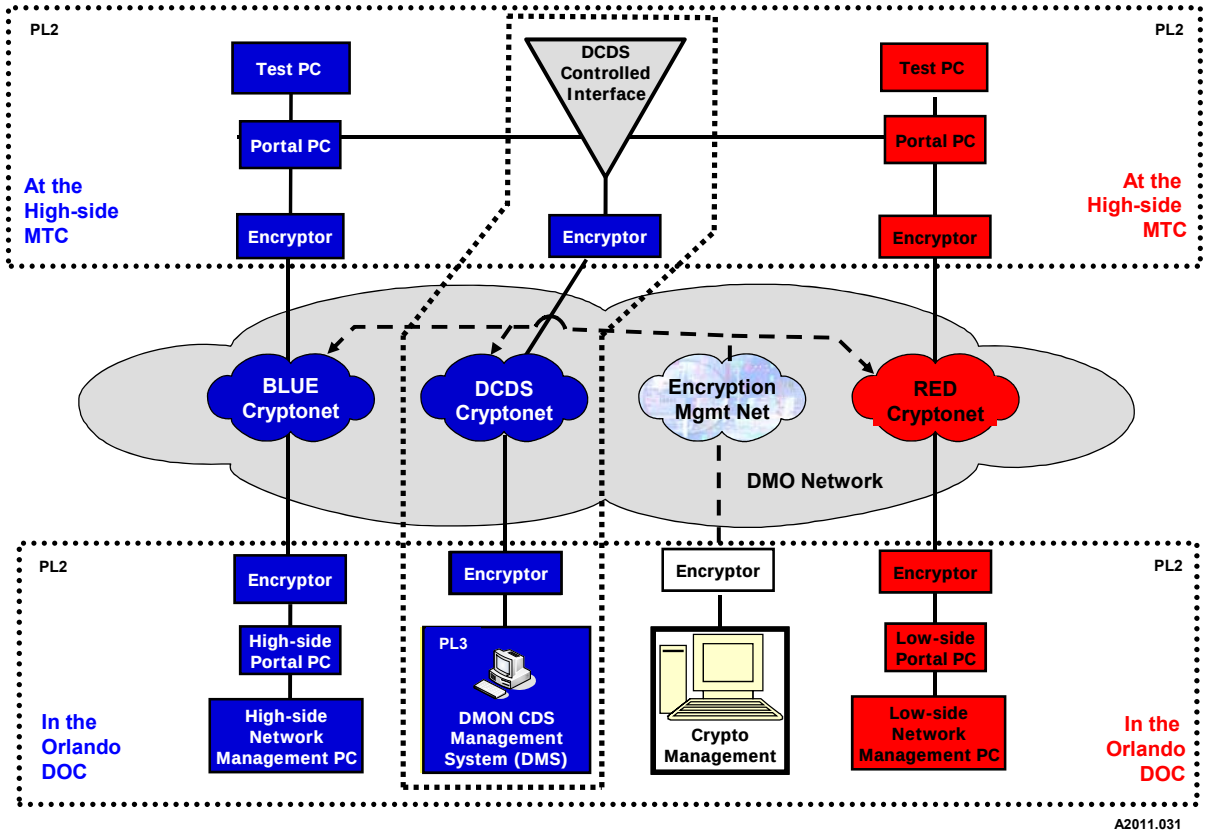


**Figure 2. DCDSv1 Remote Management Architecture**

## DCDSv2

With the introduction of a new and more complex mission training center simulator platform for DCDS implementations, there was a need to examine the continued supportability of the DCDSv1 hardware/software architecture. As part of this examination, the DCDS team explored DCDSv1 viability for use with the new platform requirements and identified obsolescence associated constraints. Added complexity arising from the new simulator platform led to the determination that DCDSv1 would not completely address the new requirements without causing training impacts.

The DCDSv1 trusted operating system vendor announced plans to discontinue trouble shooting and support for the specific version used for DCDSv1. Additionally, the Controlled Interface component vendor announced an upgrade that would pose new limitations on future rules/policy development reinforcing the need for a DCDS architecture enhancement.

As a solution to address these new constraints, the DCDS team enhanced the existing DCDSv1 architecture using an improved Controlled Interface software product. The product had achieved a previous CDS accreditation in another environment under a different government organization. After discussions with the developers, the product was determined to be an excellent way forward for DCDSv2 to meet the needs for the DMO's new mission training center platform.

After option considerations and trade-off evaluations by the DCDS engineering team, the Management System was deployed on a new secure operating system platform to avoid near term obsolescence concerns and take advantage of the trust evolution. The new operating system and Controlled Interface software provided an even stronger security foundation for DCDS remote management and administration. The specific architecture for DCDSv2 is similar to the DCDSv3 architecture discussed in the next section.

**DCDSv3**

The third version of the DCDS architecture, DCDSv3, provides full Controlled Interface capabilities including complete transaction accounting for the operations of the Controlled Interface. The addition of policy driven LINUX Security Extensions, Advanced Intrusion Detection System Environment (AIDE), and restricted communications path through specified Internet Protocol (IP) tables have enhanced the trustworthiness of the DCDS. The improved monitoring and transaction management capabilities of the DCDSv3 Controlled Interface and Management System enhance the ability of the system to maintain accountability for the DIS PDU transactions within the Controlled Interface. Expanded logging and audit capability add to the assurance provided by enabling real-time examination of selected operations and by supporting realistic retention of cross domain mission training events. Role based access control is maintained in the DCDSv3 with the addition of the "Operator" role who, as the name implies, is responsible for proper operation of the DCDSv3 during daily mission training events. Other privileged user roles in this latest version continue compliance with the least privilege concept. The enhanced security features of the DCDSv3 are realized with a much simpler architecture (See Figure 3, below). The need for external data recorders to capture PDU transactions is eliminated for the DCDSv3 Remote Management architecture.

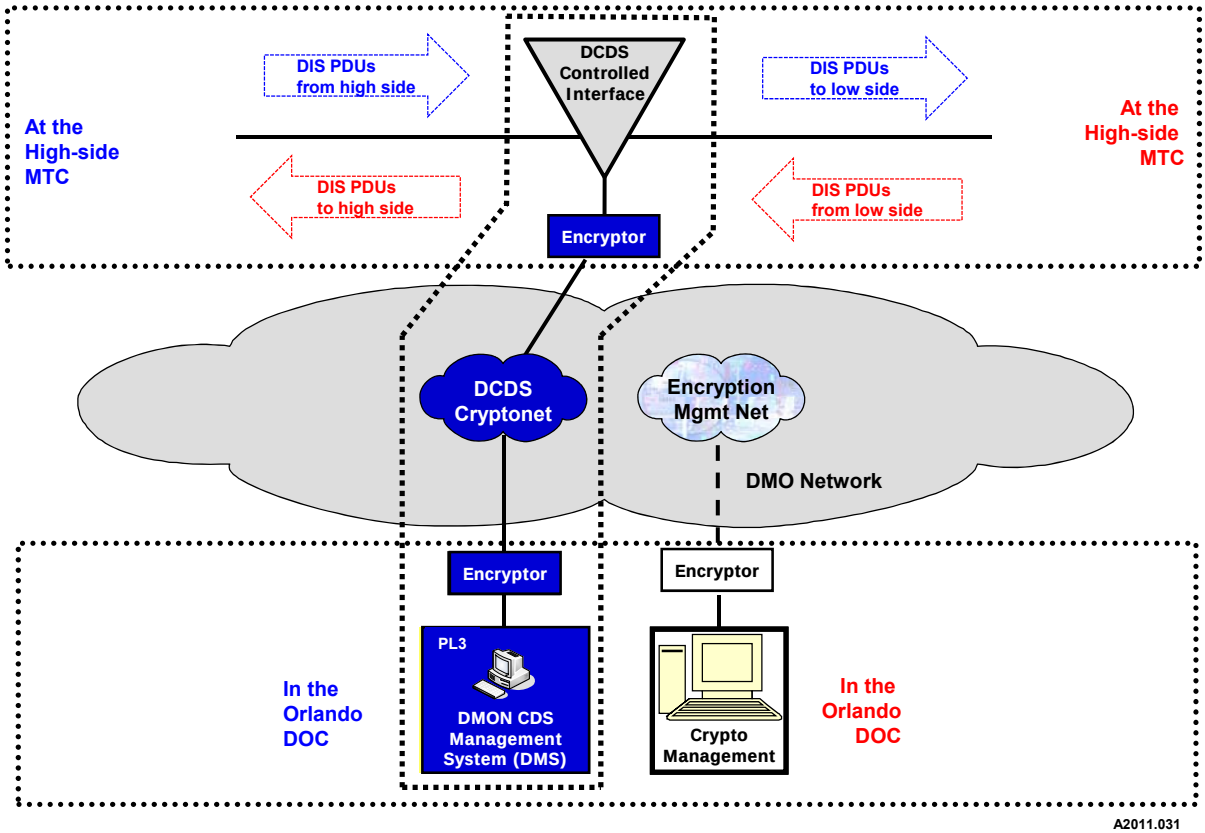


**Figure 3. DCDSv3 Remote Management Architecture**

## DCDS CERTIFICATION AND ACCREDITATION

DCDS Certification and Accreditation involves a number of activities and the associated documentation to report on those activities to the Designated Approval Authority. The source for the security requirements applied to the DCDS is JAFAN 6/3 accreditation guidance applying the PL3 requirements for specified Confidentiality, Integrity and Availability where the Level of Concern approved by the Designated Approval Authority is High, Basic (with some Medium requirements) and Basic, respectfully. All of the appropriate JAFAN 6/3 requirements have been

mapped to specific DCDSv3 security capabilities and features. The DCDS Certification Test Plan was developed to describe how to demonstrate, via a variety of tests, to the Designated Approval Authority that the DCDS provides sufficient assurance that data identified by the high side security domain will not be shared with low side security domain participants. Further, the remote management of the DCDSv3 was approved by the Designated Approval Authority and satisfies all of the specific JAFAN 6/3 security requirements (Section 7.B.2.k (1)-(6)) applied to a Controlled Interface using remote management.

**Meeting the JAFAN 6/3 DCDS Certification and Accreditation Process**

As previously mentioned, JAFAN 6/3 discourages remote administration. The following excerpt from the JAFAN 6/3 captures specifically the remote administration security requirements:

| Section | Requirement |
|---|---|
| 7.B.2.k | Remote administration of the Controlled Interface is discouraged. All remote administration of Controlled Interfaces requires written approval of the Designated Approval Authority. If remote administration is employed, the session must be protected through the use of the following techniques: |
| 7.B.2.k(1) | Strong authentication, *and either* |
| 7.B.2.k(2) | Physically separate communications paths, *or* |
| 7.B.2.k(3) | Logically separated communications paths based upon either |
| 7.B.2.k(3)(a) | NSA-approved encryption; *or* |
| 7.B.2.k(3)(b) | NSA-approved encryption and Designated Approval Authority - approved privacy encryption to provide privacy of the remote administration session. |
| 7.B.2.k(4) | Direct user access to the Controlled Interface shall require strong authentication. |
| 7.B.2.k(5) | ISSO, or ISSM have the obligation to ensure that the Information Systems comprising the interconnected Information System provide the required security functionality. |
| 7.B.2.k(6) | The introduction of a Controlled Interface does not impact the determination of the Protection Level or Levels-of-Concern of the Information Systems comprising the interconnected Information System. |

**Certifying Remote Management Capability**

The process of certifying the DCDS Remote Management Capability is embedded in the certification test and evaluation process, There is no special emphasis on showing that the DCDS satisfies JAFAN 6/3 security requirements. The principal technical requirements: strong authentication, separate communications paths and NSA approved encryption, are basic elements of the DCDSv3 Management 'net.' Security requirements relating to event monitoring, transaction logging and audit are the same requirements applied to the entire DCDSv3 architecture.

## DCDS REMOTE MANAGEMENT EXPERIENCE

The Management System has evolved as the other elements of the DCDS were updated and enhanced. The DCDSv1 Management System, while accurate, was not complete in the ability to provide persistent transactions records for the actual DIS PDU handling. The following descriptions recap the enhancements of the DCDSv3 Management System in several operating segments:

**Remote Management System Features/Capabilities**

Specifically, the DCDSv3 captures the incoming PDU, evaluates it, and then dispositions the PDU by either dropping, guising or passing unaltered the PDU based on the filtering rule. If modifications to the PDU are required, the modified PDU is recorded in a transmission log. PDUs which are unaltered or dropped are recorded once; guised PDUs are recorded when received and recorded when sent out. Each of the transactions is logged and becomes part of the audit record. The enhanced monitoring capabilities are also evident in the test and evaluation process. The Certification and Accreditation testing includes two "blind" operational test events (Phase 3 and Phase 4) where the mission training center prepares a "typical" training scenario for cross domain training. The Phase 3 test is a single domain test but the scenario produces DIS PDUs to be filtered by the DCDSv3 Controlled Interface just as they would be created during actual cross domain training. The DCDS Certification and Accreditation test team does not participate in the scenario development except to explain the requirements for particular types of PDUs to be included to exercise all technical rules in the security policy.

The DCDSv3 has the capability to capture and record all incoming PDUs, as received, evaluate, and act on

the PDUs based on the filtering rules. The DCDS Operator can select individual PDUs to examine as the scenario is progressing without interrupting the data flow. While the volume of data that makes up a DIS mission training event is too large for human review of every PDU transaction, the DCDSv3 offers the capability to select PDU types to focus on during the Certification and Accreditation test events and during day-to-day mission training events.

**Preparation for Cross Domain Events**

The first DCDS version had to overcome a long held belief that precise monitoring of the DMO Network DIS PDU stream was not possible. Throughout the DMO Network history, efforts had been made to compare PDUs sent from one mission training center with PDUs received at a second mission training center, and by all accounts those efforts had moderate success, but were never able to account for each PDU. The initial DCDSv1 event preparation for test events evolved to the stage where the test tools and the DCDS Controlled Interface were recording exact numbers for PDUs generated and received. These statistics formed the assessment basis for the operational DCDSv1 and have been the foundation for each subsequent version.
With DCDSv3 the amount of setup and event preparation activity is reduced. Attention to the same issues regarding control of data flow through the DCDS is the same with v3. However, with Designated Approval Authority approval and authorization of DCDSv3 operation for day-to-day mission training, the DCDSv3 is able to operate without external log file recorders and the events can be conducted without the extraordinary review efforts common in the DCDSv1/v2 operational environments.

**Cross Domain Event Execution**

The typical mission training event is initiated by one mission training center wanting to train with another unit, currently within the same security domain. The DCDS offers training opportunities where mission training centers with common mission components that operate in different security domains can train together without fear of compromise of the high side sensitive information. This translates into requirements that must be met when developing training scenarios and conducting pre-and post-mission briefings. Those issues are beyond the scope of this paper, but suffice it to note that the mission training centers are working those issues with their major command's assistance.
The technical process for setting up a DCDSv3 supported mission training event is done within the current time lines defined for the DCDSv1 cross domain event. Essentially, setup is expected to take 60 minutes versus 30 minutes for a current single level DMO Network event. The added preparation time is needed to setup the external log file recorders and to give the Event Managers and the DCDS Operator sufficient time to ensure all configuration steps to create the cross domain environment have been completed.

During the cross domain mission training event, the DCDS Operator can select and review individual PDU transactions and track the operation of the remote DCDS Controlled Interface components. The additional DCDSv3 logging capability affords the DMO Network management and operations community the opportunity to examine individual PDUs analyzing security and non-security issues. Finally, audit of the cross domain event becomes a near real time activity. As the enhanced audit functions become more mature, more sophisticated alerts and advisories can be added enhancing the assurance that the DCDS is maintaining proper control over high side sensitive data.

**Cross Domain Event Completion**

At the end of a cross domain event supported by the DCDSv1, the log file recorder and DCDS Controlled Interface statistics are compared to determine if there is any reason to suspect a spill of high side information into the low side. Any mismatch of the PDU counts can result in tens of hours of data analysis to resolve the mismatch.

For the DCDSv3 cross domain training events, the need to depend on the external data recorders is eliminated. Capture of all PDUs that were passed between the different security domains ensures that suspicious data can be reviewed within the Management System and issues resolved in a more timely manner. In addition, the process of retrieving log files at the conclusion of the cross domain event becomes unnecessary because the DCDSv3 logging process is accomplished throughout the course of the event, potentially reducing the event time by as much as one and a half hours.

**System Administration and Maintenance**

Remote management facilitates remote administration and maintenance of the deployed DCDS components and software. The DCDS Management System accommodates privileged user access from the DCDS Management System in the Orlando DOC. With the privileged user access controls for the DCDS Management System and the role based access control implemented on the remote components, routine

maintenance and, when required, software maintenance can be accomplished without having to visit the distant mission training centers.

## SUMMARY - LESSONS LEARNED

The deployment of the DCDSv1 proved that a Controlled Interface was a viable solution for conducting DIS mission training events with mission training centers that operated in different security domains. The issues with DCDSv1 led to the realization that a truly reliable cross domain solution depended on a remote management capability to provide assurance and accountability. In addition, the administration and maintenance experiences with the earlier DCDS versions led to addition of the security features to the DCDSv3.

The DCDSv3 has significantly reduced the level of effort necessary to setup and conduct a cross domain mission training event. The addition of Linux Security Extensions policies enhanced system access control which provides greater accountability in turn enabling additional remote capabilities beyond monitoring the DCDS Controlled Interface during training events. The added logging of PDU transactions bring all required audit data into the boundary of the DCDSv3 eliminating the need to depend on external log file recorders. Having the PDU transactions as part of the audit logs for a particular training event reduces the amount of time needed to complete the event. The DCDS Management System architecture also enabled real time assessment of data flowing through the DCDS Controlled Interface.

## FUTURE CONSIDERATIONS

Remote administration and management of the DCDS continues to be a key discriminator for the current system. USAF warfighters have the ability to conduct daily team training across different security domains under a persistent approval to operate the DCDS on the DMO Network. With the provision of significant security assurance evidence to the approval authorities the remote management solution helped reduce security management concerns at each remote mission training center DCDS. As the DMO Network continues to grow adding new participant sites and new security domains, assessment of the security posture of the remote management solution will be important.

### Evolving Technology

With a Global Information Infrastructure Enterprise focus on CDS and recognized goal for centralized security management, the Unified Cross Domain Management Office (UCDMO) oversees the evolution of common solutions. These solutions are increasing in complexity in environments more open than the tightly controlled DMO Network environment.

There is an emphasis across government to develop secure, centrally managed CDS systems to meet the enterprise need for cross domain information sharing. New technologies and approaches will evolve from CDS enterprise research and development initiatives. These new technologies and approaches may or may not prove to be directly applicable to the DCDS remote management solution implemented and accredited for DMO training today. Staying current with technology advances and new remote management approaches will be critical in determining the future path for DCDS implementation and the evolution of the remote management approach.

### Meeting Emergent CAF DMO Training Needs

As the DMO Network continues to grow**,** new security guidance, airframe platforms, simulation training strategies and technologies are emerging that may require additional considerations for DCDS and the remote management capabilities. The DCDSv3 architecture is currently robust enough to meet new requirements with relative ease. With the flexible policy/rule set management capability and strength of the security systems present in DCDSv3, straightforward system modifications will be possible. These changes may come from the need to address such things as rule set/policy and management complexities associated with larger enclaves, classified DMO standards evolution, common-models enhancements, additional degraded operations functions, and advances in technology.

## ACKNOWLEDGEMENTS

Special recognition is warranted for the significant contributions to this technical effort provided by Mr. Gene Williams, CISSP, ISSEP, FITSI-D, senior security engineer at Cobham Analytics Solutions. The author wishes to thank the following USAF ASC/WNS technical advisors for their guidance and support: Mr. Heath Morton, Mr. Mike Baker, Mr. Ken Nairn and Mr. Mike Mills. The author thanks Mr. Bob Chapman of ACC/A8AZ and Mr. Rich Grohs of ACC/A8TN for their insight and support and Ms. Beth Powell of

SAF/AAZ for her security guidance. The author also expresses gratitude to the O&I contractor contributors to DCDS planning and preparation including, Mr. Bruce McGregor, Mr. Desmond Holoman, Mr. Dennis Smith, Mrs. Kelly Djahandari, Mrs. Joan Archer, Mr. Joe Osorio, Dr. Khanh Bui, Mr. Logan Rodrian, Mr. Craig Conrad, Mr. Martin Leidy, Mr. Chris Huey, Mr. Randy Hobbs, Mr. Charles McElveen, Dr. Tony Valle, and the Orlando, Johnstown, and Hampton DOC, NOC and DTC teams.

## REFERENCES

ASC/WNS and DMT O&I Contractor (2010). Cross Domain Solution Configuration Management in the Simulation Training Environment, *I/ITSEC 2010, Paper 10049*

CAF DMO O&I Contractor (2004). *Draft DMON MLS Guard O&I Contractor Workshop Report.*

DMT O&I Contractor (2001). *DMO Integration Standards* and *DMO Common Definitions* from https://secure.dmodmt.com/standards/index.cfm

DMT O&I Contractor (2002). Multi-Level Security Feasibility in the M&S Environment, *I/ITSEC 2002, Paper 167.*

DMT O&I Contractor (2005). *Multi-Level Security* Assessment for the Distributed Mission Operations Network, *I/ITSEC 2005, Paper 2165.*

DMT O&I Contractor (2006). A Distributed Mission Operations Cross Domain Solution for Recurring Team Training, *I/ITSEC 2006, Paper 2775.*

DMT O&I Contractor (2008). Cross Domain Solution Policy, Management, and Technical Challenges, *I/ITSEC 2008, Paper 8343*

DMT O&I Contractor (2009). Cross Domain Solution Challenges Transitioning from Concept to Operations, *I/ITSEC 2009, Paper 9133*

DMT O&I Contractor (2009). Cross Domain Solution Certification and Accreditation for Persistent Simulation Training, *I/ITSEC 2009, Paper 9142*

DMT O&I Contractor (2010). Implications of Interoperating with Non-Hierarchical Security Domains, *I/ITSEC 2010, Paper 10041*

DMT O&I Contractor (2010). Cross Domain Rule Set Verification Tools and Process Improvements, *I/ITSEC 2010, Paper 10042*

DMT O&I Contractor. Applying Cognitive Work Analysis to Event Management, *I/ITSEC 2010, Paper 10052*

DoD (2000). Memo for Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510,

*Department of Defense Global Information Grid Assurance.* DoDI 5200.40 (1997).

*Department of Defense Information Technology Security Certification and Accreditation Process DITSCAP.*

DoD, *Joint Air Force, Army, Navy (JAFAN) 6/3 and Manual* (2004).

NSA (2003). *Guard Certification Test and Evaluation (CT&E) Handbook Version 2 .0.*

NSTISSAM (1999). *Common Criteria for Information Technology Security Evaluation.*

NSTISSAM COMPUSEC (1999). *Advisory Memorandum on the Transition from the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation.*

NSTISSP 11 (2000*). National Information Assurance Acquisition Policy*