Cross Domain Solution Challenges Transitioning From Concept to Operations

Kelly Djahandari, Joan Archer, Bonnie Danner
Northrop Grumman Corporation
Orlando, Florida
Kelly.Djahandari@ngc.com, Joan.Archer@ngc.com, Bonnie.Danner@ngc.com

ABSTRACT

Combat Air Force (CAF) Distributed Mission Operation (DMO) has the mission to train pilots, weapon system officers, and Command, Control, Intelligence, Surveillance and Reconnaissance (C2ISR) crew stations for the U.S. Air Force. To support this mission, the DMO Network (DMON) connects geographically separate mission training center simulators located throughout the world to conduct day-to-day team training events. The continued success and growth of the CAF DMO program over the past nine years has facilitated the introduction of a needed capability to allow participants in different security domains to train together.

Over the past two years the CAF DMO Operations and Integration contractor has been fielding and testing a DMON Cross Domain Solution (CDS) to enable warfighters from different simulation security domains to train together on a common network infrastructure. After successful completion of testing and certification requirements, the DMON CDS received an authorization to operate. Many technical and non-technical challenges were addressed during the transition. Transition elements in the areas of testing, deployment, accreditation, training, and event operations were anticipated. Other elements such as operational security concerns, expanded scope of coordination efforts, and the extent and complexity of configuration management presented significant challenges. This paper presents several of the challenges experienced during the transition from the DMON CDS concept and test environment into the CAF DMON CDS day-to-day operational training environment. This paper describes lessons learned from the experience.

ABOUT THE AUTHORS

Kelly Djahandari is a security software engineer at Northrop Grumman Information Systems and is leading a Cross Domain Solution Research and Development task order under the DMT program. Her information assurance experience includes more than 12 years of software engineering and project management in network security research. She has co-authored several conference papers on previous work in automated intrusion response approaches. She received a bachelor’s degree from George Mason University and a master’s degree from the University of Virginia.

Joan Archer, CISSP, is a Security Engineer at Northrop Grumman and is supporting all of the Cross Domain Solution efforts on the DMT program. Her information assurance experience includes 12 years in varying capacities as a Security Engineer, Information Security Analyst and Information Security Consultant. She received a bachelor’s degree in computer information systems and business administration from Strayer University.

Bonnie Page Danner, CISSP, has more than 20 years of information technology experience in systems engineering, software development, and information assurance. She is currently managing Distributed Mission Operations Network (DMON) Cross Domain Solution Services tasking. She received a bachelor’s degree from Virginia Tech and a master’s degree in mathematical sciences from Virginia Commonwealth University.

Cross Domain Solution Challenges Transitioning From Concept to Operations

Kelly Djahandari, Joan Archer, Bonnie Danner
Northrop Grumman Corporation
Orlando, Florida
Kelly.Djahandari@ngc.com, Joan.Archer@ngc.com, Bonnie.Danner@ngc.com

INTRODUCTION

The challenges involved in the evolution of a USAF Distributed Mission Operations Network (DMON) Cross Domain Solution (CDS) from research concepts to actual implementation and operations are significant. Cross domain solutions are necessary to meet the Combat Air Force (CAF) Distributed Mission Operations (DMO) vision. This vision is to train pilots, weapons system officers, and command, control, surveillance, and reconnaissance crew members in a realistic manner mirroring the actual warfighting environment in daily simulation training missions.

During 2008 and early 2009, CAF DMO cross domain solution services efforts resulted in approvals to operate a persistent cross domain capability at five different DMON Mission Training Center (MTC) sites for three different rule sets. The success in achieving the approvals was the culmination of government and contractor hard work and dedication overcoming and addressing many management and technical challenges along the way. With the cross domain capability still new for DMON training events, there will be additional challenges ahead as new issues arise and lessons learned evolve from daily cross domain operational use.

This paper presents background information on the DMON CDS, herein referred to as DCDS, and its transition from early concept to daily operations. This transition required addressing numerous technical and non-technical challenges, many anticipated and some unanticipated. Anticipated challenges included the need to create a repeatable rule set development process, the need for extensive testing, and challenges concerning deployment, security accreditation, operations personnel training, and development of CDS procedures for event execution. Unanticipated challenges included new operational security concerns, expanded effort for complex coordination, and the extended effort required for stakeholder involvement in the cross domain solution services configuration management to maintain the approvals to operate the DMON CDS. It describes many of the efforts to address challenges and apply lessons learned over the tasking time frame. The USAF DMON CDS tasks have involved both research and services areas moving from concepts to operations over the past eight years.

BACKGROUND

The DMON has provided connectivity between geographically separated USAF Mission Training Centers (MTCs) allowing daily collaborative team training for air combat missions in the same security domain for over eight years. In 2009 the DMON received security approval to operate allowing daily team training between different U.S. security domains using a cross domain solution. The cross domain solution allows higher security domain sites to train effectively and realistically with sites at a lower security domain. The DMON Operations and Integration (O&I) contractor responsible for DMON operations has transitioned from operating only single level training events to operating both single level and cross domain training events.

Single Level DMON Event Overview

The DMON O&I contractor operates and maintains the DMON and coordinates daily team training events. Encrypted network connections (also called cryptonets) between the MTCs, which create a private network for a specific event, are disabled until all systems and security readiness are confirmed. Preparation by the sites and the O&I contractor occurs before the MTCs are connected for a training event. Single level event management has evolved and become routine. Multiple single level events in a number of different security domains are conducted daily.

CAF DMO Portal Overview

Each DMON MTC has a Portal located at the site to provide simulator connectivity to the DMON. Figure 1 shows simulation traffic data flow during mission team

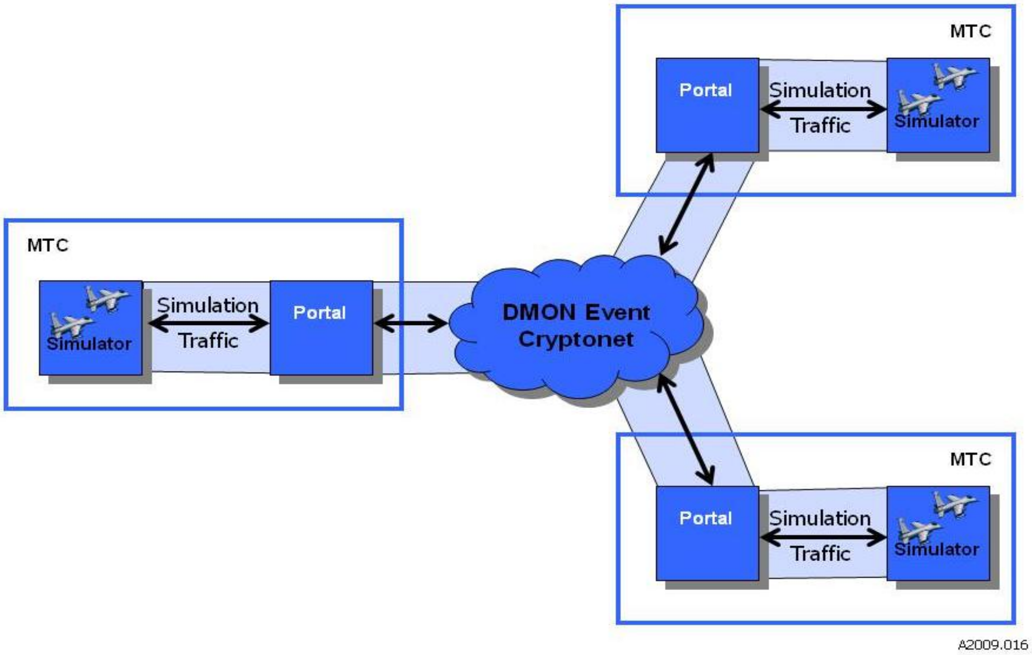

Figure 1 DMON Single Level Mission Training

training between three MTCs at a single security level. DMON Operations Center Event Managers manage the remote site Portal to provide interoperability between the MTC simulators. Event Managers configure each site Portal to connect to each of the other site Portals participating in the event. The Portal sends and receives simulation data to and from the MTC simulator(s) and simulation data to and from each remote Portal participating in the event. Mission data flows only between the MTCs in a specific event.

DMON Cross Domain Solution (DCDS) Overview

A cross domain event involves MTCs operating in two different security domains (high and low) that share a common low security domain battlespace connected through a cross domain solution. The DCDS is a collection of hardware and software that includes a controlled interface that provides the mechanism for executing a rule set. Each DCDS controlled interface resides with the Portal at the high-side MTC and is remotely controlled by a management system located in the DMON Operations Center. The DCDS was accredited in accordance with Joint Air Force, Army, Navy (JAFAN) 6/3 Protection Level 3 (PL3) security requirements. Also located at the high-side MTC are high-side and low-side proxy servers which are Protection Level 2 (PL2) components used to perform limited data conditioning before and after processing by the controlled interface.

The DCDS ensures protected data is not shared outside of its domain by permitting only authorized Distributed Interactive Simulation (DIS) Protocol Data Units (PDUs) to traverse its boundary. The DCDS protects data bi-directionally by blocking, guising and passing, or passing without change, DIS PDUs in accordance with its deployed rule set. Only one rule set is deployed on the controlled interface. Figure 2 shows the data flow of the simulation data in a cross domain training event.

Hosted on a trusted operating system, the DCDS Management System provides role based access control with each privileged user having a defined role, enforced by the system and there are no general users. However, for auditing purposes, privileged users have personal accounts into which they log on before assuming their roles. Assigned roles give users the authorization and privileges necessary to run specific software applications with limited functionality. An example of some of the responsibilities of the roles include the Rules Administrator who verifies the correct rule set is deployed, Information Systems Security Officer who performs start up and shutdown, Security Administrator who performs security-related tasks, and System Administrator who performs routine system administrator tasks.

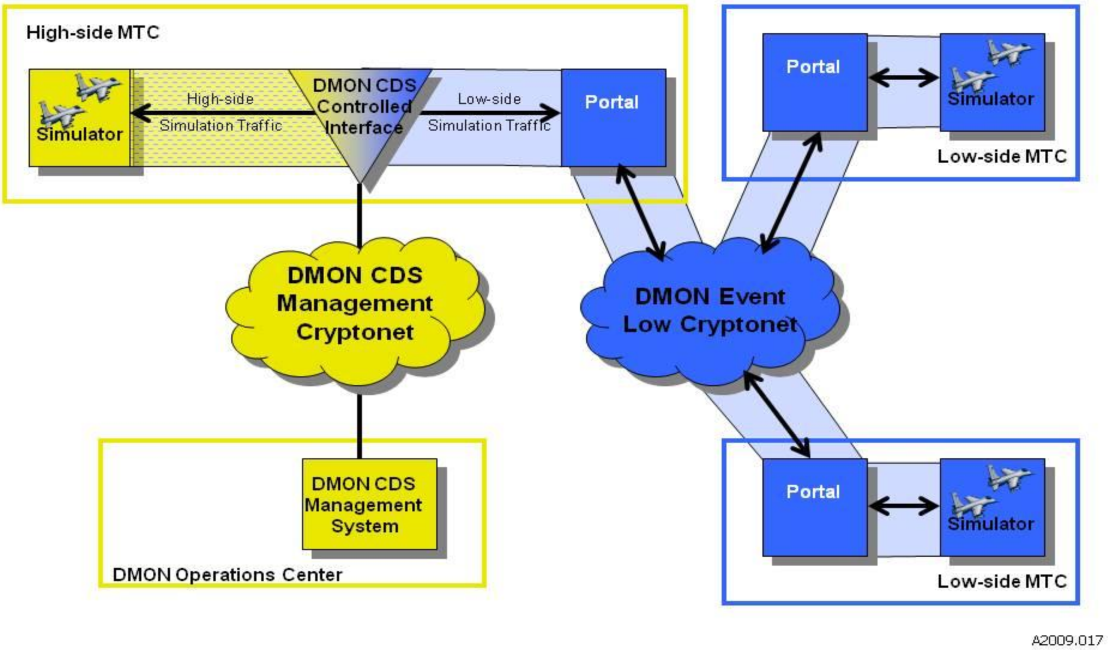

Figure 2 DMON Cross Domain Mission Training Data Flow

The DCDS controlled interface provides a separate out-of-band management network interface which supports all configuration and programming interfaces to the device. The DCDS controlled interface connects to the Management System via the dedicated management cryptonet which allows configuration, rule set deployment, audit logging, and viewing of system health and statistics. Figure 2 shows a DCDS mission training event with the two security domains separated by cryptonets. The Management Cryptonet for DCDS management activities is illustrated in yellow, and the Event Cryptonet which allows the MTCs to perform team training in the low security domain battlespace is illustrated in blue. Another separate high-side cryptonet (not shown in Figure 2) is created between the DMON Operations Center and high-side LAN, used for setting up the high side test machine for data logging and configuring the high-side Portal if needed, but simulation data does not flow through this cryptonet.

Four phases of security testing are conducted on each DCDS. Phase 1 test procedures verify the proper configuration, integration, and functioning of the DCDS components in an unclassified environment. After Phase 1 testing is complete, the equipment is ready to be shipped to the MTC site. Phase 2 tests the classified rule set using classified log data in the classified environment on standalone DCDS test equipment. For Phase 3 testing, a single level test event is performed with the high-side MTC and a “fake” low-side MTC, both operating at the same security level, using live simulation traffic. For Phase 4 testing, a cross domain test event is performed with a low-side MTC operating at the low side security level. Both Phase 3 and Phase 4 tests run at least three separate test events using scenarios developed to exercise all the rules in the rule set. Approvals are needed to perform Phase 3 and Phase 4 testing.

ANTICIPATED CHALLENGES

The DCDS transition from concept to daily operations is still evolving. Throughout the transition, numerous technical and non-technical challenges were successfully resolved while some remain in the resolution process. Many of the challenges were anticipated and some unanticipated. Anticipated challenges included the need to create a repeatable rule set development process, the need for extensive testing, and other challenges concerning deployment, security accreditation, technical and operational personnel training, and development of CDS procedures for event execution.

Rules Set Development Process

The DCDS takes actions based on the instruction given by its implemented rule set. Ensuring each rule set was thoroughly vetted and concurred with by all parties with a vested interest in the protection of the high-side data was of paramount importance. Initially, this was very challenging due to the lack of a defined process for creating, testing and attaining concurrence on a rule set. Although Rule Set Working Groups existed and provided initial Rule Set consensus, consistently having in attendance the requisite skill sets to provide subject matter guidance and obtain consensus was very difficult. From the working groups came only the recommendation of a rule sets sufficiency, in the form of an English Language Rules Plan, which was then sent for concurrence with the DAA. Once the English Language Rules Plan achieved concurrence, the rule set was implemented into system code which was then tested. Once fully tested, the results of the rule set testing were presented to the DAA for rule set approval.

Rule Set Working Group members include many different subject matter experts including; pilots, simulator builders, DIS protocol experts, controlled interface builders, security engineers, aeronautical simulation experts, and concurrence from program security representatives. Rule Set Working Groups make decisions on what sensitive information a given high-side domain is required to protect yet still provide adequate training to the low-side participants. They accomplish this by identifying what and how simulation data is passed, blocked, or guised and passed. This information is assembled into an English Language Rules Plan.

Determining the correct balance of high-side data protection with training effectiveness was very difficult and time consuming. Simulation data sent to the low-side had to be examined to ensure both high and low-side domain participants would receive effective training. For example, deciding to block all high-side data would have no security ramifications, but would result in unproductive team training for the low-side participants.

Another responsibility of the Rule Set Working Group was to address the non-technical components of a rule set. Technical rules alone executing in the CDS are insufficient to provide proper separation between the two domains (e.g., technical rules cannot execute on simulated voice radio). Non-technical rules are rules that involve one or more of the following: certifications of simulator implementations, mandated security procedures or operational rules, constrained scenarios, and restrictions on personnel. Certification of the simulator implementation requires the simulator developer to certify that the software is implemented as required for correct operation of the DCDS rules. Mandated security procedures refer to any additional event specific requirements that are given as part of a specified event. Operational rules refer to the actions or procedures needed to constrain aircrew behaviors, restrict actions that low-side observers could draw inference from, and the prohibiting of activities that would directly compromise security during a CDS event.

Extensive Testing

As anticipated, one of the greatest hurdles in attaining the approving authorities' confidence was to ensure that once implemented, the testing diligence of the DCDS met the needed assurance requirements. To accomplish this, the testing process defined and approved during the concept stage was reused, only modified slightly to adjust for the additional documentation requirements as identified by the approving authorities.

The testing of the DCDS consisted of completing the testing phases as described above. Initially during the Phase 3 single level testing, the team received observations and inputs from the low-side operators, who are cleared to the high-side, regarding the effectiveness of the team training. They indicated a need for inclusion of information on the low-side to improve team training. The requested information was not being blocked for security reasons, but constrained because of broad restrictions contained in the rule set. This observation prompted the need to have low-side operators who are cleared for high-side discussions invited to participate in the Rule Set Working Groups to assure useful team training by the low-side participants.

Another area identified during implementation testing was the need for more complex test event planning to complete the Phase 3 and Phase 4 testing simultaneously at sites where possible. Overlapping site testing allowed the DCDS team to complete Phase 3 testing activity of one rule set while waiting for an Interim Approval To Test (IATT) to conduct Phase 4 testing of a different rule set at different MTCs. Close coordination with all implementation activities was essential to perform parallel installation, configuration, deployment and testing of multiple instantiations.

Prior to the initial test event at a site, classified teleconferences were conducted with site personnel to discuss rule sets and scenario planning, and to answer scenario development questions. A DCDS team member was also assigned to communicate directly with the sites during site test event planning, coordination, and scheduling. Test events were scheduled as early as possible and considered alternate test periods for test data recovery to limit training impacts on the MTCs.

One specific note of difficulty was that scheduling test events in August and September became difficult due to training conflicts from time pressures for more training at the end of the fiscal year and the scheduling of some large-scale training events. Since warfighter training on the DMON must have priority over testing, scheduling test events as planned was difficult and not always possible. For future planning, the DCDS team recognizes that September testing should be avoided, but if any testing required in the September time frame, it must be scheduled as far in advance as possible.

CDS Deployment

The deployment of multiple, simultaneous DCDS implementations required significant coordination with the sites. Achieving timely coordination was both difficult and challenging compounded primarily due to schedule compression. To alleviate this problem, several actions were implemented. Pre-coordination meetings with all new DCDS sites were conducted to educate each site about the DMON CDS prior to the scheduled site survey. Site surveys were enhanced to include gathering information such as space and power resources needed for the addition of the new equipment. New equipment approval authorizations needed to be attained and communicated to the site prior to DCDS equipment shipment and installation and proposed testing schedules were communicated as soon as the information was available. Coordinating and communication this information in advance knowledge allowed more effective scheduling of MTC resources.

In addition to improvements in the coordination and communication with the MTC site personnel, the team also addressed improvements in the DCDS equipment deployment. Deployment activities of the DCDS equipment at the MTC now include equipment installation, configuration, connectivity testing, single level security testing of the DCDS, and training of the Site Agent personnel. A security engineer member of the DCDS team now accompanies the installation team. The security engineer conducts connectivity and configuration testing with the DMON Operations Center during the equipment installation, trains Site Agents early, and discusses DCDS questions with site personnel. In addition, the DCDS team now schedules single level security testing at the site during the site installation. This provides system and security engineering support at the operational site for single level DCDS tests and helps shorten the testing schedule.

CDS Type Accreditation

Each step of the security accreditation approval process had challenges for both the DCDS team and the customer. Much of the documentation that supports Certification and Accreditation (C&A) of the DCDS is the same for each site implementation. With five sites replicating the same DCDS architecture, the challenge was to identify the best way to leverage the same documentation, streamline the testing process and in the case of implementing the same rule set for a second or subsequent implementation, reduce the testing requirements for each MTC implementation. To best address this challenge, type accreditation of the DCDS was sought. The process of type accrediting the DCDS was used as a means to eliminate the need to separately accredit or re-accredit the DCDS components for each deployment.

The C&A package created for requesting type accreditation included the following documents: Security Requirements Traceability Matrix; System Security Plan; Risk Assessment; Privileged Users Guide; Certification Test Plan; Controlled Interface Certification Test procedures; Controlled Interface Functional Test procedures; the subsequent test results from each phase of testing. One additional requirement identified from the previous implementation was a request to present the test results in a format that included the testing methodology, and requirements traceability from the classification guide to the system security assurance features mapped to their respective test results. This resulted in the creation of the rules implementation plan and later rules implementation report.

The DCDS type accreditation package did not include rule sets as they are independent of the DCDS hardware and software architecture and design implementation. Each DCDS rule set required individual approval prior to its first use in Phase 4 testing. The type accreditation concept also facilitated a reduction in the amount of testing for deployment of previously approved rules to additional sites. For DCDS implementations involving the same rule set at additional sites, the testing required for the new site was limited to completion of the Controlled Interface Certification Test and a single

Phase 3 test before requesting approval for Phase 4 testing at the new site.

The type accreditation request served as a means to reduce the amount of DAA documentation review required and reduce the amount of testing needed to demonstrate proper DCDS configuration and correct rules deployment for the new MTC. The DCDS team requested the DCDS type accreditation after the implementation and successful completion of Phase 4 testing of the first site.

Operations Personnel Training

Cross domain events are scheduled and conducted differently than single level events. The transition from single security level event operations to both single level and cross domain event operations brought about several changes to the environment. Some of the changes included identifying how to best integrate the new equipment into the existing environment, who would operate and manage the components, and how they would be trained. During testing, DCDS engineers had performed the operation of the CDS equipment.

DMON single level training events are conducted by operations personnel called Event Managers who configure and manage the DMON for recurring daily training events. The integration of the DCDS equipment to the DMON environment required modifying Event Manager roles, developing new policies, procedures, and training materials, and providing training. Also, due to the separation of roles and least privilege implementation on the DCDS Management System, a minimum of two people of separate trusted roles are required for a cross domain event requiring an additional Event Manager or event management support person to be identified and trained.

Training existing single level event managers on the additional tasks and complexities introduced by the DCDS equipment was accomplished by initially limiting the amount of additional actions necessary to be performed by the Event Managers by supplementing the operations team with Event Support personnel from the DCDS team. The tasks between the Event Manager and the Event Support personnel were divided to alleviate the Event Manager workload in cross domain event setup and shutdown.

In addition to their normal training event equipment configuration preparation, setup, and assurance checks, Event Managers' responsibilities for cross domain events included verifying the correct software version is implemented at the high-side MTC, using the DCDS Management System to confirm the desired rule set is deployed to the controlled interface, assisting with the start of recording tools and logs for the cross domain event.

Event Support personnel responsibilities for cross domain events included ensuring the DCDS Management System is communicating with the controlled interface, performing audit archives, starting additional recording tools and logs, saving the statistics and performing audit log archives, and event shutdown procedures. After the cross domain event, the Event Manager assists the Event Support person in verifying the controlled interface statistics are correct.

CDS Site Procedures

Implementing the DMON CDS into the operational environment also created the need for new procedures at each DMON CDS site. The procedures identify the proper operation and maintenance actions for the DCDS equipment. New Site Agent procedures for the DCDS site were created for the high-side sites. Low-side sites had only a minor requirement to sign the new DMON Interconnection Security Agreement with the CDS Annex, in which they agree to the understanding that any DMON participant may be included in a CDS event and the risks associated in doing so.

The new Site Agent procedures for the DCDS identify the event setup, proper disk insertion on all equipment, powering up the high-side and low-side proxies, and powering up the controlled interface. When all personnel, system, facility, and procedural security are appropriate and ready for the cross domain event, the site agent faxes a Security Readiness to the DMON Operations Center that verify that the site meets the operational and security requirements for operating in accordance with the DMON Interconnection Security Agreement and the Common Security Operating Instruction.

A revision to both the event request ticket and event readiness fax was also required due to the changes associated with scheduling a CDS event. The revised forms provide a means for the site to verify they are using the approved software version, confirm and record that operational security briefings have been conducted, and that all procedures are being followed for a CDS event as identified in both the Common Operation Security Instruction and Interconnection Security Agreement. Changes were made to both of these documents to account for the additional requirements introduced by cross domain events.

Brief and Debrief

Both briefing and debriefing are important for effective mission training, however cannot easily be accomplished during a cross domain event. A pre-mission briefing is usually conducted before an event to communicate important event information. A post-mission debriefing is usually conducted to reflect on the overall training experience and replay the mission event if desired.

To address this challenge, non-technical operational procedures instruct sites to conduct mass brief/debrief at the lowest common security domain. This is an inconvenience for the high-side sites since they must change drives in the Portal and simulators taking additional time to perform, however no further solution is currently available. Improving cross domain event mass brief/debrief remains an unsolved challenge and research and development of a solution is being pursued.

UNANTICIPATED CHALLENGES

Unanticipated challenges included new operational security concerns, expanded effort for complex coordination, and the extended effort required for stakeholder involvement in the cross domain solution services configuration management to maintain the approvals to operate the DMON CDS.

Operational Security Concerns

Operational Security (OPSEC) challenges experienced during the deployment of the DCDS spanned across deployment, site process changes, event operations, and brief/debrief areas. During the initial stages of DCDS development and coordination activities, the instruction was given not to disclose a CDS implementation at a specific site because of overly restrictive protection policies. This created many challenges to all life cycle stages from the initial concept and architecture discussions, through procurement, testing, training and into the implementation stages. The security representatives later granted the approval to discuss the DCDS locations as needed in an unclassified environment as long as no specific DCDS details were specifically identified. This approval allowed for the continuation of normal DMON event procedures without additional internal OPSEC constraints for the scheduling and event management processes.

Prior to operations, the OPSEC focus at a site becomes ensuring that the controls needed at the high-side site for a successful cross domain event are in place. Of primary concern is that the high-side site receives the OPSEC briefing. The OPSEC briefing covers all of the responsibilities for that site not controlled technically by the DCDS. OPSEC rules are briefed to the high-side and low-side participants, scenario developers, pilots and operators before every cross domain training event and include instruction about specific actions to be taken or not taken during a cross domain event.

Expanded Effort for Complex Coordination

A significant challenge introduced by the deployment of multiple DCDS implementations was the need to communicate and coordinate all plans activities and expectations early and regularly. During the previous CDS task, lessons learned provided the example that without continuous and diligent communication and coordination efforts with the DAA, Security representatives, Government personnel site personnel and subject matter experts, failures due to insufficient communication generally resulted.

To address this challenge, the DCDS team communicated with the customer regularly to pass along plans and status information to support their requirements. The complexity involved in tracking the status of five implementations and three rule sets made the exchange of status information challenging on both sides. The customer created a status matrix tool to address the challenge. This tool tracked the planned, anticipated and actual testing, requests and approvals dates on a single spread sheet. The DCDS team updated the matrix monthly which the customer in turn used to update the DAA.

An experience from the first installation identified that the sites receiving the DCDS desired very early communication from both the DCDS team and the government. This site communication explained the general DCDS purpose and ultimate plans for testing and implementation going beyond the normal receipt and installation of DMON equipment. These early communication efforts improved coordination with the site stakeholders and proved necessary to help with the scheduling of DCDS test events that supported the C&A assurance.

Configuration Management

The creation of the DCDS Security Configuration Management Plan was a vital activity required prior to transitioning to the operational DCDS. Strict configuration control of DCDS and related interface security baselines is essential to ensure continuation of secure DMON operations, security maintenance of DCDS rule sets, and validity of the security approvals for operation. The DCDS Security Configuration Management Plan went through several reviews and modifications as the configuration items and Configuration Management processes were clarified and refined.

A key component of the configuration management process is the Configuration Review Board, which is crucial to the successful maintenance of the DCDS accreditations and continued cross domain operations on the DMON. The board was established to review security impact analysis statements and approve security relevant change requests before they can be deployed. The Configuration Review Board processes require careful determination of necessary and acceptable configuration items to be controlled by a stakeholder board. Any changes that may affect the DCDS configuration item baselines and/or affect technical or operational rules for the DCDS will trigger the need for the Configuration Review Board process. Close coordination with the DAA and all stakeholders is required to ensure adequate understanding of the security impacts of proposed changes to the MTC simulation baseline, the DMON Portal, the DCDS software, hardware, and rule sets.

CONCLUSION

The successful transition from concept to the operational DCDS provides the warfighter with the ability to train in their simulators across different security domains in day-to-day team training events and is another step forward in their efforts to train like they fight. The challenges experienced through the transition provide valuable lessons learned that have and will continue to improve DCDS operations.

ACKNOWLEDGEMENTS

The author wishes to thank the following USAF 677th AESG technical advisors for their guidance and support: Mr. Patrick Imlay, Mr. Lou Schwieterman, Mr. Andy Hostetter, CAF DMO O&I PM; and Mr. Mike Mills. The author thanks Mr. Bob Chapman of ACC/A8AZ and Mr. Rob Hunter for their insight and support. The author also wish to express gratitude to the O&I contractor contributors to DCDS planning and preparation including; From Northrop Grumman; Ms. Lisa Harris, DMT O&I Program Manager and senior engineer, Mr. Bruce McGregor, senior manager and senior systems engineer, Mr. Desmond Holoman, network engineer, Mr. Joe Osorio, systems engineer, Ms. Cindy Walker, security engineer, Mr. James Multeri, CM specialist, Mr. Shane Marcus, systems engineer, Mr. Benjamin Leppard, software engineer, Mr. Jim Bryan, systems engineer, Mr. Logan Rodrian, software engineer. From SPARTA/Cobham; Mr. Martin Leidy, security engineer, Mr. Charles McElveen, security engineer, Mr. Gene Williams, security engineer, Dr. Tony Valle, subject matter expert and modeling and simulation engineer, and from SERCO-NA, Mr. Steve Howard, subject matter expert,.

REFERENCES

DMT O&I Contractor (2002). Multilevel Security Feasibility in the M&S Training Environment. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2002,* Paper 167.

DMT O&I Contractor (2005). Multilevel Security Assessment for the Distributed Mission Operations Network (DMON). *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2005,* Paper 2165.

DMT O&I Contractor (2006). A DMON Cross Domain Solution (*CDS*) for Recurring Team Training. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2006,* Paper 2775.

DMT O&I Contractor (2008). Cross Domain Solution Policy, Management, and Technical Challenges. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2008,* Paper 8343.

DMT O&I Contractor (2009). Combat Air Force Distributed Mission Operations (CAF DMO) Network Users Guide, Version 1.0. Retrieved June 22, 2009, from *https://secure.dmodmt.com/document.cfm?id=2248* .

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