How to Connect an Unclassified Trainer to a Classified Trainer in Five "Easy" Steps

William Kaczor
MTS Technologies, Inc.
Orlando, FL
kaczorw@mtstech.com

Craig Thornley
PEO STRI
Orlando, FL
craig.thornley@us.army.mil

ABSTRACT

In today's evolving security environment, decreased live training budgets are inevitably producing an increased need to connect their replacements: Classified and Unclassified training systems. Connection solutions have been limited because of specified, goal-driven requirements of achieving security certification and accreditation and protecting the cross-classified data. This paper defines five "easy" steps required to connect a Classified trainer or simulator to an Unclassified system. The five steps include certifying and accrediting the system, identifying the appropriate Multiple Security Level (MSL) and Cross Domain Solutions (CDS) solution, obtaining the memorandum of agreements for connectivity, validating and testing the solution, and operating the system securely throughout its lifecycle. We will also demonstrate the options used to accomplish this once rare and daunting connection.

For each identified issue, the discussion will include the security requirements for the connectivity of systems at different classification levels and recommend technical and procedural solutions. Critical to understanding how connectivity is achieved are the discussions of the meanings and detailed examples of MSL/CDS. The MSL and CDS solutions discussion will focus on "baking in" security into the initial design so that an approved solution can be implemented. Requirements to secure trainers from corruption by malicious code and to filter data traffic to ensure that only approved data types are passed will be examined, including the need to protect the Classified data from access by unauthorized persons. The processes, tools, and configurations required for such connectivity have not been used to their fullest extent.

The Department of Defense and industry team can achieve the Learn, Train, and Win objectives by maintaining a paramount principle, the required protection for Classified data, yet allowing Unclassified trainers to participate. All trainers, regardless of classification can, with the proper MSL/CDS solutions, provide the training our military can afford, requires, and deserves.

ABOUT THE AUTHORS

William Kaczor is the Department Head for *MTS Technologies, Inc* in Orlando, Florida and has been in the Information Assurance field for nine years as well the IT realm for over 15 years. He has a Bachelors degree in Information Technologies with a specialty in Networks and Network Security and has multiple security certifications including Information Assurance Security Officer from the US Army and Cisco Certified Network Administrator. He has certified and accredited over 50 training and operational systems for all four branches of the DoD and is currently the Lead Security Engineer for the VH-71 Presidential Helicopter. He has completed a Master's in Business Administration (MBA) degree and achieved the Program Management Professional (PMP) Certification.

Craig Thornley serves as the Information Assurance Program Manager (IAPM) for the Program Executive Office for Simulation, Training and Instrumentation (PEO STRI). Craig is responsible for Information Assurance of a $1.6 billion a year organization with over 1,025 military, civilian, and industry personnel servicing over 334,000 training systems around the world. He holds a Bachelor's of Science in Electrical Engineering (BSEE) from the University of Central Florida and has specialized training in security engineering and IA. Craig has completed 20 years of service to the Government focusing on military intelligence and IA.

How to Connect an Unclassified Trainer to a Classified Trainer in Five "Easy" Steps

William Kaczor
MTS Technologies, Inc.
Orlando, FL
kaczorw@mtstech.com

Craig Thornley
PEO STRI
Orlando, FL
craig.thornley@us.army.mil

FRAMEWORK: WHAT ARE CDS AND MSL?

Have you ever been sitting in an H-60 Black Hawk trainer wishing that you could be flying missions with the classified USMC AH-1 or AH-64? Have you ever been flying in an F/A-18 E/F/G for the US Navy or US Marine Corps and wanted to coordinate with an Unclassified, ship-based air traffic controller trainer through a Classified exercise network? Have you ever used an Army Forward Air Controller training simulator and wanted to work with new pilots, whether US, NATO, or allied, to help perfect the delivery of munitions?

Did you know that you can complete all of these connections…at once? This paper will discuss the five easy steps in which a cross domain solution (CDS) can be designed, implemented, fielded and maintained. The Information Assurance (IA) umbrella covers cross domain solutions, multiple security levels (MSLs), and multi-level security (MLS) and allows training and operations to span different levels of classification, as long as the necessary and acceptable levels of security are in place.

This paper will not be an IA training course for certification and accreditation (C&A), nor will it be a rehash of the widely published regulations. This paper will demonstrate the path to connect an Unclassified or lower classified trainer to a higher classified trainer quickly, cost-effectively, and with the least amount of road blocks along the way. This paper will also demonstrate how to connect a trainer to a NATO or allied training system while protecting US classified data. Finally this paper will clearly define the means, methodology and ease of connecting an unclassified trainer to a classified trainer to provide the train as we fight environment.

A large misnomer is that security and information assurance are difficult activities to complete during the acquisition and development of a new training system. The training and development of a Government or industry IA team is critical to the success of any training system's certification and accreditation. This experienced team is doubly important while trying to implement a CDS/MSL solution. Once the Government and industry integrators and developers realize and accept that they need specialized assistance from IA experts or they need to invest in training their people to become IA experts, security loses its black hat aura. The cost of setting up your team will come in one of two packages; having internal or external IA experts on day one or paying a larger fee to have a crash IA implementation of your system after activities begin. Security should be second nature if information assurance is "baked in" to system design and development and IA should be implemented from the very first day of system design.

Several types of solutions exist that can be used to connect Unclassified/Classified systems for different information security needs, including file transfer, real-time data at rest, data separation, data-in-transit protections, virtual machine classification separation, and adding Unclassified voice and video to a Classified network. The basic definition as Defense Information Systems Agency (DISA) defines a CDS as "a form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains."

The highlighted and main focus of these regulations is to ensure separation and protection of Classified and Unclassified networks. Protection of Classified data is the overarching concern and must be the direct goal for planning to use a CDS, MSL, or MLS. The implications of contaminating an Unclassified network or having Classified info exposed to those without a clearance is highly dangerous and can be very costly to fix. The prospect of having to purge an entire network due to classified data exposure is frightening, but can be avoided simply by planning for the IA and Security controls to be implemented from day one of the project.

The main directive of the Department of Defense (DoD) CDS is the Chairman Joint Chiefs of Staff

Instruction (CJCSI) 6211.02b regulation. Its vision is "to provide net-centric, service-oriented, cross domain information sharing solutions with guaranteed quality of service for authorized users anywhere on the Global Information Grid (GIG)." This translates to approval for connectivity between different classifications, but requires users follow the guidelines to make the connection possible.

IA is a requirement assigned to all DoD Information Systems (ISs) and is discussed several dozen pages into a statement of work. IA is a requirement that should be a critical path item, but is often not until it is pointed out in a contractual Integrated Product Team (IPT) meeting. The methodology of a CDS/MSL is even less thought about due to the perception of it being too hard, unnecessary, or just not thought about. The add-on capability is incalculable when a training system can provide as realistic a training scenario as possible.

A CDS, in its simplest sense, allows a network or trainer of a lower classification to pass specified data onto a Classified network or source. The protection mechanism prevents or limits data flow back to the Unclassified side. Depending on the methodology, filtered data from the Classified environment can be passed to the Unclassified network, allowing for a real-world training mission to be accomplished at a much lower cost. The lowered cost and decreased risk result from using processes already approved instead of "reinventing the wheel."

A MSL solution can also be a CDS, but it is more defined and can span multiple domains of classifications. The domains usually involve several different approving authorities and different classifications or at least "need to knows."

MSL is a method of separating different levels of data by using separate PCs or virtual machines for each level. It aims to give some of the benefits of MLS without needing special changes to the operating system (OS) or applications, but at the cost of requiring extra hardware.

A MLS is the application of a computer system to process information with different sensitivities (that is, at different security levels), permit simultaneous access by users with different security clearances and need-to-knows, and prevent users from obtaining access to information for which they lack authorization.

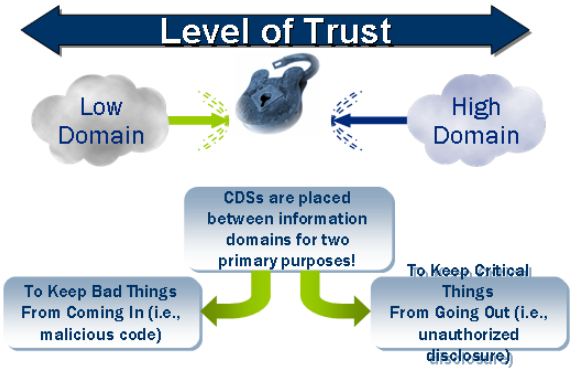

Figure 1. Levels of Trust

COMPARE AND CONTRAST CDS, MSL, AND MLS

CDSs always have a safety mechanism built in to the architecture to prevent malicious data or inappropriate data from going across them (if they didn't, they wouldn't be any more useful than a crossover cable between the networks). These safety mechanisms are virus scanners, "dirty word" filters, document dissemblers (for example, to take a Microsoft® Word® document and convert it to plain text or Adobe® PDF®), etc. Additionally, auditing, intrusion detection, file change management, real-time scanning, and intrusion prevention are needed, depending on the systems used, for a successful CDS solution. The type of safety mechanism primarily depends on what kind of network or trainer the system is connecting to.

MSL should not be confused with MLS: MSLs are limited to separate application displays. and downgrading of information can result in loss of valuable data.

WHY DOES DOD NEED CDS OR MSL?

No approved open or direct connections to the very stern rule that a Classified system may not connect to an Unclassified system have occurred. The separation of classifications has been paramount in the past and will continue to be that way in the future. The assurance of the protection of Classified data is paramount and necessary to operate a CDS.

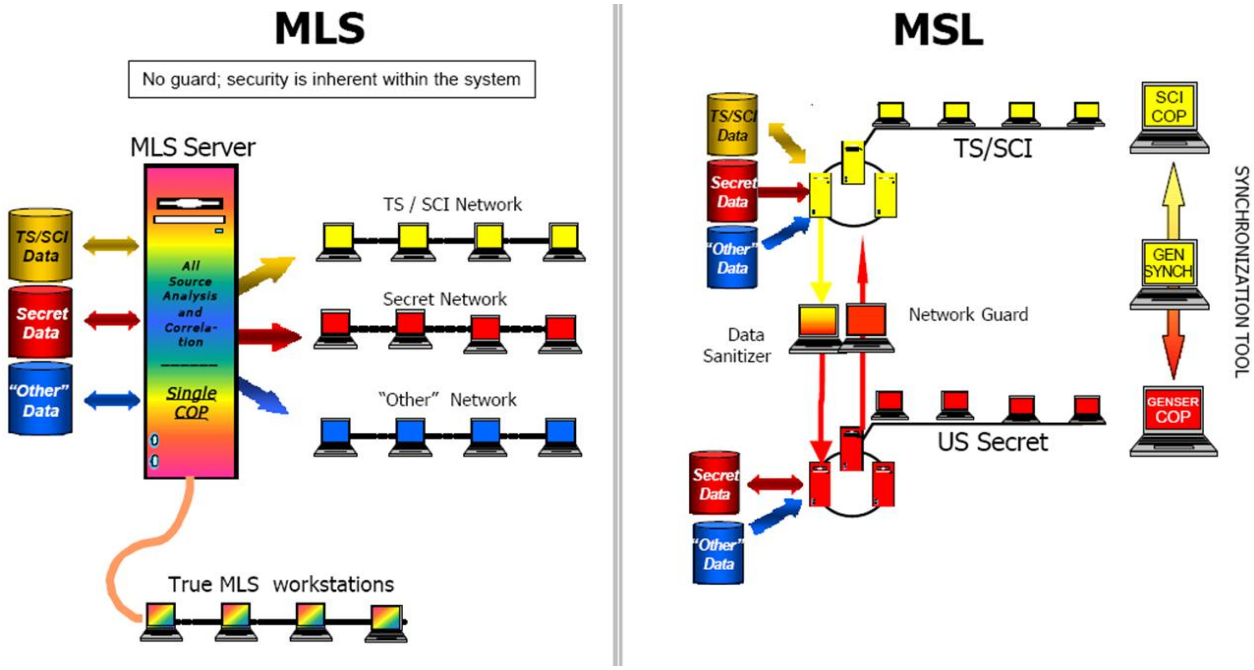

Figure 2. MLS and MSL

With the dwindling budgets for real equipment training, simulators and trainers are being used more frequently as real-world substitutes. The training systems of tomorrow will most certainly need the ability to provide as realistic training as possible. This may involve the use and dissemination of classified information.

The need to train Warfighters to handle cross classification scenarios is paramount to their survivability and their execution of a real-life mission. So why wouldn't a training or operational command want to have the capability to connect Unclassified and Classified trainers through a CDS to support a robust training event? The cost savings alone, as compared to not training in a realistic environment, justify the initial expense of adding a CDS or MSL to any and all training systems.

SO HOW *DO* YOU CONNECT UNCLASSIFIED TO CLASSIFIED?…OR THE 5 "EASY" STEPS

The Five "Easy" Steps are in fact nothing more than following current DoD policy and directives to achieve the Authority to Operate (ATO) and the Authority to Connect (ATC). The steps also include C&A, Identifying the Appropriate CDS/MSL Solution, Connecting the Systems, Validation and Test of the connections, and Maintaining the Security During Operations.

The term "easy" is used in this description so as to state that if adequate planning, development, testing, and maintenance of the trainer are accomplished, an ATC/ATO can be achieved. In addition to the technical process, key programmatic issues, such as cost and schedule, need to be identified at the start of the program. The "baking in" of the IA controls during the planning phase allows for the Government customer and contractor to view the path forward. The early identification of the IA requirements ensures that they are built into the design and schedule. Testing, both self inspection and formal, will guarantee that the IA requirements are being met and that the system is secure. Maintenance keeps the system safe during operation and avoids any unintentional exposure for Classified information.

The bottom line is to plan for security, build security, validate the appropriate and necessary securities are in place, and continue to protect the system. If all of these steps are completed, then two systems of differing classification, using an approved CDS, should be allowed to connect. The best way to achieve this solution is to use team work.

What better way to use Government and Industry resources than to approach these scenarios with a team

concept in mind. The team for the entire process should consist of a representative from Program Management, engineering, IA, and software development IPTs from each side. The IA IPT should be the primary organizer of the effort to ensure that all steps toward the CDS connection are identified, verified, and assist with the validation of the CDS solution.

STEP 1: C&A OF THE TRAINING SYSTEM

The C&A process for the system must be the first step in completing a CDS. The three reasons for this are security, validation, and approval. The ultimate goal of the C&A process is to achieve an ATO. The process that one can go though to achieve the ATO is the standard Defense Information Assurance Certification and Accreditation Process (DIACAP) found in DoD 8510.01. For more sensitive intelligence or compartmentalized systems, the Director of Central Intelligence (DCID) 6/3 or Joint Air Force Army Navy (JAFAN) 6/3 processes will be used to ensure the protection of Top Secret, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) systems.

The DIACAP contains five activities that will lead to the ATO. The activities include Initiation, Validation, C&A Decision, Maintenance, and Disposal.

The first reason of security is very self-evident in that DoD data, as per regulations and more importantly national security interests, must be protected. The Initiation Phase consists of describing the system to the point that all network connections are drawn, operating systems are identified, and planning to implement security as soon as practical in the program life cycle.

The most important activity is to agree upon IA requirements, known as IA Controls, which are located in DoDI 8500.2. The applicability and traceability are activities that the contractor must complete. The agreement of the applicability and the implementation plans for the IA Controls is imperative for the Government to ensure that the system meets the IA Controls and will operate securely.

DoDI 8500.2 also identifies the requirements for CDSs and how they are to be used. The control states that multiple levels of protection must be in place to protect the entire IT infrastructure. Additionally, the regulation endorses the use of approved products and procedures for protecting classified data.

Within the DCID and JAFAN, the IA control states that the system shall meet National Security Agency (NSA) and Defense Intelligence Agency (DIA) acceptance criteria for approval. The detailed information that is required to connect to a SCI or SAP system exceeds most training programs, however, for special operations or other missions a need or desire may exist. Figures 3, 4, and 5 are snapshots from DoDI 8500.2 and Figure 6 is a snapshot from DoD 8510.01.

MAC	Loss of Integrity	Loss of Availability	Protection Measures
MAC I	Unacceptable	Unacceptable	Stringent
MAC II	Unacceptable	Difficult	Additional Safeguards
MAC III	Tolerated	Tolerated	Protective; Commensurate with Best Practices

Figure 3. Mission Assurance Category (MAC) Levels

Classified	High level required for Systems Processing Classified Information
Sensitive	Medium level required for Systems Processing Sensitive Information
Public	Basic level required for Systems Processing Public Information

Figure 4. Confidentiality Levels (CLs)

MAC	CL	MAC IA Controls Actual		Confidentiality IA Controls	Required Baseline Score
		Integrity	Availability		
MAC I	Classified	32	38	45	115
MAC I	Sensitive	32	38	37	107
MAC I	Public	32	38	11	81
MAC II	Classified	32	38	45	115
MAC II	Sensitive	32	38	37	107
MAC II	Public	32	38	11	81
MAC III	Classified	27	37	45	109
MAC III	Sensitive	27	37	37	101
MAC III	Public	27	37	11	75

Figure 5. Required Baseline Scores

The second activity includes developing the system including creating a security baseline as early as possible in the development lifecycle. This will ensure that any system development or integration will be conducted on top of a secure system.

The third activity includes the decision to formally issue an ATO or to issue a Interim Authority to Operate (IATO). This activity involves formal Government C&A testing and can be accomplished

directly by the Certifying Authority (CA) or by an appointed agent. This testing will include DISA Gold Disk scanning, additional approved scanning activities, and test procedures completion culminating in a report to be delivered to the Designated Approving Authority (DAA) recommending approval or required fixes before fielding.

The fourth activity is maintaining the CDS throughout it's lifecycle by installing the latest patches and fixing any new security vulnerabilities . The fifth activity is the decommissioning of the system to include proper destruction. This paper and the process forward will only discuss and refer to the first 3 activities.

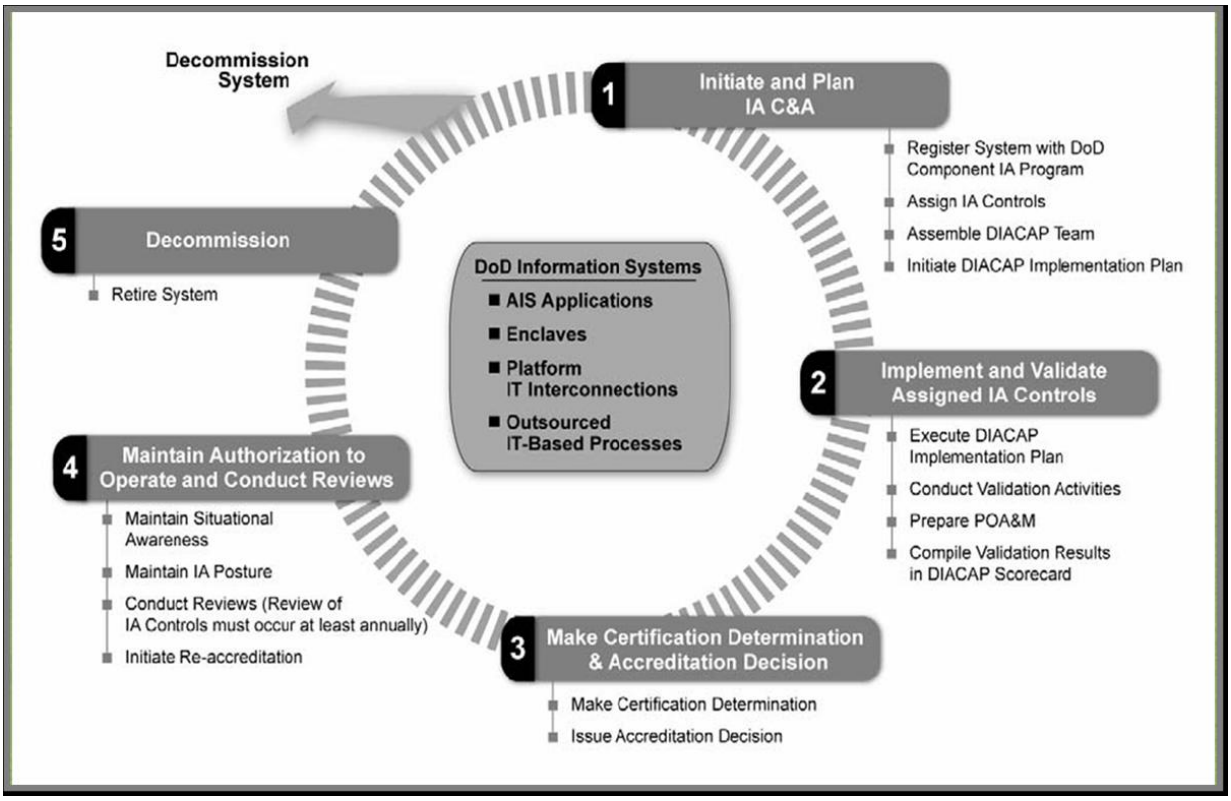

Figure 6. DIACAP Workflow

STEP 2: IDENTIFY THE APPROPRIATE MSL/CDS SOLUTION

Step 2 is the shortest connection step, but it is also one of the most important. The primary criteria used to select either a CDS or MSL solution is clearly stated in DISA and Department of National Intelligence (DNI) guidance, which requires users to choose a solution that ensures protection of the highest level of data and anti-contamination of the lower classified boundaries. This choice must be made from a list of approved and validated solutions provided by the National Information Assurance Partnership (NIAP) list. This list is developed by a partnership of the National Institute of Standards and Technology (NIST) and NSA laboratories.

One of the easiest components used to select the proper CDS is the NIAP Validated Products List (VPL) or the Common Criteria List (CCL) for approved CDS products. The products are divided into separate sub-categories that will support file transfer, multi-level operating systems, network separation, data at rest/process/transit, and training community video/audio.

Additionally, when choosing a solution, the operating systems and applications must be compatible and the security features enabled. Four operating systems to use in a CDS or MSL are Trusted Solaris™ 10, SE Linux®, and HP Net Top, and Green Hills with Integrity.

SE Linux is free with every licensed copy of Red Hat® Enterprise 5. This is a fact that is often not known by developers and integrators. From a Government programmatic point of view, it is cost beneficial to use SE Linux over Red Hat Linux due to no additional

cost. The major issue with SE Linux is that many custom scripts must be added to the basic security template. This requires a Linux expert to write, configure, and integrate scripts into a systems design and development.

Trusted Solaris 10 offers many pre-configurable and graphical user interface (GUI)-based security tools to lock down the system. An integrator will still need to write scripts, but not as intensive as SE Linux. This is due to the separation of Zones. Zones are areas that can be set up to manage classification of the systems and define all access to actions as simple as what a user can open or use.

HP Net Top is an integrated operating system that allows a user to distinguish different virtual machines based on classification. It uses data encryption to secure data in each virtual environment so that if a classified piece of information accidentally crossed boundaries, it would be encrypted and therefore useless. The security measures of locking down each virtual environment are configurable to the minutest detail.

Green Hills Integrity is a more embedded OS that allows for data to be handled at the processor level. The use of data separation at the machine level further enhances the level of protection.

A list of the approved products can be accessed easily online through the Common Criteria Validated Products List website, which is located at http://www.commoncriteriaportal.org/products.html. The NIAP VPL is located at http://www.niap-ccevs.org/cc-scheme/vpl/. However, the NIAP list will refer you to the Common Criteria portal. Since many different products located at each site, it is recommended that users thoroughly research options.

STEP 3: OBTAINING THE MEMORANDUM OF AGREEMENT FOR CONNECTIVITY

Once the system's DAA has decided that the system can operate at an acceptable level of risk, the socialization of connecting a Classified network to an Unclassified network can begin. To reiterate, it is highly unlikely that a unaccredited system, whether Classified or not, will be able to connect to another system without first obtaining an ATO. Additionally, it must be determined if the connection is going to an established training network, such as the Navy's Continuous Training Environment (NCTE), or if it will connect to a new training network. The level of classification, the need-to-know, and the different users/operators of the system are extremely important in completing this step. This information is necessary because the approving authority on the other side will ask these questions. So the more that this information is readily available the easier the process will be.

Connecting to a federated or existing network is the easier of the options. This is primarily due to the possibility that a process for connecting Unclassified/Classified networks already exists. An additional risk-lowering possibility is that an approved CDS is already in use and there is plenty of experience on how to configure it.

The probability is that not every network will have a defined process for CDS connectivity. The goal for the IA team should not only be to get its system securely connected, but to be the example and template for the command or at least the similar training community. The process of documenting lessons learned is critical to prevent re-work and wasted dollars.

STEP 4: VALIDATING AND TESTING THE SOLUTION

The NSA and DoD have created the lead for CDS management by creating the Unified Cross Domain Management Office (UCDMO).

DISA has created the Cross Domain Enterprise Services, which assists with "full service cross domain technology (i.e. guards), procurement, development, testing, certification/accreditation, installation, maintenance, life-cycle Sustainment, and help desk support." In other words, it tries to be the one-stop shop for CDS solutions.

The process of validating and testing is often lumped into one activity, but from a Government/industry standpoint, it must be realized that two separate activities are taking place. The importance for conducting a self-assessment test has two major benefits: the development team will know if any issues exist prior to formal testing and, hopefully, will be able to mitigate those risks; and a solid security baseline and test plan will always add credibility to the formal validation.

The first step of the first activity is validating the security requirements and that task will fall with the project's IA team. The team needs to have three items ready for their internal testing: a solid baseline to test, a plan of attack for the testing, and a fully vetted test plan. The system may be simple enough to allow using a scanning tool and running through the STIG is

sufficient enough or it may be more complex and require specialized test procedures to satisfy the IA Controls.

The solid baseline in which the internal testing is conducted is a standard engineering practice. The plan forward must be to secure the systems as soon as they are in place. A standard DoD scan must be accomplished and the latest patches installed. Once it is determined that the baseline will pass Government inspection, a lock down of the system must occur.

The CDS/MSL component must also be configured exactly how it is to be used. The system should have all ports and protocols closed, except for the ones needed for operation. This information should be documented, therefore adding to the ease of connection/acceptance.

The plan of attack from a developmental stand point is to align the schedule for formal Government testing with enough leeway before the training event or connection is required. This will alleviate any stress to meeting the desired date of use. The old adage of proper planning and emergencies is as critical with a CDS/MSL approval as any other formal Government testing.

The second step of the first activity is to create a test plan to include specialized testing procedures. These procedures should list all steps that a tester will need to ensure that all CDS/MSL requirements are being met for the specific system that is being built.

The second activity is allowing for one of the UCDMO/NSA approved labs to verify that the system is secure. This once again goes back to the very beginning in stating that this should be an easy step for the team. If the program team locked down the system to meet all applicable IA requirements and internal testing demonstrated that the system is secure, the NSA should have minimal issues approving the solution. The bottom line is that IA must be "baked in" to the solution in order to avoid costly schedule and design changes.

This process is the longest part of the schedule because these labs are thorough enough to ensure that the system truly can be operated while protecting Classified data and negate the risk of contaminating a Unclassified network. Additionally, the sheer volume of other solutions that are being tested increases the wait time. It has been suggested that the more light that can be shined on this issue of too much work and not enough people will increase the labs' workforce, therefore decreasing the wait time.

For any questions regarding specific service-oriented IA or CDS/MSL solutions a applicable point of contact (POC) should be contacted.

STEP 5: OPERATING THE SYSTEM SECURELY THROUGHOUT ITS LIFECYCLE

One aspect often overlooked for a CDS, MSL, or achieving a C&A is what to do with the system after it's fielded. Often due to budget constraints, low amounts of IA training, or sheer complacency can cause a breach in classification. Several activities that must be planned to protect Classified data are prevention, detection, reporting, and future defense.

The CDS/MSL must have the Information Assurance Vulnerability Alerts (IAVAs) installed as soon as they are released. These are patches that are released by the operating system or application manufacture that will fix security vulnerabilities. The sooner the patches are installed, the greater protection that the high side requires will be met.

Also the DIACAP and DCID require annual reviews. One lesson learned is that of a flight training system did not follow this requirement. They had a scheduled annual review and tried to install 36 IAVAs the day before the annual review. Since they did not have proper patch management, once they installed all 36, the system ended up breaking. So not only did they not meet the requirement, but they disabled a necessary training system.

EXAMPLES OF IA/CDS SCHEDULES

Depending on the MAC Level, Classification, Criticality, and size of a trainer the C&A effort can be accomplished within a 9 to 12 months. During this time, the process goes from start to finish and achieves and ATO.

The CDS portion of the connection can take any from 6 to 10 months depending on the complexity of the connection, system, and accreditation agency. The workforce that most approving authorities have is sparse at best, so if the DoD desires to have a true train as we fight capability, there needs to be more flexibility and availability to approving resources. Industry, on the other hand, needs to choose CDS/MSL solutions that are already approved and then configure those solutions to meet their IA requirements.

The process from start to finish is illustrated in Figure 7. It illustrates the recommend IA strategy for a 12-month program. The IA work is usually completed within 10 months with additional support for the IAVA management. The CDS/MSL solution should begin directly after this C&A process.

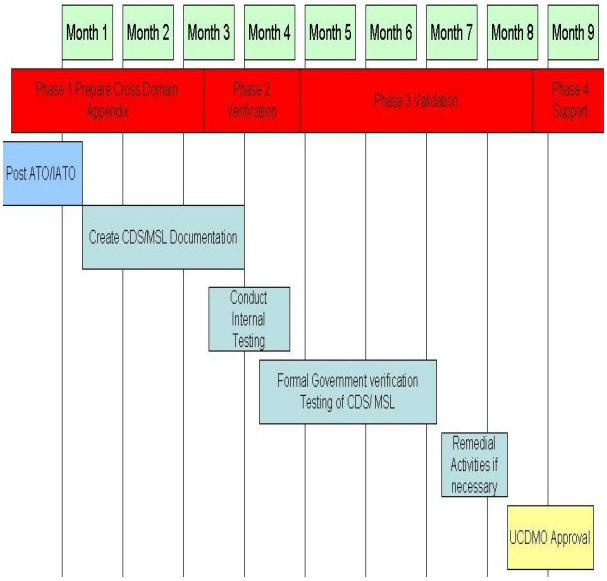

Figure 7. Typical CDS Approval Schedule

GOVERNEMENT ROLES AND RESPONSIBILITIES

In 2006, the DoD and NSA created the UCDMO, whose mission is to manage all approved CDS/MSL options. The main goal of this organization is to educate services and organizations about the usage of proven CDS/MSL solutions. The UCDMO's baseline list of approved CDS devices can be found at https://www.intelink.gov/mypage/ucdmo.

All CDS connection involving the secret internet protocol router network (SIPRNet) activity needs to follow the DISA certification process. The DISA IA32 group is the organization that allows for verification and validation testing and serves as the primary interface to the customer. The final approval authority is the DISA Chief Information Officer (CIO). The system must meet all IA requirements and pass the rigorous CDS/MSL testing process to be qualified as a true solution.

Director of National Intelligence (DNI) and its partner in the intelligence community are the ultimate testing authority and recommended approving authority for all CDS/MSL solutions. They have made a distinct business in ensuring their clients' Classified networks are compliant and secure. Furthermore, DNI is the leading force along with NSA, DIA, and DoD in ensuring that all information systems have an ATO and an approved CDS/MSL connection.

Each service has its own CDS approval process as well. The process leverages higher DoD, NSA, or DISA CDS/MSL certification process. The service process may not be as clear as the DoD and agency level in that massive changes exist within the Air Force in restructuring its communications field to a Cyber Warfare Command. The Navy and USMC are re-defining their IA C&A processes as well. A move is at foot to consolidate the IA C&A process to include every activity into one process.

LESSONS LEARNED: A VISIT TO CDS/MSL SOLUTIONS OF THE PAST

The largest complaint for training systems starting out is that approving authorities for a CDS/MSL solutions do not have the bandwidth to approve systems as quickly as the Warfighter needs these to be in place. The number one lesson learned from having been through this process, is the more that your system meets the IA Controls, the greater probability of acceptance and approval. So a "baked in" strategy is essential for success. If IA is not in the system development, from a general C&A acceptance or a CDS/MSL point of view, the less likely the system's schedule and cost will be met.

The second lesson learned is that the earlier the CDS/MSL solution is presented to the DAA, UCDMO, or specific service CDS/MSL approval authority, the better. The various agencies are very efficient, but with the sheer volume of requests, the earlier the communication and interaction within the program schedule the greater chance for success.

The third lesson learned is not to wait until the last minute to start applying for the CDS/MSL approval process, let alone begin the process.

Finally do not reinvent the wheel or make a new CDS/MSL in your system development. Chances are that an already proven solution exists that your system can use. These software and hardware products and solutions can be found on the NIAP/CCL website http://www.commoncriteriaportal.org.

ADDITIONAL CONSIDERATIONS

The team concept must also take into consideration that certified IA professionals are members of the team. DoD 8570.1 mandates that personnel working on DoD systems are certified through ISC2 with the Certified Information System Security Professional (CISSP®) or CompTIA™'s Security + certifications. The Defense Federal Acquisition Regulation Supplement (DFARS) has been updated and the certification requirement must be in all new contracts (DFARS clause E8-193).

An additional consideration would be to have at least biweekly IPTs to discuss potential findings, new threats, and current status.

A final consideration should be the use of experienced IA personnel. A CDS solution is more intense for understanding the process than a standard IA C&A. The planning, design, and development will require several IA savvy personnel who have done multiple DIACAP C&A efforts and, as a greater benefit, a CDS C&A effort.

NEEDED AND RECOMMENDED IMPROVEMENTS TO THE PROCESS

The main improvement to the entire CDS process is greater communication, access, and advertisement to the UCDMO CDS process, and experience with going through the process. For reference and to stay abreast of all the latest CDS/MSL solutions/information visit https://www.intelink.gov and register to receive notifications of the latest threats and solutions. The information should not be a detailed advertisement of the technology, but instead it should include the beneficial capability. Experience is the most lacking of the three improvements as not many contractors or even DoD organizations have been through this process on multiple occasions, or even at all.

From a Government standpoint, the contractor has had difficulty in the past of understanding the requirement, so integrating the developer and Government entities into an IPT is key to building the solution needed. The Government also needs to adhere to DoD 8570 certifications and ensure that the IA/CDS/MSL staffs are properly trained in IA. The IA IPT should work with the contractor using a team mentality to accomplish the goal of an ATO/ATC.

Industry must deliver secure systems, but also must meet the contract deliverables specified in the statement of work. In other words, the acquisition process must clearly identify IA and CDS/MSL requirements so that the contractor can effectively build/integrate the required solution. If the prime contractor does not have this IA/CDS/MSL experience, internal/external training should be used to educate the staff thus leading to securing the system. If not, the prime should look to augment its staff with a firm that specializes in IA and CDS/MSL to lower the risk to schedule and cost.

For generations of training exercises, a brick wall has existed between the lower classified trainers and the higher classified trainers. These 5"easy" steps will give our Warfighters the tools that they need to operate securely in Joint and NATO/Alliance environments. The path this paper describes is the basis of the easiest way forward. The details described the who, the when, and the, why, which should also allow users of a CDS/MSL to feel comfortable when choosing this as their training solution.

In the future, the need to connect Classified and Unclassified systems will become more a of a necessity than a nice to have. In order to properly train the Warfighter, an IA and CDS/MSL plan to success is critical to deploy a secure system. The key is to start with the IA protections, develop the CDS/MSL around the protections, test, connect, and operate securely throughout its lifecycle. If these five steps are followed, the system will be secure, the cost of the effort will be lower, and the Warfighter is guaranteed to win.

REFERENCES

Department of the Army, Army Regulation 25-2. (2007). *Information Assurance*.

Department of Defense, 8510.01 (2008). *DIACAP Application Manual*.

Department of Defense Directive, 8500.1. (2002). *Information Assurance*.

Department of Defense Instruction, 8500.2. (2003). *Information Assurance Implementation*.

Department of the Navy, 5239. (2005). *Information Assurance Program*.

An Introduction to the DOD Cross Domain Enterprise Service (2008) DISA CDS CPK Cross Domain Solutions Branch IA 32

UCDMO (2008) Cross Domain Inventory and Portal https://www.intelink.gov

Common Criteria and NIAP web portals http://www.commoncriteriaportal.org/products.html.

Heller, S., SPAWAR (2005) FORCENET: Cross Domain Solutions Communication and Networking Session