White Paper

JOINT WARFIGHTING CAPABILITY: A FRESH LOOK AT MULTI-LEVEL SECURITY (MLS)

David Robinson
Systems Engineering and Operations Manager,
MacAulay-Brown, Inc.

Christopher Jacobson, PhD
Chief Technologist, IBM

Edward Ballanco
President, EMB Information Technology, Inc.

May 13, 2013

Introduction

The success of the warfighter is increasingly dependent on information that cuts across multiple security domains. The lack of a comprehensive and integrated solution is impacting mission success, which is why military leaders are looking for a new capability. The current architecture available through the Unified Cross Domain Office (UCDMO) baseline, provides a piece-meal approach for operations across multiple security levels. This paper canvasses warfighter needs, addresses technological advances and discusses the process to achieve Multi-level Security (MLS) necessary to enable our national security strategy for the next 20 years.

Background

The US Armed Forces have become increasingly dependent upon coalitions and alliances to achieve national objectives. As we saw in Operations Desert Storm, Iraqi Freedom and Allied Force, we have become ever more reliant on the formation and maintenance of multinational forces to deliver decisive combat power. We have also experienced an increase in the number of military operations, other than war, where multinational military forces, interagency task forces, international relief agencies and other civilian organizations have combined forces to achieve their objectives. Decreasing budgets and global political pressures ensure that this trend toward mutual dependence will continue for the foreseeable future. This move toward collective action is recognized by the CJCS Joint Vision 2020 document which states: "The joint force of 2020 must be prepared to win across the full range of military operations in any part of the world, to operate with multinational forces, and to coordinate military operations, as necessary, with government agencies and international organizations."[1] This increased reliance on amalgamated forces presents significant challenges in the command and control and information security arenas. These challenges may be ameliorated by the application of a comprehensive MLS.

While MLS is imperative, it remains a much maligned topic. Its goal is to provide segmentation of data, applications and individuals based on security classifications. At the same time, it works to aid collaboration and sharing across these security networks. In the 1980's, MLS began with the Orange book for Security and B1 (described more thoroughly in later sections) which was considered an acceptable level for an MLS solution. Multi-level mode accreditation at B1 was achieved in 1991 on IBM mainframes with IBM COTS operating system and related utilities (e.g. Multiple Virtual Storage (MVS), Resource Access Control Facility (RACF)).[2] As with all levels of system solutions, it's about the end-to-end workflow that is critical to manage the security of a mission capability. As depicted in Figure 1, three major areas for consideration are the presentation, application and data layers associated with the mission capability.

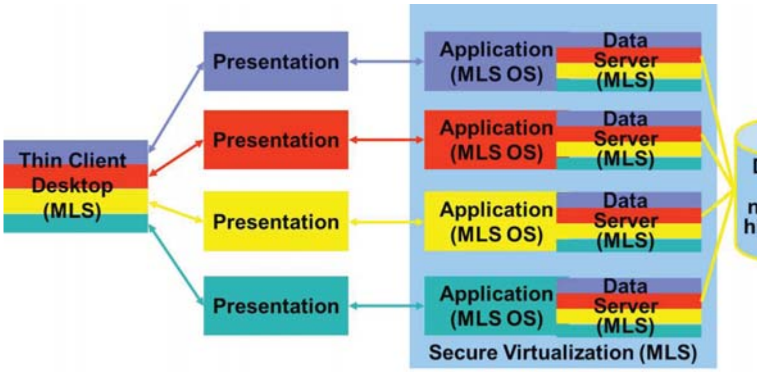

Figure 1. *Three Tier MLS Depicting Presentation, Application and Data Layers.*

Components contributing to MLS at the presentation layer (e.g. end user interface) include the Raytheon Trusted Computer Solution's and Trusted Thin Client. Components contributing to MLS at the data layer include Oracle, DB2 and Unix file systems that have been modified to operate using MLS technology, along with their associated operating systems. While mission capability can be supported using MLS components, work continues on certified middleware support at the application layer for a fully implemented MLS solution. There are production systems leveraging MLS technology. GE Aerospace modified IBM's MVS operating system in the late 80s to provide a GOTS MLS implementation that would allow sharing across the Defense Mapping Agency (now the National Geospatial Agency) and its mission partners. In 1997, IBM began working with Lockheed Martin, the successor of GE Aerospace, to take the system modifications and add them to what are now the z/OS operating system and the DB2 for z/OS database system as a COTS solution. This system and database have been evaluated with the Common Criteria Labeled Security Protection Profile at the Evaluation Assurance Level (EAL) 4+ level, beginning with z/OS R5 and DB2 V8. RACF, beginning with z/OS 1.12, has achieved Common Criteria certification at EAL5 under the Common Criteria Evaluation and Certification Scheme. In addition, the hardware partition manager, PR/SM has been evaluated at EAL5+ and the system hypervisor, z/VM and Linux for System z have been evaluated with Labeled Security Protection Profile (LSPP) at EAL4+. Finally, WebSphere Application Server (WAS) middleware solution for z has been evaluated at EAL 4+ for the Controlled Access Protection Profile (CAPP). In February 2008, this system was put into production. In September 2009, Lockheed Martin issued a press release stating the value of their MLS solution.[3] In addition to government usage, commercial customers, such as Univar, have leveraged IBM MLS technology to share data with its supply vendors. Building on this MLS technology base, a Proof-of-Concept (PoC) and project is being planned at the Langley AFB Operational Support Facility (OSF) to continue advancing an MLS solution for key Department of Defense (DoD) stakeholders and their critical use cases. Authors of this paper, working together across MacAulay-Brown, Inc. (MacB), IBM, EMBIT and Jeskell, are committed to pursuing the MLS imperative of CJCS Joint Vision 2020.

Stake Holders

When we talk about stakeholders for developing and fielding a robust MLS capability, we start at the Secretary of Defense and work our way down through the DoD echelons to the soldier "rucking" his hand-held, end-user device through the mountains of Afghanistan. Our Nation's computer networks are under constant cyber attack; our defense budgets are being cut; and our IT enterprise now includes more than 15,000 classified and unclassified networks that must be protected and maintained.[4] In response to these emerging issues, the Deputy Secretary of Defense published the IT Enterprise Strategy and Roadmap in late 2011. One of the roadmap's long-term goals is to enable the warfighter to access information at any time, from any place and on any computer. The roadmap specifically names MLS as one of the 26 key IT *Consolidation Initiatives*.[5] The document also features goals for increased effectiveness across joint and coalition lines and reduced network resources.[6] The overarching goal of the strategy is: "Providing our warfighters with the assured access to information and services that are required to defend our country in the 21st Century."[7] The roadmap's discussion of the MLS initiative states: "Deploying an enterprise identity, authentication, authorization and access management service will extend security protection from the network to the data on the network providing security controls to better enable secure information sharing."[8] Consistent with the architecture presented in Figure 1, the roadmap also provides a notional MLS workstation that incorporates the consolidation of networks and credentials-based MLS.

During the first Gulf War, almost 800,000 troops, 2,800 fixed wing aircraft and 225 naval vessels from 38 nations participated in combat or support operations.[9] Although this diverse coalition ultimately proved to be very effective in achieving its objectives, the campaign was rife with problems related to chain of command and information sharing. Political and cultural issues aside, the timely availability of relevant intelligence information was a significant obstacle to effective and efficient operations. Although the Gulf War coalition was probably one of the most successful in history, the bifurcation of command structures (Arab and Western nations) created significant challenges for information sharing that might have been easily overcome by a credentials-based MLS system.

During Operation Allied Force, the mission to stop Serbian aggression in Kosovo, NATO experienced similar challenges. Although the NATO alliance had existed for more than 50 years when Allied Force began, there were still significant problems with information sharing. "In some instances, the United States withheld information about missions involving the use of F-117s, B-2s and cruise missiles, to ensure strict U.S. control over those U.S.-only assets and to maintain a firewall against leaks from any allies who might compromise those operations."[10] Suffice to say, this created problems when U.S. aircraft showed up on NATO radars without prior notice. "Even when the U.S. opted to share information, the process was complicated and cumbersome, hampering the alliance's ability to act effectively. In addition to being unwieldy and slow, the alliance suffered from other troubles as well. According to Supreme Allied Commander Europe (SACEUR) GEN Wesley Clark, who led NATO's campaign, leaks were a constant source of trouble. As early as October 1998, one of the French officers working at NATO headquarters had leaked key portions of the operational plan for the campaign to the Serbians."[11] Apparently, the information sharing problems hampered assessment efforts to the point where "some 80 percent of the targets hit in the first month of the campaign had been hit at some point before."[12] Even though NATO was a well-established alliance with standardized procedures and command relationships, an MLS system would have eased information sharing and enabled greater efficiencies in planning, operations and assessments.

U.S. Forces Korea (USFK) faces some unique challenges with regard to information security. In addition to maintaining our on-going alliance with the Republic of Korea, the Commanding General of USFK serves as the commander for United Nations Command. One might call the command structure a hybrid between an “alliance” (US-ROK) and a “coalition” (UN forces). As the situation exists today, warfighters in South Korea must share information on several different domains, (e.g. U.S.-only, ROK-only and combined) at varying levels of classification. The challenge of sharing information across domains and classification levels is further compounded when UN forces join the fight. Furthermore, the existing command structure is in a state of flux as the U.S. and ROK negotiate the dissolution of the Combined Forces Command so that South Korea may regain control of its own forces in wartime. The uncertainty and complexity of the Korean War situation create obstacles to information sharing that may be mitigated through the employment of a robust MLS capability. The Chairman of the Joint Chiefs of Staff further emphasizes the need for multi-national and interagency sharing of information stating, “The global reach of the United States, and its position of prominence in global affairs, dictate that the DoD does not operate in a vacuum. As a result, success is ensured by operating in conjunction with domestic agencies and federal departments, armed forces and governments of foreign countries and international non-governmental agencies. Regardless of the spectrum in which the DoD is operating, from disaster relief to full kinetic warfare, the information environment must support collaboration and information sharing to be effective.”[13]

Use Case

Members of the 480th Intelligence Surveillance and Reconnaissance (ISR) Wing are working to improve information sharing, “enabling them to send and receive data to coalition partners in an easily discoverable and retrievable way.”[14] The 480th ISR Wing Commander explains that improved capability “provides our coalition forces real-time access to our collection decks, status of our tracking and high-quality digital imagery, along with contextual reports that correlate to mission and platform.”[15]

Building on these successes, as shared responsibility for processing, exploitation and dissemination (PED) increases, the need to close capability gaps becomes more critical. A collaboration of retired Air Force officers, who worked the critical seam between ISR and operations, identified gaps impacting the Distributed Common Ground System (DCGS) and the Air and Space Operations Center (AOC) as providing the basis for a key use case to drive valuable mission improvement. These officers, authors of this paper, formulated a strategy to leverage resources across industry in partnership with elements of DoD experimentation and doctrine. This paper describes mission context and technology that demonstrates an MLS capability compliant with DoD certification requirements and in conformance with DoD standards for coalition information exchange. The focus on a coalition sharing use case also permits a companion PoC that operates on a network domain below the classified level. As depicted in Figure 2, the ISR coalition sharing use case focuses on improved PED action for shared Full-motion Video (FMV), in support of coalition operations. The use case complements a time-sensitive targeting (TST) interoperability experiment also ongoing at the Combined Air and Space Operations Center Experimental (CAOC-X) at Langley AFB.

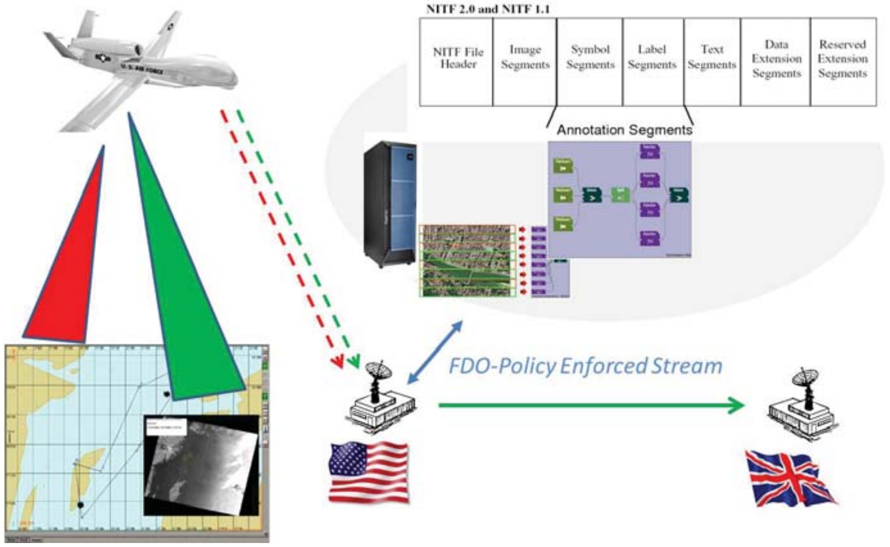

Figure 2. *FMV Sharing in Support of Coalition Operations*

As part of the use case, disclosure policy managed by the Foreign Disclosure Officer (FDO) is enforced for multinational information exchange, using the same MLS components certified for use today at the National Geospatial Agency (NGA). Using a policy tool, such as the NGA FDO policy web-tool, the PoC calculates Field-of-View (FOV) for 10 second FMV segments based on platform metadata associated with Area of Responsibility (AOR) constraints. Calculations are accomplished using IBM real-time analytics (InfoSphere Streams) and NITF 2.0 annotation segments are updated with FDO policy tags. As depicted in Figure 3, MLS data segmentation and multi-nation sharing is supported with an integrated COTS components solution, in production since February 2008.

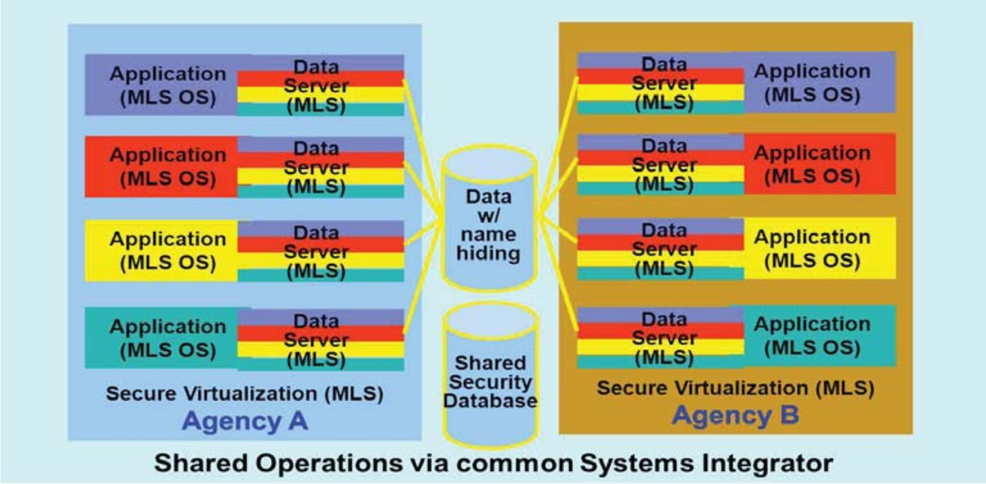

Figure 3. *Multi-agency Production MLS Solution*

Today, Cross Domain Solution (CDS) capabilities, underlying this and related joint warfighting use cases, are formally supported by solutions, as documented on the UCDMO baseline. As an example, the AFCENT AOC utilizes a Raytheon Trusted Computing Solution and Trusted Thin-Client multi-level access (MLA) solution for supporting information access to segregated security domains. Additional advances for CDS within the AOC baseline include plans for a multi-tenant solution that operates within the same domain of the geographic Combatant Command (COCOM). Building on the strengths of IBM's work since the 1980's, including NORAD and NGA, the work at Air Combat Command's Operational Support Facility (OSF) within the Operational Support Center (OSC), will bring together UCDMO baseline processes with IBM advances in technology and common criteria certification/compliance.

MLS Technical Overview

As mentioned earlier, in the 1980s, the DoD provided guidelines and requirements for establishing data processing security in its computer systems.[16] The criteria corresponded to a particular security designation, depending on the type and amount of security provided by the system. The NSA performed a formal evaluation to determine whether a data processing system adhered to the guidelines and requirements for a given security designation. Between 1988 and 1990 IBM enhanced such key subsystems as MVS, RACF, Job Entry Subsystem (JES)2, JES3, Time Sharing Option (TSO), Virtual Telecommunications Access Method (VTAM®), Decimal Floating Point (DFP) and Print Services Facility (PSF) to meet the B1 criteria, which was considered an acceptable level for an MLS solution. The NSA performed a formal evaluation on IBM's MVS/ESA™ and a B1 security designation was achieved. Eventually, the Common Criteria and ISO 15408 superseded the older U.S. Government standards described in the Orange Book. IBM's MLS functions for z/OS build on the work done on MVS to meet the B1 criteria, and provide functions consistent with those described in the Common Criteria and some of the Common Criteria Protection Profiles.

What is MLS?

MLS is a security policy that allows the classification of data and users, based on a system of hierarchical security levels, combined with a system of non-hierarchical security categories. An MLS security policy has two primary goals. First, the controls must prevent unauthorized individuals from accessing information at a higher classification than their authorization. Second, the controls must prevent individuals from declassifying information. A fundamental requirement of a secure system is that there is a set of guidelines that specify the authorization of subjects to access specific objects. "Access" is a key concept. It implies a flow of information from a subject to an object or from an object to a subject. For example, when a user (a subject) updates a data set (an object), the information flows from the subject to the object. When a user reads a record from a data set, the information flows from the object to the subject. The subject in these interactions is active; the subject is attempting to access an object (or the information that the object contains). The object, on the other hand, is passive; it contains the information that the subject wants to access, or it is the receiver of information from the subject. Each time a subject attempts to access an object the system must decide whether to allow the access. Two central concepts of security are security policy and accountability. A security policy is a set of laws, rules and practices that regulate how an organization manages, protects and distributes its sensitive data. It is the set of rules that the system uses to decide whether a particular subject can access a particular object. Accountability requires that each security-relevant event must be able to be associated with a subject. Accountability ensures that every action can be traced to the user who caused the action.

Characteristics

Characteristics of an MLS system include the following:

- The system controls access to resources.
- The system does not allow a storage object to be reused until it is purged of residual data.
- The system enforces accountability by requiring each user to be identified and creates audit records that associate security-relevant events with the users who cause them.
- The system labels all hardcopy with security information.
- The system optionally hides the names of data sets, files and directories from users who do not have access to those data objects.
- The system does not allow a user to declassify data by ‘writing down’ (that is, write data to a lower classification than the classification at which it was read) except with explicit authorization.

Security Labels

A security label enables a system to classify subjects and objects according to a data classification policy, identify objects to be audited based on their classification and protect objects from unauthorized subject access. Objects in an MLS system have a security label that indicates the sensitivity of the object’s data. Subjects in an MLS system also have a security label. This label determines whether the subject is allowed to access a particular object. A security label is used as the basis for Mandatory Access Control (MAC) decisions. Security administrators assign security labels to ensure that data of a certain classification is protected from access by a user of a lesser security classification. In addition, through the use of Discretionary Access Control (DAC), the security administrator can further control data access based on a need-to-know requirement, such that users with approved classification levels can be restricted from data access based on need-to-know. Security labels provide the capability to maintain multiple levels of security within a system. By assigning a security label to a resource, the security administrator can prevent the movement of data from one level of security to another. Security labels can also identify the security of hardcopy output. The security label is associated with the security notation that is printed on the hardcopy output from the system. Security labels for users, MVS data sets and general resources are stored in the RACF database, in the profiles for the users and resources to which they apply. Security labels for files and directories are stored in the file security packets (FSPs) for the files and directories to which they apply as part of the zFS file system.

MLS Implementation on System z: As implemented on the System z, MLS has two components. The first consists of the database holding the data while the second component consists of the application systems accessing that data base.

Database Component: The first component uses DB2 for z/OS, which in combination with the IBM RACF stores records (rows) with different security classification levels in the same physical database.

However, DB2 and RACF ensure that users can only read, add, update or delete those records (rows) for which he or she has the appropriate security level, roles and insert/update/delete authorization level. For example DB2 would allow users with a Secret security level to access Secret and Unclassified records appropriate for their security level and roles, but would allow users with a Top Secret security level to access Top Secret, Secret and Unclassified records. And a given user might, for example, be allowed to read and update, but not add new records or delete any within that security level.

Application Component: The second component consists of the application subsystems, e.g. Customer Information Control System (CICS) or WebSphere Application Server (WAS) that access the data in DB2. The applications in each security level would run in their own separate Logical Partition (LPAR). System z LPARs have been granted Evaluation Security Level 5 (EAL5), which means that the programs and data in each LPAR is considered as secure and separate as if they were running in different physical machines. In addition, the application subsystems (e.g. CICS or WAS) in each LPAR would only allow users with the correct security level to run in that LPAR.

MLS vs. MSL: Since each security level would run in its own separate LPAR, the buffers in each security level would only hold records for that security level and all lower security levels. As a result you would have the same isolation of security levels within the application buffers as we have in the DB2 database, ensuring a very high level of MLS. IBM's MLS solution offers major advantages over MSL. For example, all application security levels are accessing the same physical MLS database, greatly simplifying database maintenance. Additionally, the LPARs are all running in the same physical box (System z), which provides greatly simplified operational procedures and lower total cost, while still ensuring that users can only read, update, delete and add those records for which they have the appropriate security level, role and authorization.

Approach to Deliver MLS Capability for the DoD

MacB and IBM have created and submitted Certification and Accreditation (C&A) packages through the DoD Information Assurance Certification and Accreditation Process (DIACAP). As an example, for the Air and Space Operations Center Weapon System (AOC WS), MacB completed all DIACAP processes to achieve an Air Tasking Order (ATO) for the AOC WS on the Secret Internet Protocol Router Network (SIPRNET) enclave. MacB maintained the accreditation package throughout the lifecycle obtaining additional three year ATOs prior to the expiration of the current ATO. After obtaining the initial ATO, MacB successfully added multiple entities of the AOC WS to the enclave. The experience MacB has gained through multiple years of operating, maintaining and supporting an enclave; and associated AOC WS Automated Information System (AIS), can be employed to achieve an MLS capability with IBM MLS technology. An MLS program would include identifying all Identification and Authentication (IA) documentation necessary to address the IA controls in the Enclave and Computing Environment, Security Design and Configuration, Physical and Environmental Continuity, Enclave Boundary Defense, IA, Personnel and Vulnerability and Incident Management.

At the heart of delivering an MLS solution lie process hurdles cutting across numerous agencies and boards. NSA, DISA and other agencies are members of the Cross Domain Solution Element (CDSE). The CDSE facilitates and provides governance over the cross domain solution connection process in accordance with DoD and National Industrial Security Program (NISP) policy requirements, as depicted in Figure 4.

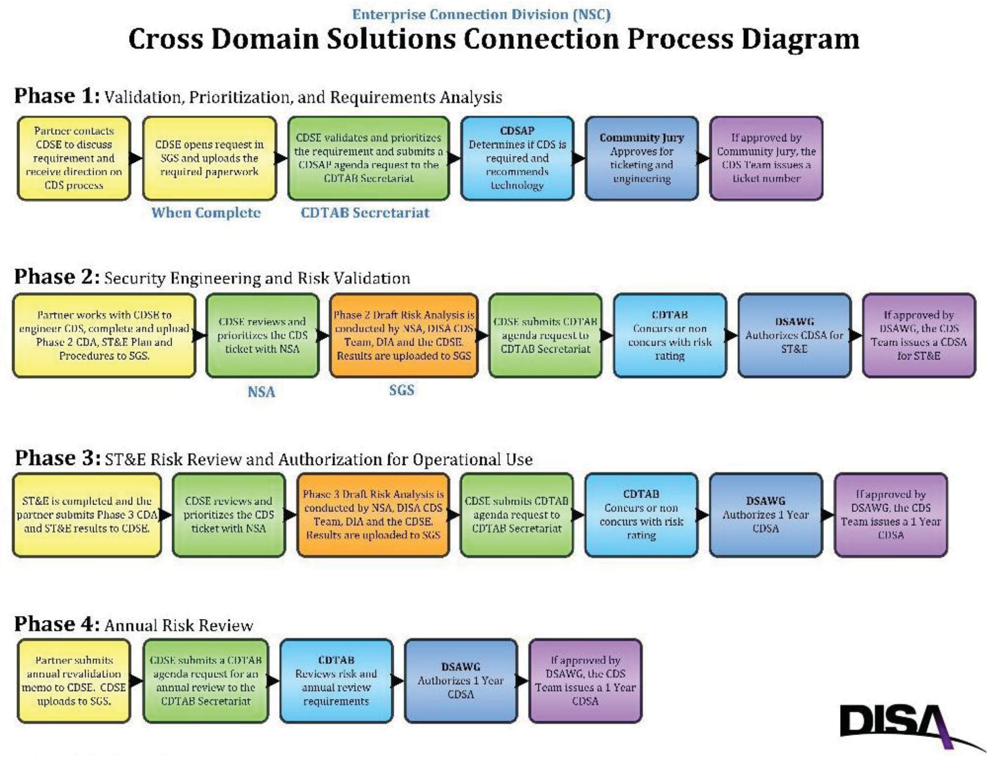
Enterprise Connection Division (NSC)
Cross Domain Solutions Connection Process Diagram
Phase 1: Validation, Prioritization, and Requirements Analysis
Partner contacts CDSE to discuss requirement and receive direction on CDS process
CDSE opens request in SGS and uploads the required paperwork
When Complete
CDSE validates and prioritizes the requirement and submits a CDSAP agenda request to the CDTAB Secretariat
CDTAB Secretariat
CDSAP Determines if CDS is required and recommends technology
Community Jury Approves for ticketing and engineering
If approved by Community Jury, the CDS Team issues a ticket number
Phase 2: Security Engineering and Risk Validation
Partner works with CDSE to engineer CDS, complete and upload Phase 2 CDA, ST&E Plan and Procedures to SGS.
CDSE reviews and prioritizes the CDS ticket with NSA
NSA
Phase 2 Draft Risk Analysis is conducted by NSA, DISA CDS Team, DIA and the CDSE. Results are uploaded to SGS
SGS
CDSE submits CDTAB agenda request to CDTAB Secretariat
CDTAB Concurs or non concurs with risk rating
DSAWG Authorizes CDSA for ST&E
If approved by DSAWG, the CDS Team issues a CDSA for ST&E
Phase 3: ST&E Risk Review and Authorization for Operational Use
ST&E is completed and the partner submits Phase 3 CDA and ST&E results to CDSE.
CDSE reviews and prioritizes the CDS ticket with NSA
Phase 3 Draft Risk Analysis is conducted by NSA, DISA CDS Team, DIA and the CDSE. Results are uploaded to SGS
CDSE submits CDTAB agenda request to CDTAB Secretariat
CDTAB Concurs or non concurs with risk rating
DSAWG Authorizes 1 Year CDSA
If approved by DSAWG, the CDS Team issues a 1 Year CDSA
Phase 4: Annual Risk Review
Partner submits annual revalidation memo to CDSE. CDSE uploads to SGS.
CDSE submits a CDTAB agenda request for an annual review to the CDTAB Secretariat
CDTAB Reviews risk and annual review requirements
DSAWG Authorizes 1 Year CDSA
If approved by DSAWG, the CDS Team issues a 1 Year CDSA
DISA

Figure 4. *DoD Process for MLS Approval (http://www.disa.mil)*

A key challenge in completing the process is the amount of time the different evaluation, certification and accreditation tasks require; the limited number of solutions currently available from the Evaluated Product List to build IA systems and the different organizations responsible for the various functions. The business case for commercial products to undergo the stringent testing required for inclusion on the Evaluated Product List, both from a financial and technical standpoint, is understandably daunting.

A key imperative to achieve Joint Vision 2020's MLS goal is for the Government to take ownership, in both time and resources, to perform the technical development and formal technical evaluation. The Government needs to sponsor the programs, advocate the solutions and streamline the politics and policy that drive the complexity and cost to viable CDS/MLS solutions. A big factor relates to the 4-6 months, or longer, required to get a solution through the DSAWG; in addition to the 2-3 years to get through the CDMO and UCDMO, depending on the complexity. Another challenge in the approval process timeline is the changing knowledge requirements placed on the evaluators who support testing. The evaluation criteria, standards and controls mandated to successfully undergo Security and Test evaluations, today are not clear. The process is complex, time-consuming and expensive. It is recognized that by the time the process is successfully completed, the solution that entered the process is two years old. This, in turn, contributes to capabilities and solutions that are approaching "end-of-life" when rolled out. It is understood the UCDMO, CDMO, DAA will require test and updates annually to first receive an ATO/ATC, as well as recertify the solution to continue with the ATO/ATC beyond one year. Based on this process, MLS initiatives will be subject to perpetual testing as necessary software upgrades occur.

Given the challenges mandated by the CDS connection process, IBM has repeatedly demonstrated the commitment of resources and dedication of talent necessary to develop and deploy MLS solutions for the Government. As previously mentioned, an IBM MLS solution has been in production since 2008 supporting multi-agency use on an NGA delivered system. Additionally, IBM is supporting Air Force Space Command 24th Air Force and the North American Aerospace Defense Command (NORAD) with an MLS solution to share information releasable to Canada (RELCAN). The continuing challenge is to keep those systems up-to-date with appropriate STIGs and controls, while creating a partnership with the Government to modernize and improve on current MLS capability for the Nation.

As an IBM partner, EMB Information Technologies is working closely with Jeskell in establishing a technical laboratory to further develop MLS use cases. This will provide a development environment to apply the IBM technology along with MacB in proving MLS capabilities.

To achieve Joint Vision 2020 goals with IBM MLS advances, MacB has a tradition of bringing technology and domain together to deliver Joint Warfighting capability. MacB has been solving some of the Nation's most complex National Security challenges and is committed to delivering mission critical capabilities, including ISR Systems and Operations, C2 Systems, Information Operations and Intelligence, IT Solutions, Research Development Test and Evaluation and offer a fresh approach to MLS.

References

1. Commander, Joint Chiefs of Staff publication: "Joint Vision 2020: America's Military: Preparing for Tomorrow", Page 6.
2. IEEE (1063-9527/92), "Security Test and Evaluation for Multi-level Mode Accreditation: Lessons Learned", 1992, Page 38.
3. http://www.lockheedmartin.com/us/news/press-releases/2009/september/Lockheed-MartinIBMDeliverR.html
4. Department of Defense IT Enterprise Strategy and Road Map, 6 Sep 11, Page 2.
5. Department of Defense IT Enterprise Strategy and Road Map, 6 Sep 11, Page 23.
6. Deputy Secretary of Defense Memo: IT Enterprise Strategy and Roadmap, 5 Oct 2011.
7. Ibid.
8. Department of Defense IT Enterprise Strategy and Road Map, 6 Sep 11, Page 14.
9. Strategic Studies Quarterly, Summer Edition 2010. "Wartime Alliances versus Coalition Warfare" by Patricia A. Weitsman, Page 118.
10. Ibid.
11. Ibid.
12. Peters et al, European Contributions to Operation Allied Force, Page 26.
13. Commander, Joint Chiefs of Staff publication: "Joint Vision 2020: America's Military: Preparing for Tomorrow".
14. '480th ISR Wing Improves Coalition Forces Information Sharing', www.afisr.af.mil/news/ story.asp?id=123266468
15. Ibid.
16. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28 STD (TCSEC/Orange Book)

Point of Contact

David "Doc" Robinson
MacAulay-Brown, Inc.
Systems Engineering and Operations Manager
757-896-6024, Ext 105
david.robinson@macb.com

Christopher "Jake" Jacobson, PhD
IBM Systems and Technology Group, U.S. Federal
Chief Technologist
757-240-8630
christopher.jacobson@us.ibm.com

Edward "Victor" Ballanco
EMB Information Technology Inc.
President
757-810-1751
edward.ballanco@embinfotech.com