Historical Snapshot and Future Direction
For the
Coalition Interoperability Assurance and Validation (CIAV)
And
Coalition Test and Evaluation Environment (CTE2)

Jeff Phipps, Chief, Coalition Branch
Joint Interoperability Test Command
3341 Strauss Ave, Suite 109
Indian Head, MD 20640-5935
301-743-4242 jeffery.c.phipps.civ@mail.mil

Todd K. Rissinger, Deputy Chief, Coalition Branch
Joint Interoperability Test Command
3341 Strauss Avenue, Suite 109
Indian Head, MD 20640-5935
301-743-4243 todd.k.rissinger.civ@mail.mil

Michael Leite, P.E., Principal Engineer
DigiFlight, Inc.
8825 Stanford Blvd. Suite 100
Columbia, MD 21045-4756
301-743-4223 michael.j.leite.ctr@mail.mil

Abstract

Coalition Interoperability Assurance and Validation (CIAV) is a process that examines the end-to-end execution of a mission thread as an element of an operational mission. It is concerned with the flow of data from its creation to its presentation to a commander as the basis for an action or decision. CIAV verifies the correct exchange of data, and it tracks the results of intermediate processing along the path from producer to consumer.

The CIAV Program incorporates both a U.S. DoD management and an international or Coalition management structure. The U.S. management is the responsibility of the Coalition Branch (JTC3) of the Joint Interoperability Test Command (JITC); it is located at JITC Indian Head, MD. The international management structure is the CIAV Working Group consisting of representatives from the current Coalition Partners and NATO.

The CIAV Program has established the Coalition Test and Evaluation Environment (CTE2). It is a distributed, persistent network operating on the Combined

Federated Battle Lab Network (CFBLNet). Participants on the CTE2 include U.S. Service and Component Laboratories as well as NATO and Coalition Partner laboratories. The CTE2 can replicate any operational mission network.

Background

The Coalition Branch (JTC3) of the Joint Interoperability Test Command (JITC) in Indian Head, Maryland, developed the Coalition Interoperability Assurance and Validation (CIAV) capability. It utilizes the Coalition Test and Evaluation Environment (CTE2). They were developed to support the United States Central Command (USCENTCOM) and the International Security Assistance Forces (ISAF) Joint Command (IJC) Afghanistan. The CIAV and CTE2 were researched, developed, and integrated in order to implement a global, coalition and mission-based interoperability assessment process that was separate and isolated from the operational networks in theater. The CTE2 specifically replicated the Afghanistan Mission Network (AMN). And, it is extensible to replicate any Coalition Mission Network.

The CIAV, using the CTE2, worked directly with the North Atlantic Treaty Organization (NATO), United Kingdom (UK) and additional Troop Contributing Nations (TCNs). It established an objective process for determining and assuring the mission-based interoperability of information-sharing systems and architectures for combat forces operating on the Afghanistan Mission Network.

The CIAV team provides Supreme Headquarters Allied Powers Europe (SHAPE), USCENTCOM, and the IJC coalition mission thread (CMT)-based assessment reports to document their systems' ability to achieve mission requirements. The scope of the assessments is determined from the current theatre enabling architecture, Coalition Tactics, Techniques, and Procedures (CTTP) and the established mission requirements. A capabilities and limitations (CAPS/LIMS) report which also includes the corresponding operational impacts is provided to key leadership of the combat commanders for each CIAV event. It is also shared with the associated program offices for knowledge management and adjudication.

The first CIAV events to be executed with coalition and allied partners included Canada, Great Britain, and NATO. The two 90-day events conducted in 2010 focused on the Battlespace Awareness CMT. It encompassed the following services: Blue Force Situational Awareness (BFSA), Air and Ground Track Management, Object Management, Significant Act (SIGACT) Reporting, and Troops in Contact (TIC) Reporting. The findings from the CIAV events resulted in critical technical modifications, process improvements and interoperability configuration adjustments to the national command and control (C2) systems that were used on the AMN by the IJC staff and its coalition partners.

Information from CIAV events is also provided to the Service training commands to ensure that the latest performance information is available to support the Relief in Process (RIP) and Transfer of Authority (TOA) processes. It provides timely knowledge to the deploying forces and thus reduces their in-processing time. In addition to assuring and validating the end-to-end interoperability of CMT's, the JITC Indian Head (JITC-IH) staff played a key role in the development and establishment of the AMN Governance which became effective on November 5, 2010.

JITC's efforts to establish the CIAV process, Working Group, and the subsequent development and integration of the AMN Governance process within SHAPE and led by the AMN Secretariat have established a mission-based interoperability (MBI) framework for identifying and correcting critical mission-based data-sharing and interoperability shortfalls with a managed and governed process called CIAV. Figure 1 shows the business process for the CIAV.

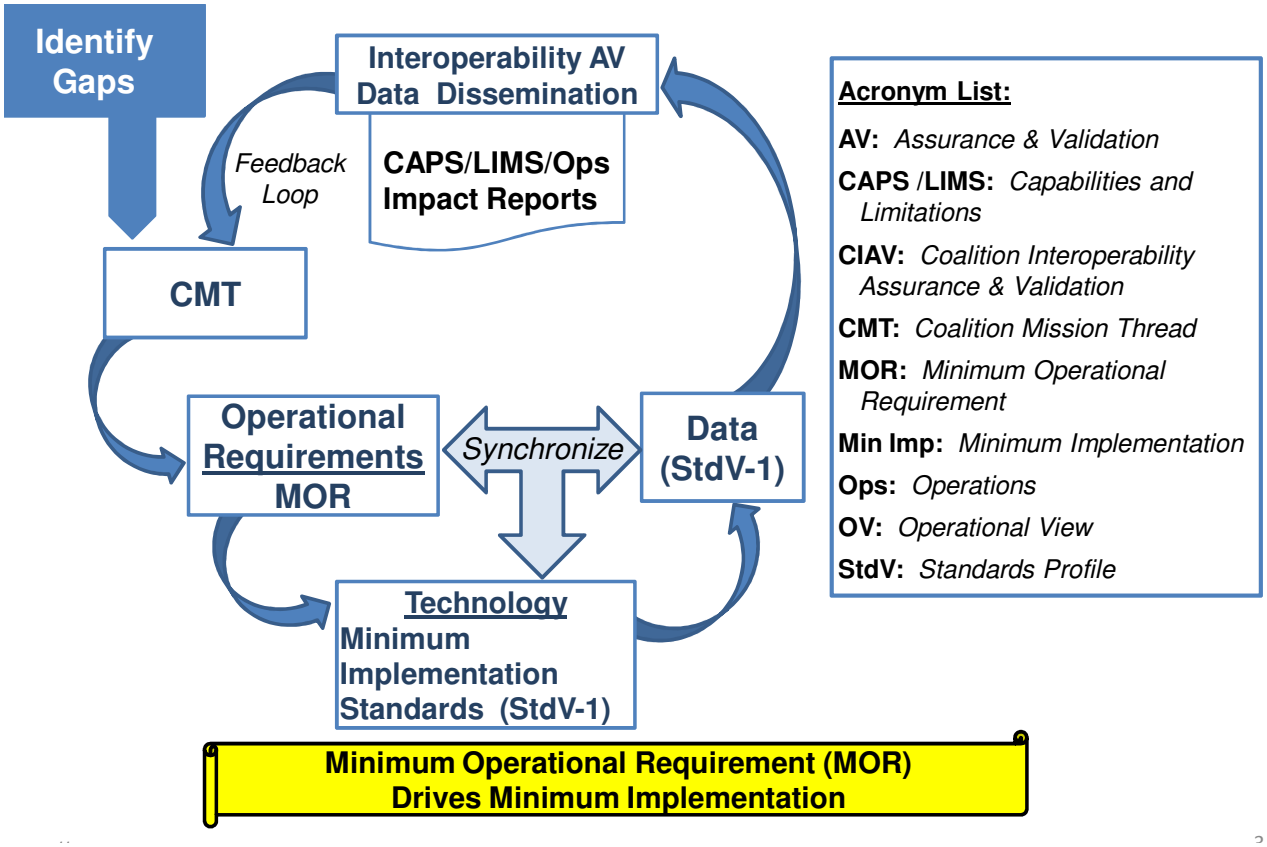

Figure 1. Operational View (OV-1) of the CIAV Business Process

Development of the CIAV Process

The initial direction for the establishment of the CIAV process came from the *Concept of Operation (CONOPS) for the Afghanistan Mission Network (AMN)*. Section 10.1 of the CONOPS directs that "… the purpose of testing and accreditation in the context of Functional Area Services (FAS) is to affirm the quality of service (QoS) provided by systems and to ensure their fitness for use. To achieve coherence and interoperability of systems and to provide high quality services, it is critical that the systems deployed on the AMN pass all required testing, meet identified standards criteria, and are assured for warfighting operational use."

The guidance was based on observed reductions in mission effectiveness due to an inability to share mission-critical information and a lack of interoperability on the part of coalition tactical data processors. The IJC and Commander Joint Operating Area Afghanistan (CJOA-A) identified interoperability as a critical shortfall; and they requested establishment of a process to provide coalition commanders with an increased information flow within their battlespace. During second and third quarters of fiscal year 2011, the JITC-IH team developed, integrated, and executed the CIAV process and conducted events on the CTE2 which included assessments of the Counter Improvised Explosive Device (CIED); Joint Intelligence, Surveillance, and Reconnaissance (JISR); and Joint Fires (JF) mission threads. Participation in the events expanded from the original two coalition partner nations (utilizing one alliance, and six geographically dispersed locations) to six coalition partners (utilizing one alliance and eleven geographically dispersed locations). The number of participating nations and sites is shown in Figure 2 and continues to grow.

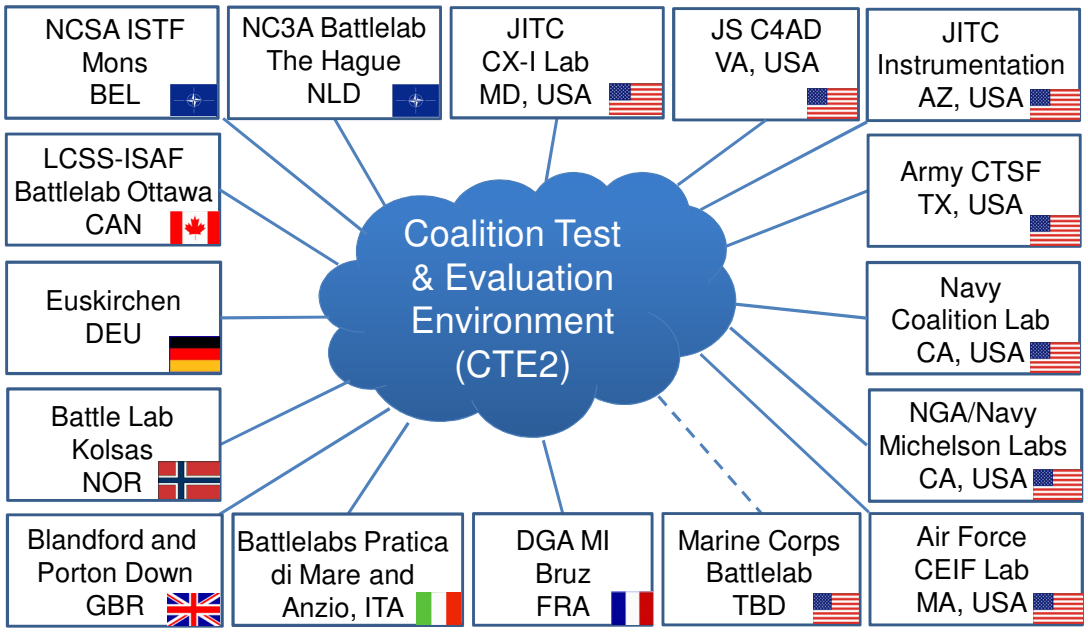

Figure 2. CTE2 Participants

CIAV Process

The thrust of the CIAV effort has been to ensure that mission threads operate seamlessly from end to end (E2E). To do this, the CIAV process works from the mission requirements and through the technical implementations for all of the systems supporting the mission thread. Figure 3 shows the notional CIAV assessment process. Because operational systems continually evolve, the CIAV process is iterative. CIAV events are mission thread focused to identify interoperability problems; they are not system tests. The CIAV reports provide MBI capabilities and limitations with respect to performance of the mission thread and also include an operational impact statement.

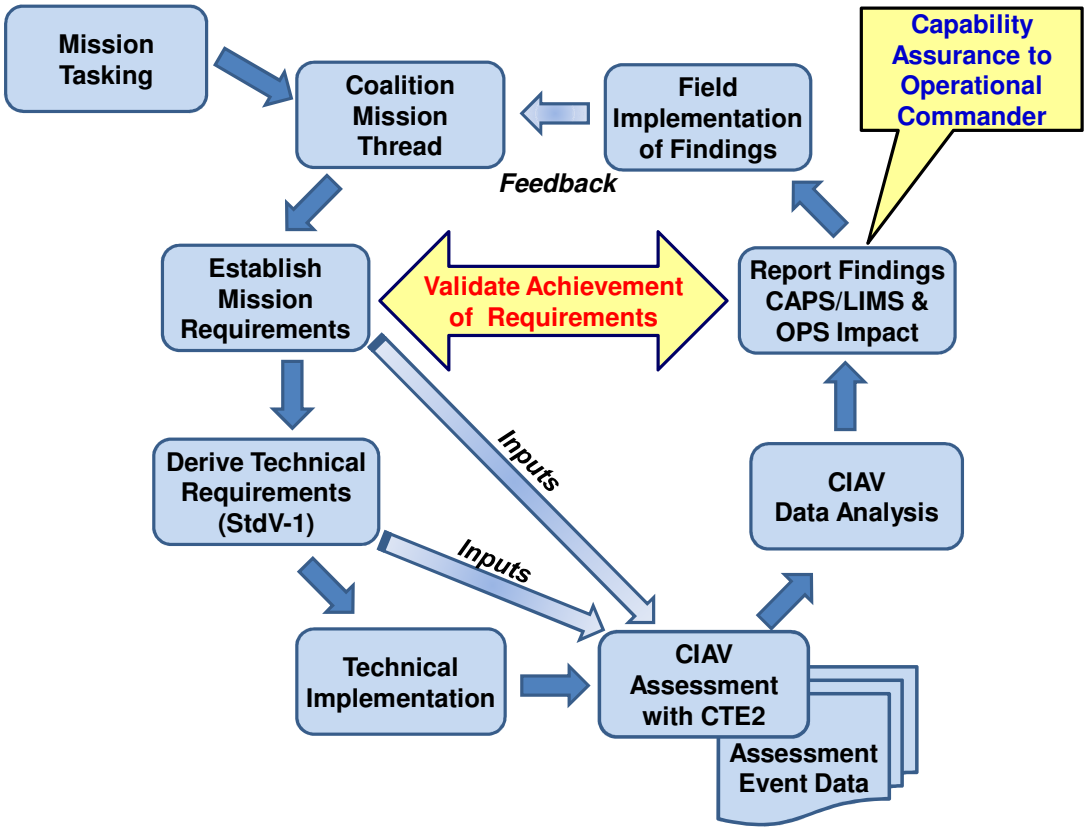

Figure 3. Notional CIAV Process

The operation of the CIAV and its process are designed for quick response. Events are scheduled on a three-month or 90-day cycle. This enables the team to schedule, plan, execute and analyze assessments in the shortest time possible and deliver a timely response to the theater commander. Focusing on mission thread execution allows large problems to be divided into smaller, manageable elements; this also facilitates the implementation of solutions across the coalition networks and processors. Additionally, when follow-on assessments are indicated, they can be scheduled in a more

timely manner—again providing a more timely response to the field. Figure 4 illustrates the notional three-month event cycle.

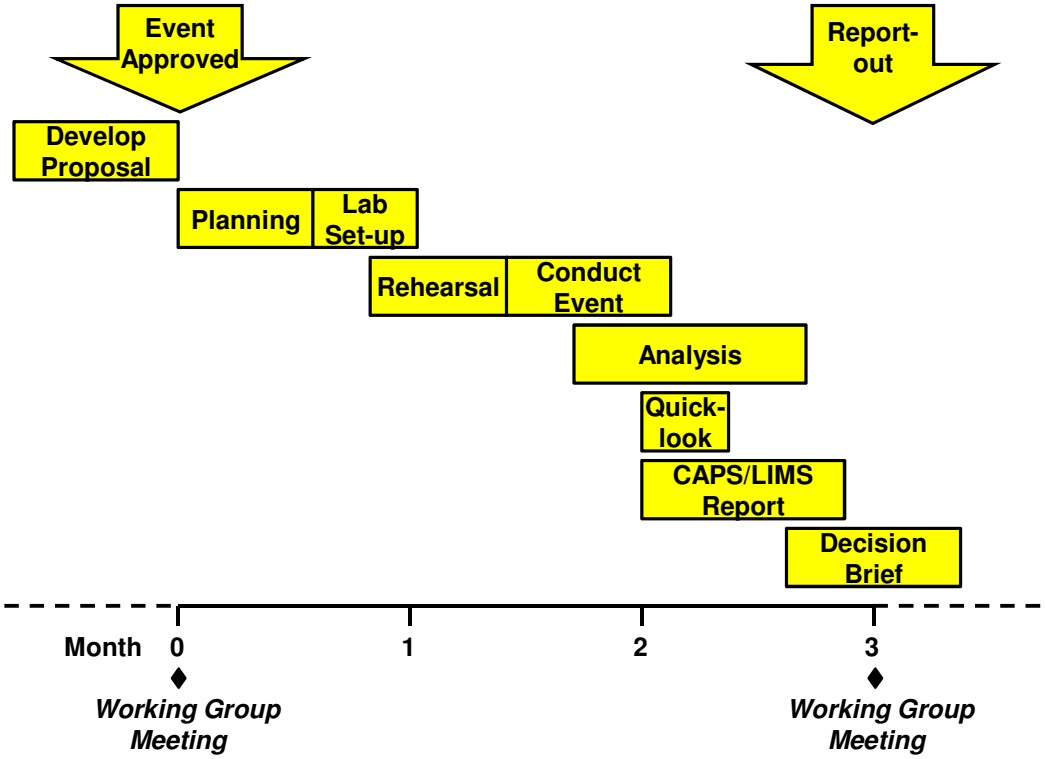

Figure 4. Three-month CIAV Event Cycle

CIAV is Critical to Global Data Sharing

The overall goal of CIAV is successful execution of the operational mission through global information sharing. The following provides a brief history and traces the evolution of the Joint Capability Areas (JCAs) for the AMN to the eight current Coalition Mission Threads (CMTs). It also shows how the CIAV process developed to support this context. The following definitions provide context to the description of the implementation of the CIAV process.

- **Joint Mission Thread (JMT)** is a US operational and technical description of the end to end set of activities and systems that accomplish the execution of a joint mission. (CJCSI 6212.01E)

- **Coalition Mission Thread (CMT)** is the operational description of the activities and operational data required in order to successfully execute a coalition mission.

- **Services** are discrete functions which are required to execute a mission thread. A service may support more than one mission thread.

Each CMT is broken down into its associated Services. The CMT and its associated services should define the complete set of requirements to execute the full CMT; however, at a minimum, they must establish the Minimum Operational Requirement (MOR) for acceptable mission success. The MOR identifies the most critical operational information necessary for the operational commanders to successfully execute the mission. This is detailed in the Commanders Critical Information Requirements (CCIRs); and a set of CCIRs is established for each CMT and its associated services. The CCIRs provide the baseline data sharing requirements for all Coalition nations to utilize when building their systems and associated architectures.

The MOR provides the operational input to the technical requirement and guidance that should be applied to the system or application designed. This frames the technical Minimum Implementation (Min Imp) criteria to be used when implementing the adopted standards from the Standards Profile (StdV-1) of the Coalition architecture. The MOR, coupled with the Min Imp, identifies the critical data required by the operational commander to conduct his mission and allows for an end to end trace of the data when applied to the associated architecture products. This is illustrated in Figure 3 above. *The CMT facilitates the Tactics within the Tactics, Techniques, and Procedures (TTP).*

The initial AMN Enterprise Services were aligned to the U.S. Department of Defense (DoD) standard known as the Joint Capability Areas (JCAs). They were subsequently restructured and renamed in 2009 as the initial eight Coalition Mission Threads (CMTs) supporting the Afghanistan Counter Insurgency (COIN) battlespace. Each CMT then identified specific functional area services (FAS) that made up the CMT mission for the COIN operational requirements. The nine JCAs and the resulting eight initial CMT's are listed in Table 1.

Table 1. Joint Capability Areas and Coalition Mission Threads

Nine Original JCA's	Eight Initial AMN CMT's
1. Force Support	1. Battlespace Management
2. Battlespace Awareness	2. Joint Fires
3. Force Application	3. Joint ISR
4. Logistics	4. MEDEVAC
5. Command and Control	5. Counter IED
6. Net-Centric	6. Freedom of Movement
7. Protection	7. Force Protection
8. Building Partnerships	8. Service Management
9. Corporate Management & Support	
NOTE: JCA and CMT numbering is not correlated; it is for context only)	

Mission threads are processes that trace a complete path contributing to the accomplishment of a mission task. They may include excursions or alternate paths based on established decision criteria. The mission thread forms the basis for the development of the use cases and their resulting scenarios to be used in the assessment event. Figure 5 shows a notional ISR mission thread.

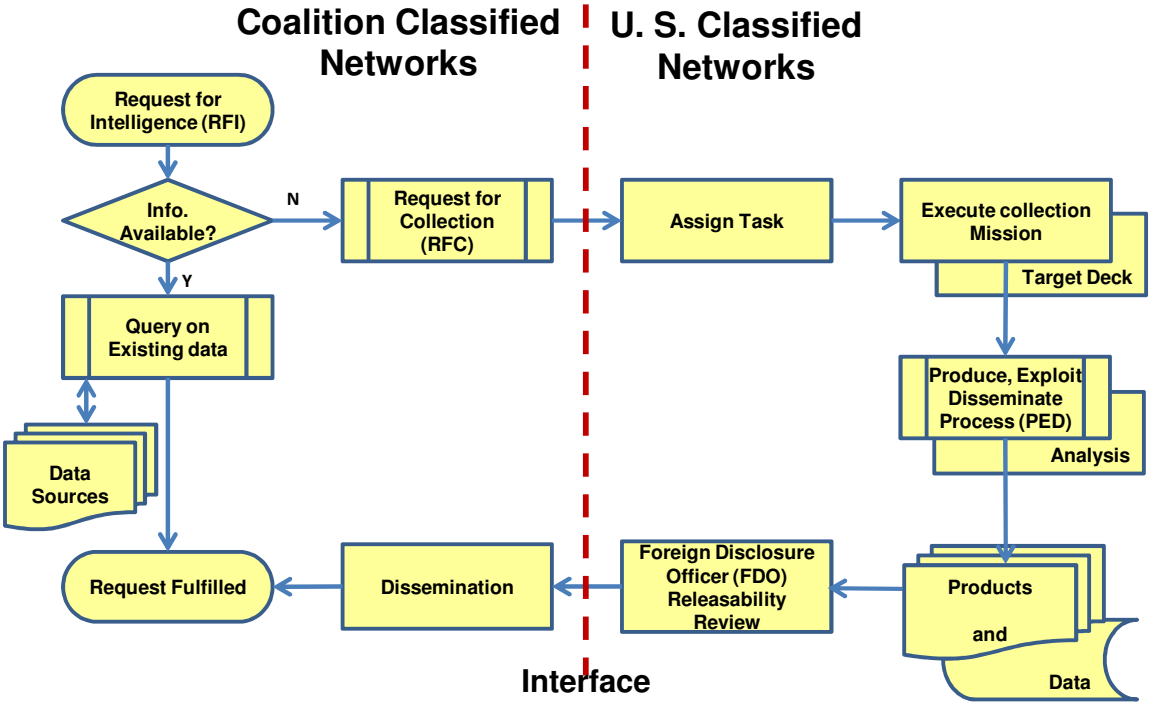

Figure 5. Notional ISR mission thread

Each mission thread has an associated set of services that are required for its accomplishments. Each service can support multiple mission threads. Figure 5 shows how individual services are aligned to the Coalition Mission Threads. By utilizing the process for the mission thread and its associated services, a data model can be developed which represents the data flow for the mission thread. An analysis of the data model will reveal anomalies which can be resolved by normalizing the data and adjusting the data flow; this is reflected in the operational systems by adjustments to the implementation of the technical standards. It also identifies instrumentation points that will be required for execution of the assessment event on the CTE2. Figure 6 shows the services associated with each of the mission threads on the AMN.

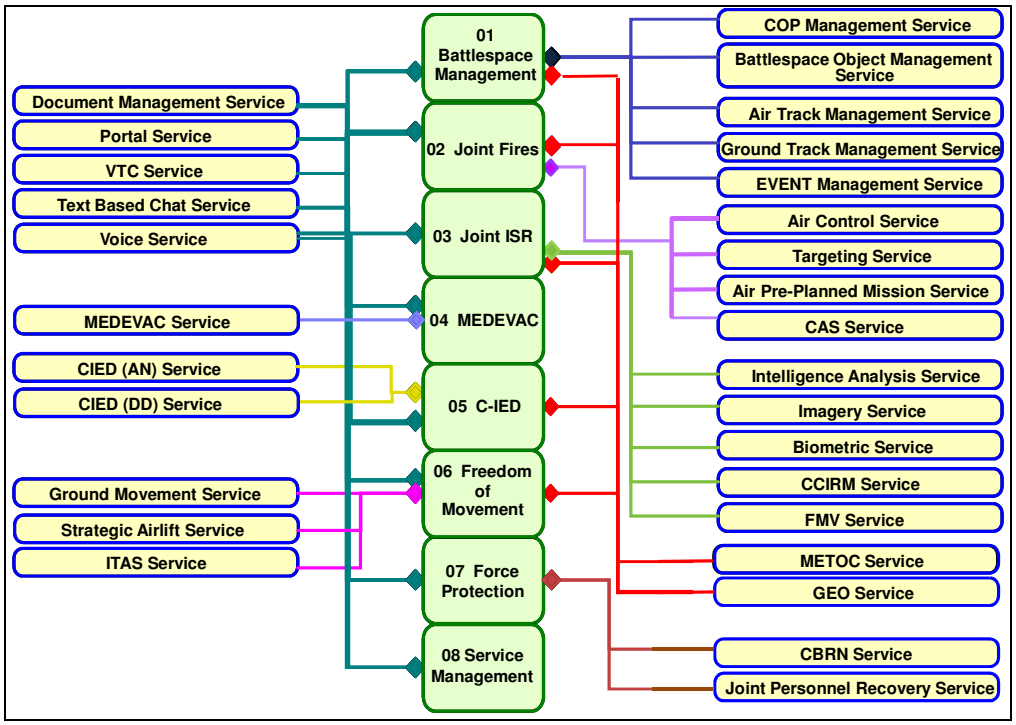

Figure 6. Relationship of Services to Coalition Mission Threads

The overarching US National network in the AMN is the ISAF implementation of the Combined Enterprise Regional Information Exchange System (CENTRIXS) or (CX-I). The Operational View (OV-1) for the AMN depicts the information sharing environment with common enterprise and C5ISR services supporting the commanders' "Plan, Decide, Execute, and Assess (PDE&A)" decision cycle. These services, at the high operational level, should include a user-defined Common Operating Picture (COP), data standards identification, event/role/content-based data-sharing requirements, friendly/enemy status information sharing, and dynamic Communities of Interest (COI). ***This aspect facilitates the Techniques and Procedure within the TTP context.***

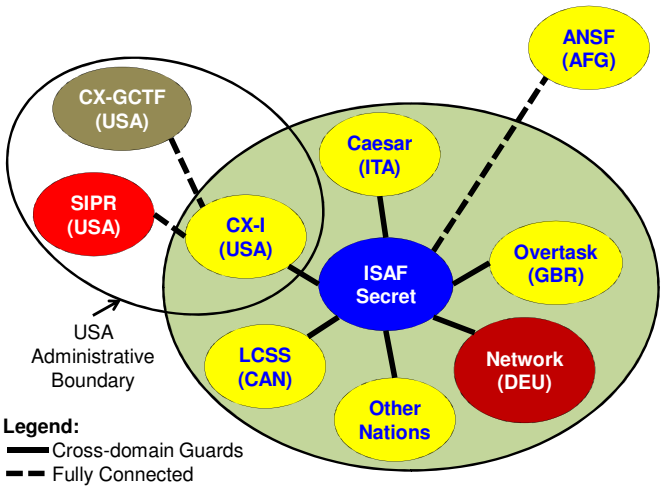

Figure 7. CENTRIXS Interface to AMN

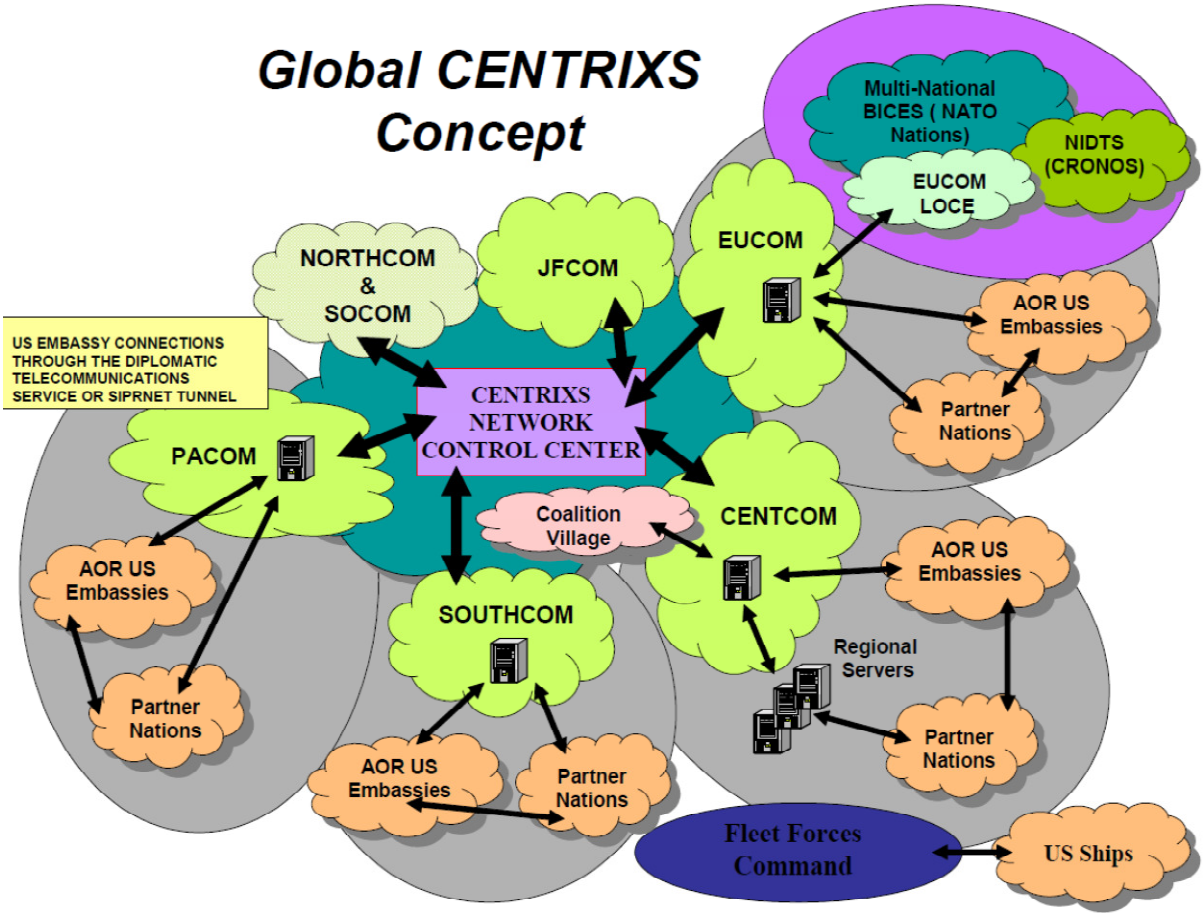

Figure 8. Global CENTRIXS Concept

Figure 7 shows the interface of CENTRIXS to the AMN for U.S. participation in Coalition information exchange. CENTRIXS is a global U.S. capability; it is illustrated in Figure 8. CIAV, with its CTE2 distributed architecture, can perform assurance and validation assessments for COCOMs in any theater.

Battlespace Management and ISR are the two core mission threads required for any global theater operation. They provide access to, and visibility of, critical mission data for command and control (C2) to allow decision makers to effectively task assets and maintain situational awareness (SA) through the Common Operational Picture (COP) and Common Tactical Picture (CTP).

To achieve economies in coalition mission data sharing and system interoperability, the formal identification and prioritization of a set of common mission-based warfighting requirements is required. It must be coupled with an assurance and validation process that is also mission-based. Since the inception of militarized conflict, the side with the best knowledge has emerged victorious because its strategies had the most accurate situational awareness. That knowledge resulted in an ability to shift the order of battle.

At the operational and tactical warfare levels, the command and control (C2) systems must support robust decision-making capabilities and provide situational awareness (SA) for planning and execution. Participating nations are required to establish formal processes in accordance with their national policies and procedures for the release of information to the other participating nations in order to successfully coordinate the execution of the Coalition mission. Access to information must be controlled in accordance with each coalition participant's level of participation and planning needs. The overall goal is to ensure that the dissemination of operational data is correct with the data being provided in the right format, with the proper fidelity, to the right people and at the right time.

Additionally, the Coalition information environment must account for and support the exchange of classified information under multiple classifications and disclosure policies in a wide variety of physical and virtual environments. Not all coalition members are granted access to all information held by member nations. Access criteria are defined in the agreements among the nations (e.g.: bilateral, multilateral and NATO) and are captured in the collective data-sharing requirements of the Coalition battlespace. This requires development of multi-level security and an accreditation capability to support the coalition information-sharing environment in support of the mission.

Within the Afghanistan Mission Network (AMN), the overarching principle for enterprise data sharing and interoperability is based upon a common definition of the coalition mission threads and their associated services. It is coupled with applied "full trust" and effective information sharing. These are based upon interoperability through common implementation of standards and special agreements as mandated by the HQ ISAF Policy on the AMN of December 2009. Each AMN participating nation has the responsibility to ensure that all operational requirements are met to successfully execute the services aligned under the CMTs. This requires that each nationally-provided system be developed, integrated, and interoperable prior to deployment to the warfighting environment. National oversight within the AMN governance structure is responsible for ensuring that all changes and upgrades to systems in support of the AMN have the proper oversight to operate interoperably prior to deployment and operational integration.

The Coalition Interoperability Assurance and Validation (CIAV) process was designed to provide objective assessments based on operational requirements. The assessments are documented in a Capabilities and Limitations (CAPS/LIMS) Report and an Operational Impact Report (OIR). The reports provide the coalition leadership with findings and recommendations to understand how the AMN and its associated services perform in support of the CMTs. In other words, CIAV provides the operational commander a "fit for use / fit for purpose" report based upon his mission execution criteria and identifies the operational gaps to mission accomplishment.

To facilitate the establishment of a network structure for future coalition operations, the processes established for the AMN can serve as the guideline for the development of the Future Mission Network (FMN).

Addressing identified mission gaps is the second focus of the CIAV. For U.S. entities supporting the Afghanistan AOR, mission-based interoperability requirements are coordinated through USCENTCOM (CCJ-2, 3, and 6). However, with the USCENTCOM's priority to fight the war, sponsoring changes to U.S. systems is a tertiary responsibility; and thus, it is not a priority of the main USCENTCOM thrust. Rather, it is entrusted to the US CIAV team. Accordingly, CIAV-developed recommendations coordinated with USCENTCOM are also passed to the Joint Staff and the applicable Services and their program offices for action. The goal is to ensure U.S. modifications to mission-based services and systems are developed, integrated, and tested prior to fielding and deployment. The CTE2 is a venue that allows for assessing new and emergent systems for Allied and Coalition interoperability. In short, CIAV provides feedback to mission commanders as well as acquisition programs regarding potential interoperability problems.

Lastly, the Coalition information sharing environment must be capable of global operations, accepting data from or providing data to existing operational networks regardless of location. Potential coalition members will continue to develop and evolve their C2 and ISR systems which, in turn, will have to exchange mission-critical information upon joining a coalition. Those systems must be interoperable within the multinational information sharing environment. Maintenance of each member's mission contribution to the overall information-sharing environment is their individual responsibility. The only current method to conduct MBI and assure the mission and capability of our own and our partner systems is through CIAV events.

CIAV & Mission-based Data Sharing, Management, & Interoperability

Data sharing, interoperability, and management are among the critical areas that comprise the growing challenges facing the global battlespace. In the recent past, mission data were largely developed and maintained by individual national systems. This created stovepipes of mission-critical information that was non-interoperable and not formatted for enterprise sharing. Based upon this observation, some key themes emerged from AMN lessons learned:

- Data sharing problems are not unique to any one mission, functional area, organization, or nation.

- There is a need for standardized coalition and enterprise-wide mission-based data sharing policies, doctrine, plans, processes, and supporting infrastructure.

- Mission-based operational data requirements must be clearly defined and drive the technical solutions

- Mission-based data sharing requirements and data management plans are not currently addressed adequately in the budget or acquisition processes.

- A paradigm shift away from a system-centric approach to a command and mission-centric approach is needed immediately. It must be based upon operational requirements and standardized processes.

Figure 9 depicts the major elements of a data strategy. The major elements are based on past and current DoD guidance.

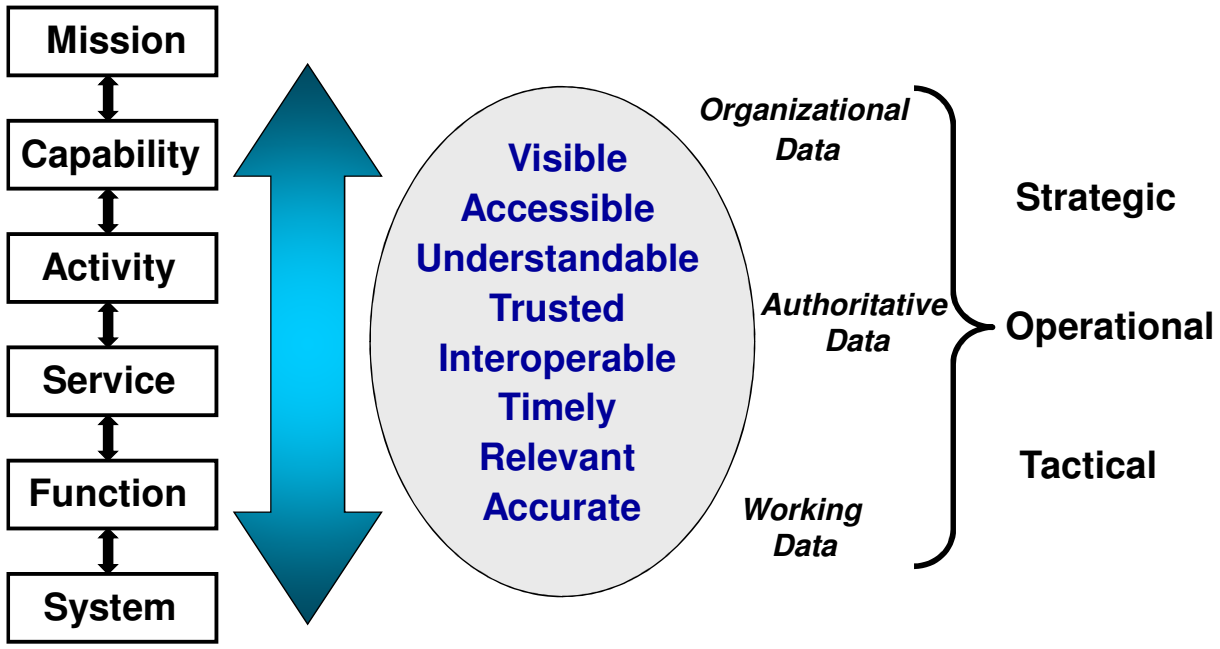

Figure 9: Data Interoperability and Synchronization

The principal knowledge gained to date from the operational AMN and CIAV mission-thread lessons learned is the need for enhanced operational mission-based data-sharing (interoperability). Mission-based data-sharing is the optimization of information flows across the Coalition Enterprise. The success of the AMN and "cloud" warfighting has introduced a global data-sharing (interoperability) requirement that has changed the way we think about the management of mission-critical information. It includes the need to ensure the operational requirements and the standards comprising the technical architecture are coordinated for implementation across the coalition warfighting environment.

Some enabling concepts should be addressed for the implementation of an enterprise approach to data management, they include:

- Data ownership will shift as information traverses the Coalition enterprise from producer to consumers.

- Produced data will be shared across the operational continuum. It will be used by a multitude of services and functions. Many of these will be different from those for whom it was originally intended to support, and they will constitute an expanding group of consumers not envisioned by the data producers.

- The visibility and accessibility of mission data across the enterprise will create an imperative that the enterprise must institutionalize and maintain designated, authoritative data sources (i.e., data producers and custodians) to ensure information is trusted and traceable.

- Data must be developed with embedded, specific release caveats and fixed tracking numbers from its inception in order to avoid corruption, storage stovepipes and duplication of information which could significantly hamper network performance and reliability.

- Enterprise data must be discoverable and understandable to the extent it does not violate information assurance (IA) requirements or security release agreements.

Governance

Governance has been an essential aspect of the success of the AMN and CIAV strategy and for the technology implemented for mission execution. The successful development and transition of technology requires a formally structured governance process that provides leadership, direction, and oversight. The AMN governance developed by the CIAV team facilitated the rapid testing, assessment and remediation of deficiencies in mission thread execution. Key CIAV member nations participated in the development of the AMN Governance structure; this ensured that their concerns were addressed in the execution of CIAV events and facilitated their participation in the implementation of recommended actions. The team also established a standardized approach that utilized proven system engineering processes, assessment methods, and reporting practices.

Figure 10 graphically depicts the relationship between CIAV and the operational AMN through the AMN Governance structure. It also shows CIAV support provided through the pre-deployment/training process where units are introduced to AMN while in garrison, at training sites, and/or pre-deployment stations.

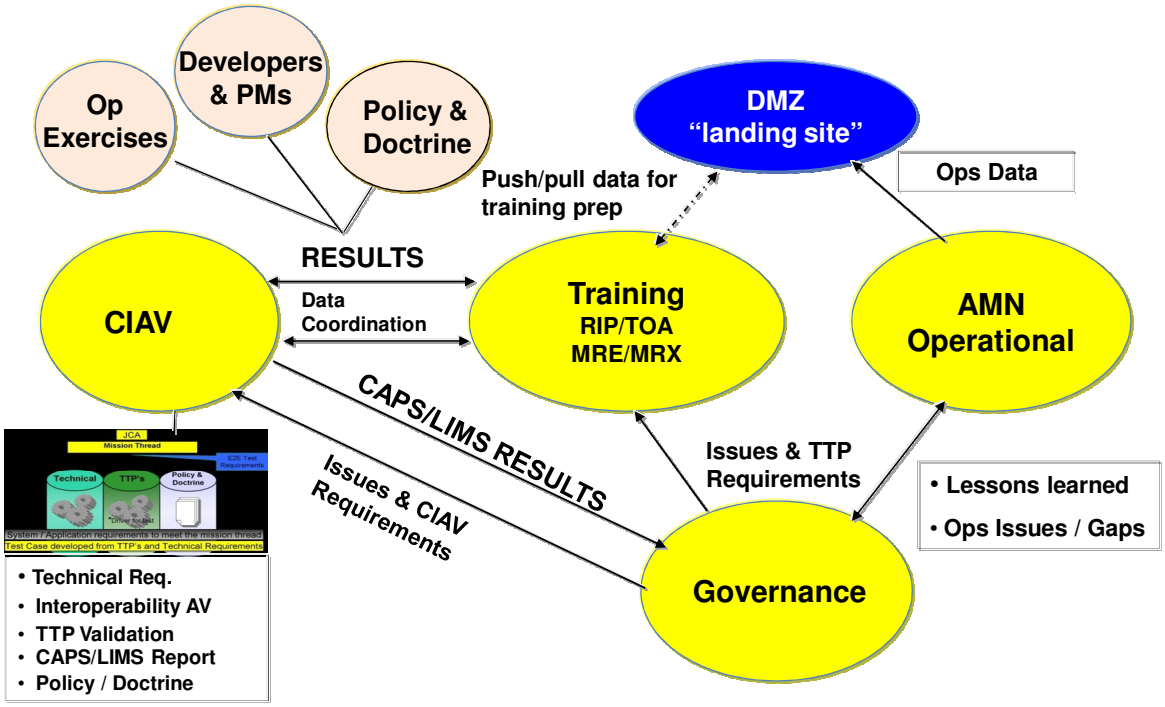

Figure 10. Operational View (OV-1) of the CIAV Operational Process

Summary

The direct benefits of the CIAVprocess to the US DoD are:

- Maintaining constant focus on mission accomplishment from initial planning to final Full Operational Capability (FOC) delivery
- Standardization of mission-based operational requirements and providing objective Capabilities and Limitations (CAPS/LIMS) reports on CMT performance to the warfighter and leadership which permit a "fit for use, fit for purpose" decision by theater leadership
- Presenting leadership with mission-based Earned Value (EV) data for return on investment (ROI) reporting as technology transitions to operational use
- Expanding overall program transparency by providing enterprise end-to-end progress reporting of mission performance with the overall goal of reducing current silo processes

Conclusion

Establishing and standardizing a DoD-wide Coalition Interoperability Assurance and Validation (CIAV) process will implement a mission-centric, value-added capability to support all aspects of a mission-based development. And, it will ensure that critical mission data are produced and made accessible across the enterprise. The direct focus of the CIAV process is geared toward assuring the successful operational execution and delivery of warfighting capabilities to support our global forces. The availability of a process that addresses the operational mission threads at the Coalition and Theater levels is critical to U.S. mission success.

CIAV is a new strategy that supports rapid discovery, design, development, integration, information assurance, and interoperability of mission-based systems. Using the CTE2, the CIAV can replicate any theater or coalition network and architecturally validated mission data flow enterprise in an environment that does not interfere with operational traffic.

The global battlespace and geo-political landscape are constantly changing. This requires an assurance and validation environment that is capable of meeting the challenges of technology change and also maintaining visibility and control as the coalitions develop and mature. As demonstrated in Afghanistan, CIAV can meet the challenge with its MBI standardized process and provide Coalition support and value-added insight for all phases of the DoD Acquisition Process.

AUTHOR BIOGRAPHIES

Jeff Phipps is Chief, Coalition Branch, Joint Interoperability Test Command (JITC); in that capacity he serves as US Chairman for Coalition Interoperability Assurance and Validation (CIAV), Test Manager for the DISA Multinational Information Sharing (MNIS) Program Management Office (PMO), and JITC Indian Head Lead for the DoD Interoperability Communications Exercise (DICE). Prior to joining JITC, he served in the U.S. Air Force; his assignments included Hellenikon AB, Greece; Bitburg AB, Germany; Grand Forks AFB, ND; and Hurlburt Field, FL. During Operation Enduring Freedom he served in in Oman, Pakistan, Uzbekistan, and Afghanistan.

Todd K. Rissinger is Deputy Chief, Coalition Branch, Joint Interoperability Test Command (JITC), where he leads the operational strategy and execution of the Coalition Interoperability Assurance and Validation (CIAV). He also leads tasking for mission-based business, testing and warfare areas affecting the Afghanistan Mission Network. He has supported initiatives of the Office of the Secretary of Defense, Joint Staff, U.S. Central Command, the Services, and multiple coalition national efforts. Following his retirement from the U.S. Navy, his career has included: SPAWAR FORCEnet Project Manager, Tactical Data Link and C4I Interoperability Test Division Head at the Naval Center for Tactical Systems Interoperability, U.S. Navy Participating Test Unit

Coordinator at JITC, Tactical Data Link Subject Matter Expert to the Chief of Naval Operations (CNO N6/7), C4I consultant to the Naval Network Warfare Command, and a subject matter expert on NetCentric and GIG-related projects at the Naval Space and Naval Warfare Systems Command (SPAWAR).

Michael Leite is a Principal Engineer for DigiFlight, Inc., where he provides Test and Evaluation support to the Coalition Branch of the Joint Interoperability Test Command. In previous assignments he provided test and evaluation support to the Director of Operational Test and Evaluation and the Army Test and Evaluation Command. His Test and Evaluation experience also includes Developmental Testing for the Naval Sea Systems Command and AEGIS Shipbuilding Program and Operational Testing for the PATRIOT Missile Program. A retired Navy Captain and a Registered Professional Engineer, he has previously supported modeling and simulation efforts at the Defense Modeling and Simulation Coordination Office, Missile Defense Agency, DD-21 Gold Team, Cooperative Engagement Capability Program, and the Joint Theater Air and Missile Defense Organization.