



# TechNet Augusta

August 16–19, 2021 | Augusta Marriott at the Convention Center | Augusta, GA

## 2021 SOLUTIONS SHOWCASE





# AFCEA TechNet Augusta Solutions Review

## Welcome to TechNet Augusta and the 2021 Solutions Review.

With assistance from the U.S. Army Cyber Center of Excellence and industry experts, TechNet Augusta 2021 is designed to open the lines of communication and facilitate networking, education and problem solving. This Solutions Review Compendium complements the event and helps build engagement in advance.

In preparation for the conference, AFCEA, working with the U.S. Army, identified a series of problem statements, and the commercial sector was offered the opportunity to respond to the statements by describing their proposed solutions in the form of products, services and ideas. The industry abstracts submitted are included in this compendium and cover many of the complex challenges the Army faces, both from peer and from near-peer adversaries, not only on the sea and land but also in the air and in cyberspace.

The Solutions Review offers industry the opportunity to engage and respond to pressing problems. Companies were invited to offer solutions to the following areas:

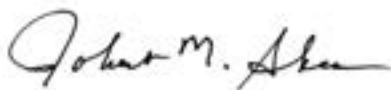
- C4ISR/EW Modular Open Suite of Standards (CMOSS) Compliant Capability
- Non-Traditional Waveforms for Information Advantage (IA)
- Near Term Emerging Radio Technologies
- Network Modernization
- Human Behavior Modeling in Support of Information Advantage Effects Adjudication
- Identify Capabilities that Can Support Army Military Information Support Operations Using Radio Frequency Delivery Methods
- Cross-Domain Solutions for Army Tactical Networks
- Automated Signal Recognition and Technique Generation
- Managing Information Related Data
- Publicly Available Information (PAI)
- Cross-Domain Solutions

Organizations that developed problem statements included:

- Army Capabilities Manager, Networks & Services
- Army Capabilities Manager, Cyber
- Cyber Battle Lab (CBL)
- Army Capabilities Manager, Electronic Warfare
- Army Program Office-Information Advantage (APO-IA)

We encourage you to review the problem statements and solutions to understand both the military's requirements and industry's creative approaches to address how to build a multi-domain force.

Sincerely,



**Lt.Gen. Robert M. Shea, USMC (Ret.)**

President and Chief Executive Officer, AFCEA International

# Problem Statements

## Army Capabilities Manager (ACM) Networks & Services

### C4ISR/EW Modular Open Suite of Standards (CMOSS) Compliant Capability

**Problem Statement:** From competition through conflict, what CMOSS compliant capabilities building upon existing CMOSS mounted form factor (CMFF) efforts are required to achieve information advantage in multi-domain operations (MDO)?

The Army is pursuing methods to improve size, weight, power, and cost (SWAP-C) and integration of overall cost, schedule, and performance factors relevant to supporting warfighting functions during multi-domain operations (MDO). The Army identified the need for a CMFF materiel solution to facilitate the consolidation of disparate systems into a common ruggedized chassis. (C4ISR/EW modular open suite of standards [CMOSS] form factor [CFF] [CMFF]- Abbreviated – Capability Development Document [A-CDD] signed January 4, 2021.) The Army is seeking the best methodologies, CMFF chassis technologies, and CMOSS compliant capability cards to achieve information advantage (IA).

**Why this is important:** CMOSS implementation has the potential to improve SWAP-C, overall costs, schedule timelines, and performance, to simplify integration, and to increase the pace of modernization. Modernizing IA capabilities to pace threats and meet operational demand plays a critical role from competition through conflict.

### Non-Traditional Waveforms for Information Advantage (IA)

**Problem Statement:** In competition and crisis, what waveforms does the Army require to be implemented on available software-defined radios for information advantage to maintain freedom of action and impose its will against peer adversaries in all domains to deter conflict while re-establishing a position of strategic advantage?

Traditionally waveforms implemented on software-defined radios have been developed and employed with resiliency in mind to gain and maintain decision dominance and support to tactical maneuver through effective voice and data communications. This traditional function is an essential element to achieve multi-domain operations (MDO). However, other waveforms are required to achieve needed electronic warfare (EW), cyberspace operations, and information effects.

**Why this is important:** Answers to this problem will inform future experimentation and requirements for tactical software-defined waveform and radio development.

### Near Term Emerging Radio Technologies

**Problem Statement:** In crisis and conflict, how does the Army maintain resilient data and assured voice communications to gain and maintain decision dominance while persisting through adversary anti-access/area denial (A2/AD) capabilities?

To support information advantage at the tactical edge, the Army will require intelligent software-defined radios, waveforms, and ancillaries that improve mobility, cover (hardening/concealing), and deception.

**Why this is important:** Answers to the problem will inform future experimentation and requirements for tactical software-defined waveform and radio development.

## Army Capabilities Manager (ACM) Cyber

### Network Modernization

**Problem Statement:** The Army has a requirement to advance its tactical networks to counter emerging threats, enable new forms of maneuver, and maintain integration with military information technology (IT) services available stateside – all while taking advantage of rapid innovation from the commercial IT industry.

Communicating securely with command-and-control and other units within the increasingly communications-reliant battlefield landscape is critical to ensure the success of the mission and the safety of warfighters. However, as the battlefield evolves, missions require units to be mobile and support a myriad of tactical capabilities, such as:

- Networks that are self-healing; provide ease of entry; enable high data bandwidth; are protected and resilient; support mobility (no static infrastructure to support); are light weight; and are extensible when augmented with aerial nodes.
- Maximize cyber (CY)/electronic warfare (EW) effects delivery through network and tactical radio frequency (RF) systems.
- Integrate systems/data with Electronic Warfare Planning Management Tool (EWPMT), cyber situational understanding (CY SU), and unified network operations (UNO).

**Why this is important:** To enable our warfighters to communicate at all echelons in contested and congested environments during the conduct of multi-domain/joint all-domain operations (MDO/JADO) up through large scale combat operations.

**Question 1:** What impacts will information advantage (IA) operations have to the DoDIN-A within the integrated enterprise network (i.e.: network security, network transport, services infrastructure, computing environment, Department of Defense Information Network (DoDIN) Operations, etc.)?

**Question 2:** What impacts will information advantage (IA) operations have to the DoDIN-A within the integrated tactical network (i.e.: network security, network transport, services infrastructure, computing environment, Department of Defense Information Network (DoDIN) Operations, etc.)?

## Cyber Battle Lab (CBL)

### Human Behavior Modeling in Support of Information Advantage Effects Adjudication

**Problem Statement:** Current Army modeling and simulation (M&S) capabilities generally do not incorporate human behavior modeling at the tactical/avatar level, and only limited human behavior modeling capabilities exist at the operational/group level. The video game industry, however, has utilized basic to advanced human behavior models and algorithms for decades.

How can the Army leverage private industry's work by incorporating human behavior models and algorithms into Army programmatic M&S capabilities, particularly for virtual and constructive M&S capabilities?

**Why this is important:** Increasing emphasis on adjudicating the effects of operations and actions within information advantage's information related capabilities will quickly require greater demand to model human behavior and reactions to complex stimuli.

## Identify Capabilities that Can Support Army Military Information Support Operations Using Radio Frequency Delivery Methods

**Problem Statement:** The data outputs from information warfare (IW), open source intelligence (OSINT), publicly available information (PAI), public affairs officer (PAO), and Military Information Support Operations (MISO) do not strongly conform to the object based production in practice across the Intelligence Community (IC). The automated ability for entity objects generated from activities related to IW is very relevant to the transformative nature of deep sensing for intelligence and cyber operations.

**Why this is important:** The Army must know how to maintain resilient data and assured voice communications to gain and maintain decision dominance while persisting through adversary anti-access/area denial (A2/AD) capabilities during completion and armed conflict.

## Army Capabilities Manager (ACM) Electronic Warfare

### Cross-Domain Solutions for Army Tactical Networks

**Problem Statement:** Army electromagnetic warfare systems, including the Electronic Warfare Planning and Management Tool (EWPMT) operate and process or utilize data on the Secret NOFORN (S//NF) classification domain at brigade and below. However, the Command Post Computing Environment (CP CE) on which most Army computing systems will function has a mandate to operate no higher than Secret Releasable (S//REL) classification domain at brigade (BDE) level and Sensitive But Unclassified (SBU) classification domain at battalion (BN) level.

**Why this is important:** Without a viable cross-domain solution, many Army capabilities will effectively become useless as they will not be able to access, process, or share critical data.

## Automated Signal Recognition and Technique Generation

**Problem Statement:** To achieve electromagnetic spectrum dominance, the Army desires the ability to automatically detect and identify signals from 1kHz – 40GHz with an output of equipment notation (communications emitter notation (CENOT), electronic intelligence notation (ELNOT), commercial ID, or waveform) and generate techniques to mimic, or disrupt, signals at the given range from the receiver or recommend optimum transmitter placement based on user selected terrain and desired effect (disruption, emulation/spoofing or link establishment for connectable devices).

**Why this is important:** This will reduce the task load on Army electronic warfare operators in a dynamic and saturated multi-domain environment.



## Army Program Office-Information Advantage (APO-IA)

### Managing Information Related Data

**Problem Statement:** The Army requires a means to aggregate, store, and secure information related data across disparate platforms and sensors to provide a common operating picture of the information dimension in the operating environment. Currently there are many different organizations and systems that obtain information related data but most of those are not shared. With the development of information advantage organizations and capabilities, there is a greater need to share this data.

**Why this is important:** When all information related data is shared and displayed in a common operating picture, the commanders are able to speed up the decision-making process and decrease adversaries' ability to make decisions.

### Publicly Available Information (PAI)

**Problem Statement:** The Army lacks the ability to achieve information advantage through the use and application of publicly available information. The Army will require the ability to sense, understand, act, and decide on publicly available information (PAI). PAI increases the situational awareness and enhances the common operating picture and information operations.

**Why this is important:** To conduct effective operations across the competition continuum, soldiers, leaders, and organizations must master the use of PAI in each of the Army's strategic roles: competition below armed conflict, prevail in large-scale ground combat, and consolidate gains.

### Cross-Domain Solutions

**Problem Statement:** The Army lacks an effective, timely, and collaborative means to collect, process, analyze, and share information across domains and disparate classification systems.

**Why this is important:** The Army requires the ability to merge data across classification domains and standardize data structures, which will enable information related data to be able to better sense and understand information advantage activities.

# Table of Contents

## PROBLEM STATEMENTS

### Army Capabilities Manager Networks & Services

C4ISR/EW Modular Open Suite of Standards (CMOSS) Compliant Capability

**High Performance Edge Computing for AI/ML in a DIL and Contested Environment**

Joe Howard, Army Account Manager, Hewlett Packard Enterprise ..... 12

Non-Traditional Waveforms for Information Advantage (IA)

Near Term Emerging Radio Technologies

### Army Capabilities Manager Cyber

Network Modernization

**TAKcyber Solution**

Jeff Palumbo, Chief Engineer, Booz Allen Hamilton..... 14

**Network Modernization Through Holistic Integration**

Gus Anderson, Senior Director, Business Development, Leonardo DRS ..... 16

### Cyber Battle Lab (CBL)

Human Behavior Modeling in Support of Information Advantage Effects Adjudication

**Leveraging Liminal Space Technologies to Accurately Model Human Behavior**

Sean Guillory, Associate, Ph.D., Booz Allen Hamilton

Deborah Karagosian, Senior Associate, Booz Allen Hamilton ..... 19

Identify Capabilities that Can Support Army Military Information Support Operations Using Radio Frequency Delivery Methods



## Army Capabilities Manager Electronic Warfare

### Cross-Domain Solutions for Army Tactical Networks

#### **Accelerate The CPCE To The Hybrid Cloud With Zero Trust Identity And Attribute Access**

Andrew Whelchel, Senior Solutions Engineer, Saviynt ..... 22

#### **Behavior Based Zero Trust Migration for Remote Access**

Jack DeGannaro, Account Executive, U.S. Army, Forcepoint Global Governments and Critical Infrastructure, Forcepoint ..... 24

#### **Cross-Domain Solution**

Timothy Goben, U.S. Army Account Manager, BAE System ..... 25

#### **Cross-Domain Solutions for Army Tactical Networks**

Steve Wagner, Vice President, Enlighten IT Consulting, LLC ..... 26

### Automated Signal Recognition and Technique Generation

#### **R.AI.DIO®: An AI Enabled ELINT Solution**

Alex Saunders, Lead Engineer, Booz Allen Hamilton ..... 29

## Army Program Office-Information Advantage (APO-IA)

### Managing Information Related Data

#### **Data Fabric Architecture for Global Information Access and Sharing**

Joe Howard, Account Manager, Hewlett Packard Enterprise ..... 31

#### **Managing Information Related Data**

Steve Wagner, Vice President, Enlighten IT Consulting, LLC ..... 32

#### **Open Data Environment (ODEN) and JADC2 Development, Adoption, and Operations**

Vish Patel, Principal/Director, Booz Allen Hamilton..... 34

### Publicly Available Information (PAI)

#### **AI-Based PAI Collection and Exploitation for Information Operations at Scale**

Nanda Ramanujam, Managing Director, AI Ops, Alion Science and Technology ..... 37

### Cross-Domain Solutions

#### **Cross-Domain Solutions**

Steve Wagner, Vice President, Enlighten IT Consulting, LLC ..... 39

#### **Integrated Cross-Domain Solutions**

Timothy Goben, BAE Systems Integrated Cross Domain Solutions, BAE Systems ..... 41

**C4ISR/EW MODULAR  
OPEN SUITE OF  
STANDARDS  
(CMOSS) COMPLIANT  
CAPABILITY**

# High Performance Edge Computing for AI/ML in a DIL and Contested Environment

**Joe Howard, Army Account Manager, Hewlett Packard Enterprise •**

joe.howard@hpe.com

## ABSTRACT

When the Army assesses deployed computing and communications capabilities, size, weight and power (SWaP) have always been the three measures used to constrain deployable equipment sets. This is one of the drivers for CMOSS.

Information advantage (or dominance) will increasingly rely on artificial intelligence and machine learning (AI/ML) and other compute intensive processes as combat force multipliers at the tactical edge. A typical application is sensor ingest at the tactical edge, applying machine learning and analytics at the edge to rapidly assess sensor input (i.e. images) to dramatically speed up the sensor-to-shooter kill chain, which is currently still heavily reliant on slow and often inaccurate human visual assessment.

This capability needs to be forward deployed because of the DIL nature of tactical networks, where sending large volumes of data to a central cloud for processing is not reliable or practical. This presentation will review hardware advancements for CMOSS interoperable high-performance computing at the tactical edge and the application stacks to provide edge AI/ML, analytics, C5ISR, and other critical capabilities.

**BIO:** Bill Burnham is the chief technology officer for Hewlett Packard Enterprise's U.S. Public Sector Business Unit. Burnham joined HPE in 2018 after seven years of federal service as the chief technology officer for the United States Special Operations Command and before that as a career Army Signals officer.

# **NETWORK MODERNIZATION**

# TAKcyber Solution

**Jeff Palumbo, Chief Engineer, Booz Allen Hamilton • Palumbo\_jeff@bah.com**

## ABSTRACT

The rapid adoption of commercial smartphone and networking technologies has provided a tremendous enablement for our troops. Core to much of the Army's use of smartphones is the Tactical Assault Kit (TAK) ecosystem. This suite of applications has emerged as the tool of choice for tactical users. TAK is a government-owned, extensible platform that provides soldiers on the ground situational awareness and mission enabling tools in a smartphone application, with data federation between networks and across echelons using a server component.

While the adoption of commercial networks and technology serves as a force multiplier, it also opens the threat surface for cyber-attacks, and near-peer adversaries are taking full advantage of this. They have already executed tactics that leverage hacked smartphones to gain intel, interfere, and geolocate soldier-level communications. These tactics were seen in Ukraine, where Russian hackers compromised and targeted with great effect the smartphones of key Ukrainian artillery units, and more recently in Armenia, where Azerbaijani and Turkish forces conducted extensive cyber operations that included targeting military and government personnel through the applications on their smart phones.

Of specific concern was the discovery of stalkerware on the Android phones of several individuals who accessed their social media accounts from the same device used to access their official email. Core to these concerns is the lack of host and network monitoring at the tactical edge. Combat soldiers and Signal/NetOps staff do not have a single pane of glass to monitor the communications and cyber-security status of their hosts and network transports, nor do they have a UI that provides alerts and prompts on network intrusion attempts the moment they are detected.

Booz Allen has extended TAK to address cyberspace, creating TAKcyber to enable simplified cyber operations. TAKcyber provides Android TAK (ATAK) and TAK server capabilities that monitor and report the cyber security status of units' systems. It provides ATAK users with alerts of issues with their host and network (e.g. detected jamming) and sends status updates to connected TAK servers for the S6 to analyze and maintain situational awareness. TAKcyber hardens TAK servers through host and network intrusion detection coupled with machine learning to detect, alert, and block attacks using easily updateable baselines and firewall rules.

With TAKcyber, the S6 can now see a breakdown of individual smartphones, if the phones have non-compliant software installed, and the status of connected communications. The S6 also can view historical and real-time metrics of cyber-attacks and signal events. TAKcyber provides a map-view that plots when and where communications were hindered or jammed and when cyber events occurred. It leverages the existing TAK server data federation to populate this data with peer and superior commands. Finally, as troops operate in multi-domain battlespaces, TAKcyber incorporates a means of dynamically and persistently tracking known Wi-Fi APs in an area for situational awareness, as well as a means of triangulating a targeted MAC address location using only TAKcyber's smartphone software. TAKcyber: Providing soldiers and S6/NetOps staff with the monitoring and protection they need against cyber-attacks in the new tactical internet.

**BIO:** Jeff Palumbo has been supporting the Army C5ISR community for almost 20 years in various roles and capacities focused around advanced network protocols, military tactical radios, network architectures, and system integration. He has worked with and within various R&D organizations, PEO C3T, PEO IEWS and Rapid Capability Office, integrating and expanding the capabilities of tactical networks, maneuver command and control, force protection, electronic warfare, and cyber operations. He has an engineering master's degree in networked information systems.



# Network Modernization Through Holistic Integration

**Gus Anderson, Senior Director, Business Development, Leonardo DRS •**

ganderson@drs.com

## ABSTRACT

Leonardo DRS is a leading innovator in communications, aerospace, defense, and security. We provide mission-critical solutions to complex communications requirements, which include and are not limited to multi-domain information systems, cybersecurity operations, telecommunications infrastructure, reliable backhaul terrestrial networks, and cutting-edge global satellite networks. Delivering mission-critical communications across the globe requires a proven partner capable of securing data and ensuring resiliency with a robust, no-fail information and communication technology (ICT) ecosystem. Our commitment as a leading ICT integrator is to provide our customers with best value solutions that leverage three fundamental advantages: speed, scalability, and innovation.

The ICT Ecosystem is our core offering that provides fully integrated, turn-key IT and global communication solutions tailored to our customers current and future requirements so they can focus on their mission. Leonardo DRS engineers, manages, and supports the entire ICT Ecosystem to deliver reliable, resilient, and secure solutions, including: fixed solutions; enterprise comms; command and control; warfighter/MWR comms; intelligence networks; telemedicine; distance learning mobility solutions; comms-on-the-move; comms-on-the-pause; land combat support comms; manpacks; naval comms; AISR.

By using a holistic and vendor-agnostic approach to integrating the DRS ICT Ecosystem, Leonardo DRS offers its customers a fundamental advantage of a trusted RMF accredited infrastructure to ensure mission success and the safety of our warfighters data. The Leonardo DRS ICT Ecosystem is built upon three main segments: the space segment, the ground segment, and the network management segment.

The space segment includes resilient global SATCOM coverage using LEO, MEO, and GEO satellite services. The ground segment includes geographically diverse teleports, a highly available MPLS terrestrial network with self-healing circuits, and a diverse range of user terminals and connections. The network management segment is comprised of a network operations layer that includes the Leonardo DRS Global Network Operations and Security Center (GNOSC), a continuity of operations (COOP) site, an information technology layer that provides managed network services, comprehensive enterprise IT support, and a cyber services layer that spans all ICT segments providing the protection required by government and military customers so they can perform their missions confidently with strong security built into their networks.

Another key feature offered by DRS is a customer portal. The Leonardo DRS Ecosystem Customer Portal is a web-based NetOps tool that provides a consolidated and transparent view into network performance, utilization, and situational awareness within a managed end-to-end ICT Ecosystem. The customer portal places precise analytics and actionable data in the hands of key decision-makers through the near real-time

monitoring and reporting capabilities of hybrid, complex networks consisting of disparate systems, siloed software, and various types of equipment.

The three segments of the Leonardo DRS ICT Ecosystem create a modular map to effectively advance network modernization for both integrated enterprise networks and deployed tactical networks. Leonardo DRS provides integrated end-to-end global networks that are secured to DOD standards and maximizes network optimization and reliability using state-of-the-art equipment, expert engineering, and industry best practices. Leonardo DRS offers true best value solutions with our holistic and vendor agnostic approach to integrating bandwidth, equipment, and backhaul services.

**BIO:** Gus Anderson served in the U.S. Army for 29 years as a telecommunications corps officer. During that period, he commanded numerous tactical and strategic communications organizations, to include the 509th Signal Battalion, Vicenza, Italy, and the Regional Signal Group SHAPE, NATO HQ (Belgium). During his military career he also served as an associate professor of philosophy at the U.S. Military Academy and as the military speechwriter for two Secretaries of Defense. He retired as a colonel in 2008. Currently Anderson leads DRS' Global Enterprise Solutions (GES) business development organization. Anderson has been with DRS for 10 years. His initial assignments were as a program manager, overseeing satellite networks supporting NATO forces in the Balkans; Coalition forces in Iraq and Afghanistan; and networks supporting other U.S. federal and international agencies. In the past several years, his efforts have turned to business development, helping grow customer and market understanding of DRS' Information and Communications Technology Ecosystem – a global network that provides secure managed satellite and terrestrial services to major DOD, U.S. federal, and international agencies.

**HUMAN BEHAVIOR MODELING  
IN SUPPORT OF INFORMATION  
ADVANTAGE EFFECTS  
ADJUDICATION**

# Leveraging Liminal Space Technologies to Accurately Model Human Behavior

**Sean Guillory, Associate, Ph.D., Booz Allen Hamilton** • Guillory\_sean@bah.com

**Deborah Karagosian, Senior Associate, Booz Allen Hamilton** •

Karagosian\_Deborah@bah.com

## ABSTRACT

“It is in the cognitive space where we must prevail.” Gen Richard A. Clarke, former commanding general of SOCOM USSOCOM defines a hyper-enabled operator as a “professional empowered by technologies that enhance the operator’s cognition at the edge by increasing situational awareness, reducing cognitive load, and accelerating decision making.” In short, this is the promise of JADC2: to empower all our warfighters and to enable cognitive overmatch.

Achieving cognitive overmatch on the battlefield is not solely dependent on getting our warfighters the right data at the right time. We also need to reduce their cognitive load, ensure we do not overwhelm their senses, and account for biomedical responses to stressors in the algorithms designed to reduce such load and streamline decision making.

The liminal space is the sensory threshold where a warfighter’s senses are completely engaged in the task at hand. It is the fine line between the experienced fighter, confidently executing life-saving decisions and the overwhelmed leader, frozen in place, struggling to parse the environment. Even for seasoned professionals, data shows that the ability to see, hear, perform fine motor skills and to make decisions are all negatively affected at moments of over-heightened sensory stimulation and cognitive overload. Finding the sweet spot of having the right information at the right time to make the right decision quickly—faster than our enemy—is key to realizing the potential of JADC2 for the brigade and below tactical fight.

While the video game industry has done a phenomenal job in creating environments to immerse gamers, we must glean the right lessons in developing our training and future operational environment. For example, the use of eye tracking for assessing how quickly novice gamers can transition from learning basics to higher level skills is relevant to efficiently training our warfighters. In contrast, applied mathematicians and computer scientists often harness human behavior models that assume “perfectly rational” human beings make the most Pareto-optimal decisions. Therefore, we posit that the gaming industry falls short of simulating the multi-domain environment our warfighters really face.

Lessons learned from our warfighters tell us that completely digital environments fall short of simulating and optimizing the liminal space soldiers experience. In short, it is critical that empirical human behavior data be collected at the intersection of the physical, cyber, and informational domains. Booz Allen Hamilton’s Extended Reality Analytics Engine (XRAE) captures human performance data in this space. XRAE leverages VR/AR devices, biometric sensors (eye-tracking, EEG brain activity), and physical hardware interactions.

These data sources drive the iteration and training of algorithms that are ultimately deployed at the point of need, reducing warfighter liminal load. XRAE comes with data security (and expertise) across all stages of development, from collection and curation to testing and deployment. Its framework sets a trajectory to model human behavior at the tactical/avatar level through the continuum of military competition. We welcome a discussion as we leverage lessons learned from the gaming industry, medical community, and the DOD to optimize the liminal space and achieve cognitive overmatch.

**BIO:** Sean Guillory attained his Ph.D. in cognitive neuroscience from Dartmouth College where he primarily worked with neurosurgery patients to help improve the mapping for brain functions that were personally important to their lives. After taking that experience to help build up a start-up business incubator aimed at helping humanity (Fruition Tech Labs) and working on data science efforts to help catch online scammers (ConsumerAffairs), he focused on ways of utilizing his background to help with issues within defense and national security. At Booz Allen Hamilton, he works with the firm's various cognitive domain efforts utilizing automation, biometrics, and social science methodology to help solve our customers' concerns.

Deborah Karagosian is a graduate of the U.S. Military Academy and the School of Advanced Military Studies (SAMS) and attained master's degrees in computer systems, strategic management, and military theater operations. She's led multi-functional teams to solve the most complex problems in the cyberspace domain and served as the lead author of several CONOPs. As the founder of DKI Solutions, she brought together a mission-focused team supporting multiple government and industry organizations and served as a government-recognized expert on Russian and Chinese cyber and influence operations. At Booz Allen Hamilton, she continues to serve, guiding highly technical teams to identify and solve wicked problems arising from this new era of Great Power Competition.

**CROSS-DOMAIN  
SOLUTIONS FOR ARMY  
TACTICAL NETWORKS**

# Accelerate The CPCE To The Hybrid Cloud With Zero Trust Identity And Attribute Access

**Andrew Whelchel, Senior Solutions Engineer, Saviynt •**

andrew.whelchel@saviynt.com

## ABSTRACT

In the contested peer environment, speed, mobility and cyber assurance are more important than ever. Specifically, these elements will be the sustaining force to enable a compute environment to execute its mission for operational success. Command Post Computing Environment (CPCE), as a new operational computing environment, provides a substantial data plane and pipeline for leverage in information warfare.

The solution presented here describes the challenge and identifies solution approach to solve with secure identity and attribute-based access approach to meet the mission potential of the CPCE. To tap into and use this force multiplier, the CPCE needs an identity security control plane to unlock the opportunity to fully tap the mobility and speed by de-risking the cyber impact and accelerating delivery of new capabilities in the CPCE. The operational challenge is to provide a security control plane that both de-risks cyber impact for more rapid capability delivery as well as provides a means to abstract meaningful data to CPCE security domains (S//REL and SBU).

A hybrid cloud approach presents an option to de-risk intersystem data in the CPCE through using an identity authorization process and using data entitlements for zero-trust least privilege. As data is abstracted between systems of the CPCE for use in the S//REL and SBU purposes, the security controls (particularly for identity) need a capability to provide data agility and security. To address these challenges, the solution described here provides three elements including:

- Initiate zero trust approach for access by leveraging governance requests and risk reviews for data attributes (ABAC attributes) used for authorization to abstracted data. Saviynt would be an example solution component for this.
- Deploy a hybrid cloud-based API processing function that can, at the time of request, from the API flow leverage the data through data security controls (confidentiality, integrity, and availability) to present data to S//REL and SBU environment for warfighter operator use. Microsoft Azure API Gateway and Azure Functions would be examples of this component.
- Provide data presentation capability that can collect and present the data in S//REL and SBU that is data endpoint of an API function and at the same time maintains identity chain of access metadata needed for cyber assurance of the mission operations of the CPCE. Microsoft Azure Power BI is an example component for this capability.



In the solution example provided here, the solution would leverage all existing CPCE infrastructure and then further extend this through a hybrid cloud approach. As a reference architecture example, the flow will operate in a sequence to initially allow authorization through identity, secure the data through the cloud functions, and then present to the operator the data needed for the mission. The solution presented is optimal as it would further leverage the CPCE available today and additionally at the same time enable the S//REL and SBU access needed for the operational success of the CPCE support mission.

**BIO:** Andrew Whelchel (CISSP-ISSAP, ISSEP, CAP, CCSP) started in information security and IAM after graduation from the University of Memphis. He started in management of Microsoft Identity for U.S. federal customers and later transitioned to infrastructure security and anti-fraud and most currently to public sector identity protection. The recent prior role, at Okta, focus was on authentication and authorization for protecting employee/partner for agencies as well as citizen consumer identities. At the current role at Saviynt, the focus is on leveraging identity governance and cloud privileged access to reduce cyber risk and accelerate capabilities for cloud transformation. Contributions include work as a contributor on the NIST 1800-3 ABAC (Attribute Based Access Control) standard and speaking events on identity access management and security.

# Behavior Based Zero Trust Migration for Remote Access

**Jack DeGannaro, Account Executive, U.S. Army, Forcepoint Global Governments and Critical Infrastructure, Forcepoint •**

jegennaro@forcepointgov.com

## ABSTRACT

Behavior based ZT migration is a novel approach that provides risk based, real-time protection across all security classifications for tactical and strategic deployments. Today's government agency and military workforce requires anywhere, anytime access to mission critical information in order to ensure continuity of operations.

Secure remote access is available to highly sensitive data on multiple domains including classified networks, where it is protected from compromise or loss. This approach leverages efficient virtual access for remote workers while offering controls that are localized and uninterrupted. Accredited, tested, and proven in the field.

**BIO:** Jack DeGannaro is a senior cyber engineer at Forcepoint Global Governments and Critical Infrastructure. After attending Clemson University, DeGannaro began a career in law enforcement with the city of Clemson Police Department. Over the next 15 years, he was detailed with a variety of assignments, which included working undercover for seven years. During that time, DeGannaro worked within the leadership for six years, including management of the department's IT network, criminal investigations, jail operations, and police records management. DeGannaro also worked for a computer mapping firm to provide automated vehicle location services for public safety. In 2008, he joined Visual Analytics and was assigned to the architecture, deployment, and management of the company's data sharing and crime analysis tools at 14 crime analysis centers within New York state. Upon Raytheon Cyber Products' acquisition of Visual Analytics and the subsequent joint venture to become Forcepoint, DeGannaro currently serves as a cyber solutions account executive, supporting Army and other U.S. Department of Defense accounts.

# Cross-Domain Solution

**Timothy Goben, U.S. Army Account Manager, BAE Systems •**

[tim.goben@baesystems.com](mailto:tim.goben@baesystems.com)

## ABSTRACT

In today's enterprise environments, secure data sharing and collaboration across networks of multiple classification levels is essential. Data integrity becomes increasingly complex as threats evolve and security requirements become more stringent. Both BAE Systems' XTS Guard 7 (XTSG7) and XTS-Diode (XTSD) are NSA raise the bar (RTB) compliant and a National Cross Domain Services Management Office (NCDSMO) listed cross-domain solution.

The XTS Guard 7 is certified for multi-directional automated data transfers between networks, domains, and electronic assets while the XTS-Diode enables a uni-directional transfer of data and serves as a HW enforced protocol break. A single solution supports multiple data protocols (UDP/TCP, SFTP, SMTP, XML, Office, etc.) with a variety of content inspection filters to alleviate the challenges faced by customers. As described by the Cross-Domain Solutions For Army Tactical Networks problem statement, 2021 TechNet Augusta, there is an increasing need for data to be transferred outside of (S//NF) and (S//REL) for EWPMPT and CP CE at the brigade level.

BAE Systems is the only vendor to offer a diode solution that transfers data up to 10Gb/s across domains and can be paired with our XTS-Guard 7 to disseminate and filter data as it moves across the security boundaries. As a basic design principal of RTB, use of the BAE Systems XTS-Diode alone to move said data across boundaries for actions may be a reasonable solution. The U.S. Army currently deploys 10Gb/s diodes in architectures on ranges for movement of data. BAE Systems is more than willing to test said solution to produce metrics that may meet U.S. Army requirements.

XTS Guard 7 runs on STOP 8, the general-purpose operating system with security as its core focus, developed by BAE Systems. STOP 8 ensures the diversity of Guard deployment within a multi-guard cross-domain solution, specified in RTB design patterns. The XTSG retains its own security policy for process separation, domain separation, and one-way data transfer. A mandatory role-based access control (RBAC) model uses security roles to designate permission levels, and a Bell-LaPadula/Biba (BL/B) model provides a classification element that specifies where a given process or data set can and cannot exist.

The combined RBAC and BL/B assignation is referred to as a security label. With XTS Guard, the number of security domains that can be interconnected is limited only by hardware. XTS Guard Enterprise version offered today can handle up to 20 security enclaves on either 1U - 2U hardware, and it is approved for both SABI and TSABI data transfer operations. In contrast, alternative solutions support far less domains or charge a significant fee to add domains. This hardware architecture presents the possibility of consolidating many different enterprise devices into just one enterprise guard system for large financial savings.

Lastly, BAE Systems provides a small form factor ruggedized solution as well that can handle up to 10 domains in a single 2x4x6 chassis for field deployments and holds an R5 GMS ruggedization level. Please feel free to reach out to schedule a whiteboard meeting to discuss your program's requirements. 703.689.1465, [tim.goben@baesystems.com](mailto:tim.goben@baesystems.com)

# Cross-Domain Solutions for Army Tactical Networks

**Steve Wagner, Vice President, Enlighten IT Consulting, LLC •**

swagner@eitccorp.com

## ABSTRACT

Enlighten proposes utilizing the government-owned big data platform (BDP) as the unifying data operating system to collect and share information across disparate classification systems. The BDP is an accredited GOTS capability that is currently operating in production on NIPR, SIPR, and JWICS and storing and analyzing over 37-petabytes (PBs) of all domain data across the DOD. The BDP has been adopted by the joint community as the centerpiece of the unified platform, which enables the aggregation, correlation, and analysis of information across the services, leveraging data from Army, Air Force, Marines, USCYBERCOM, Navy, Coast Guard, DISA, and others.

The proposed use of the BDP to enhance the Army's ability to share information across disparate classification systems within the electromagnetic warfare systems would be enhanced by connecting to the established unified platform. The BDP capability leverages WOLFDOOR, the integrated, accredited bi-directional cross domain service at USCYBERCOM to provide real-time decision-making across disparate classification systems.

Today, Army users utilize this cross-domain service to search up classification levels on both secret and top secret BDP instantiations to view FOUO or CUI data from their unclassified account. Similarly, top secret users can search down on both the secret and unclassified BDP instantiations to view and transport data to the high side. This capability is possible due to the decision by all service leadership to leverage the same unified data operating system baseline and results in the requirement to only store operational data on one classification system versus the historic cost prohibitive approach of duplicating storage of the data on multiple classification fabrics.

User's access to data is managed using attribute-based access control (ABAC), which provides more granular controls compared than other types controls (RBAC) and provides additional security, allowing DOD customers to externalize the authorization logic to a central policy decision point and express the authorization logic as policies instead of roles. This would allow Army EW users conducting planning on the EWPMT to reach down and query S//REL and SBU data on brigade and below CPCEs and pull up results to do additional work on the S//NF classification domain. Similarly, brigade and below units could query any S//REL and SBU data that may be available in the EWPMT and transport results down to do additional work within the CPCE.

Beyond the Army's BDP cloud environments, smaller on-premise instances of the BDP, known as lower echelon analytic platforms (LEAPs), could also be utilized to enable data ingest, processing, storage, analysis and forwarding capabilities at key brigade and below locations where CPCE is used.

LEAP can enable brigade and below units to have the same BDP functionality that is present on the Army's enterprise BDP Gabriel Nimbus cloud instantiation. This also allows for the utilization of the same enterprise BDP accreditation for the forward-located LEAPs to reduce overhead and increase operational efficiencies. This data agnostic capability is already collecting PBs of data. Integrating electromagnetic warfare data would be an important step forward in operationalizing this data to increase the speed of decision making.

Joint All Domain Operations require large scale data aggregation and integration across hundreds of data sources and data types to provide an increase in confidence and speed in decision making. The government-owned BDP is already being leveraged today in operations to collect billions of events/day from global network sensors and is processing, analyzing, and sharing this information across the services to provide real time insight into locations, availability, vulnerabilities, and readiness of global mission critical infrastructure.

The Army should use BDP in combination with key located LEAPs to aggregate additional electromagnetic warfare data sets and utilize a proven CDS that has been accredited and is in operation on the NIPRNet, SIPRNet, and JWICS networks with bi-directional data transfers across, up, and down to effectively share information across domains and disparate classification systems.

# **AUTOMATED SIGNAL RECOGNITION AND TECHNIQUE GENERATION**

# R.AI.DIO®: An AI Enabled ELINT Solution

**Alex Saunders, Lead Engineer, Booz Allen Hamilton • saunder\_alex@bah.com**

## ABSTRACT

The electromagnetic spectrum between 1kHz - 40 GHz creates a large volume of data that is difficult to process effectively. In addition, much of the data from the monitored spectrum contains useless information to units on the ground. Thus, presenting a significant challenge to electronic intelligence (ELINT) platforms. Furthermore, training datasets for ELINT signals that ML algorithms can use are hard to come by. These datasets are vital to demonstrating the advantages of edge processors. In addition, algorithms require accurately labeled and varied data to operate correctly in a real-world environment. Therefore, machine learning (ML) algorithms need to operate as close to the collection platform as possible.

This paper will discuss the difficulties of monitoring and identifying signals in a wide electromagnetic spectrum and how these challenges can be mitigated using machine learning techniques. The answer, R.AI.DIO®, is a system that can monitor a broad spectrum and automatically identify a bandwidth of interest.

R.AI.DIO® uses ML algorithms combined with an electronic warfare planning and management tool (EWPMT) that provides a fast, mobile, wideband spectrum monitoring system and highlights information for Army electronic warfare operators.

- R.AI.DIO® is a machine learning development toolset that uses data generation and simulation to quickly train algorithms for a large variety of signals in various environments.
- R.AI.DIO® networks are adaptable and trained to output various electronic intelligence notation (ELNOT) data.
- While monitoring a large amount of spectrum, a key function of R.AI.DIO® networks is to determine the relevance of a given spectrum and direct attention to areas of interest.
- R.AI.DIO® reduces the amount of data that needs to be analyzed from the whole spectrum to a few key points. R.AI.DIO® networks can take the data collected by the various systems connected through the EWPMT, process the data, and direct attention to relevant points of interest, drastically reducing the total amount of data that needs to be analyzed.

Booz Allen's R.AI.DIO® technology, combined with an EWPMT system, can provide a much-needed tool in addressing how large bandwidth spectrums are monitored.

**BIO:** Alex Saunders acquired his master of science degree in electrical engineering from California 's Polytechnic State University in San Luis Obispo. During his early career and university years, Alex worked on developing experimental nano-satellites for atmospheric monitoring and low Earth orbit signal propagation experiments. Since joining Booz Allen Hamilton, Alex works on developing and delivering technological solutions as a signals and machine learning engineer.



# **MANAGING INFORMATION RELATED DATA**

# Data Fabric Architecture for Global Information Access and Sharing

**Joe Howard, Account Manager, Hewlett Packard Enterprise •**

joe.howard@hpe.com

## ABSTRACT

Data is the new ammunition, the critical ingredient of new insights and rapid decision making that is needed to gain advantages in next generation conflicts. While the DOD has vast amounts of data, accessing and harnessing that data has proved to be difficult because of the highly distributed and diverse nature of data stores.

To overcome the constraints of current data realities and to enable large scale data analytics and AI/ML without the need to centrally locate all data (i.e. in a single cloud), a data abstraction file system layer known as a data fabric is needed. A true data fabric is hardware, geo location, and file system agnostic, providing a platform for secure and reliable access to share legacy data stores in a scalable fashion. The data fabric represents a software infrastructure to implement, administer, manage and operate data operations across the entire span of the data within the enterprise across all data activities including data acquisition, transformation, storage, distribution, integration, replication, availability, security, protection, disaster recovery, presentation, analytics, preservation, retention, backup, retrieval, archival, recall, deletion, monitoring, capacity planning across all data storage platforms enabling use by applications to meet the data needs of the DOD.

- Mesh enabling the movement of data around the enterprise
- Provides access to all data assets
- Supports the flow, processing, distribution, management, and exchange of data throughout the enterprise
- Provides coherent data framework for use by custom and acquired applications
- Is independent of specific applications
- Is independent of specific data platforms

**BIO:** Bill Burnham is the chief technology officer for Hewlett Packard Enterprise's U.S. Public Sector Business Unit. Burnham joined HPE in 2018 after seven years of federal service as the chief technology officer for the United States Special Operations Command and before that as a career Army Signals officer.

# Managing Information Related Data

**Steve Wagner, Vice President, Enlighten IT Consulting, LLC •**

swagner@eitccorp.com

## ABSTRACT

Enlighten proposes utilizing the government-owned big data platform (BDP) as the unifying data operating system to collect, process, analyze and share information across domains and disparate classification systems. The BDP is an accredited GOTS capability that is currently operating in production on NIPR, SIPR, and JWICS and is storing and analyzing over 37-petabytes (PBs) of all domain data across the DOD.

The BDP has been adopted by the joint community as the centerpiece of the unified platform, which enables the aggregation, correlation, and analysis of information across the services, leveraging data from Army, Air Force, Marines, USCYBERCOM, Navy, Coast Guard, DISA, and others. The proposed use of the BDP to enhance the Army's ability to aggregate, store, and secure information related data across disparate platforms and sensors to provide a common operating picture of the information dimension in the operating environment would be enhanced by connecting to the established unified platform to incorporate data from all domains and services.

The BDP capability leverages WOLFDOOR, the integrated, accredited bi-directional cross domain service at USCYBERCOM to provide real-time decision-making across disparate classification systems. Today, Army users can utilize this cross-domain service to search up classification levels on both secret and top secret BDP instantiations to view FOUO or CUI data from their unclassified account. Similarly, top secret users can search down on both the secret and unclassified BDP instantiations to view and transport data to the high side. This capability is possible due to the decision by all the service leadership to leverage the same unified data operating system baseline and results in the requirement to only store operational data on one classification system versus the historic cost prohibitive approach of duplicating storage of data on multiple classification fabrics.

Combining disparate data sets and sensors from the internet of things (IoT) in theater networks and assets with information like logistics, man power, task critical assets, mission systems, and force location will enable all domain visibility and a common operating picture of the information dimension in the operating environment. Among the suite of out of the box capabilities, the BDP comes with the ELK 7, enabling on the fly correlation, visualization, and analysis of theater data for operational support.

Through integration with the larger BDP community, the Army will be able to utilize a production bi-directional cross-domain service (CDS) to enable cross-domain querying and correlation of data sets. Data collected on NIPR can quickly be queried from SIPR, with just the analytic results moving to the higher network for correlation and attribution with data collected on SIPR. The bi-directional cross domain is fully accredited and managed by USCYBERCOM.

Out of the box capabilities like the Cyber Awareness Dashboard (CAD), the Realtime Executive Dashboard for Mission Assurance and Provenance (REDMAP), and the Common Operating Picture (COP) will turn this data into actionable information, presenting assets, vulnerabilities, and real time alerting.

Joint All Domain Operations require large-scale data aggregation and integration across hundreds of data sources and data types to increase confidence and speed in decision making. The government-owned BDP is already being leveraged today in operations to collect billions of events/day from global network sensors and is processing, analyzing, and sharing this information across the services to provide real time insight into locations, availability, vulnerabilities, and readiness of global mission critical infrastructure.

The Army should use BDP to aggregate additional Army data sets to effectively share information across domains and disparate classification systems.

# Open Data Environment (ODEN) and JADC2 Development, Adoption, and Operations

**Vish Patel, Principal/Director, Booz Allen Hamilton • patel\_vish@bah.com**

## ABSTRACT

Our solution open data environment (ODEN) comprised of common data fabric, DevSecOps pipeline, and MLOps platform, can provide a JADC2 solution that paces the threat, correlates data sources and sensors, and expands commanders' options across kinetic, non-kinetic, and informational domains at the speed of battle. Today's battlespace not only exists across ground, air, and space, but also in the electromagnetic spectrum where communications are contended for; in commercial infrastructure that civilians and soldiers live and operate in; and in cyberspace where these domains fill their data lakes with intelligence and noise.

Dominating opponents in this construct is like playing a multi-dimensional game of chess. Observations in the physical domain must be correlated to spectrum emissions and cyberspace activity to understand the game being played. There are many challenges that hinder one's ability to play in this multi-domain battlespace. One of those is the availability of relevant information. On one side, there is so much data on enterprise networks that finding relevant data is the primary challenge. On the flip side, accessing data or sensors feeds at the edge is a challenge given the dynamic and fragile nature of the tactical communications architecture.

We posit that the way to address these challenges is by using a common data fabric that can span from the enterprise to the furthest tactical transport. ODEN is a common data fabric that provides an infrastructure to enable data discovery, data security, and data synchronization. Beyond addressing data access challenges, taking advantage of real-time observations requires a means to deploy new software and algorithms. Integrating common data fabric with the DevSecOps pipeline provides the secure means to manage deployed platforms with algorithms to detect RF signals, increase non-kinetic electronic warfare effectivity, or update malware signatures to defend our cyber infrastructure.

Furthermore, leveraging ML capabilities effectively does not mean putting pre-trained models into the field. They need to be constantly monitored and updated in a MLOps platform that will allow their potential to be realized in the multi-domain battlespace.

We are prepared to demonstrate how the common data fabric, DevSecOps pipeline, and MLOps platform must be tightly integrated with the right people, processes, and technologies to achieve JADC2 objectives and provide commanders' data to make rapid decisions in order to fight and win decisively against any adversary in a joint, multi-domain, high-intensity conflict.

**BIO:** Vish Patel has more than two decades of experience developing commercial digital transformation solutions using big data platforms, DevSecOps and advanced analytics. As a principal/director at Booz Allen Hamilton, he is responsible for driving the digital solutions and open system architectures, which are key components of the Army's transformation. He is focused on leading data and digital software solutions aligned with multi-domain operations, which are being driven by the Army Futures Command to modernize the digital battlefield.

**PUBLICLY AVAILABLE  
INFORMATION (PAI)**



# AI-Based PAI Collection and Exploitation for Information Operations at Scale

**Nanda Ramanujam, Managing Director, AI Ops, Alion Science and Technology •**

nanda.ramanujam@alionscience.com

## ABSTRACT

Alion has developed a novel solution to exploit publicly available information (PAI) for open source intelligence (OSINT) applications. The DOD and IC clearly recognize the value of complementing traditional intelligence with information from a rich and vast volume of global PAI to provide near real time (NRT) situational awareness (SA) for information operations. Collecting and exploiting PAI to close information gaps as they appear requires not only access to a comprehensive array of media sources but also new tools and technology, such as artificial intelligence based natural language processing (AI NLP) and machine learning (ML), to effectively process this data at scale. Alion FortisAI is a platform and processing capability to extract OSINT from petabyte-scale dataflows of PAI. FortisAI hierarchically combines state-of-the-art deep-learning-based natural language processing with machine-learning, to ingest petabyte-scale text from a wide range of media feeds and distills them into enriched megabytes of media content for near-real-time analyst investigation, making FortisAI a force multiplier.

Queries in natural language phrases return precise, nuanced narratives of interest. Text spans diverse media/data types (social-media, newsprint, blogs, TV/radio-transcripts, cyber) in multiple languages and linguistic structures (formal, informal, mixed language). Some notable features of the FortisAI solution are: a network of PAI data vendors and aggregators to comprehensively source PAI data and native language search capability to mitigate translation-induced noise.

The FortisAI NLP engine currently supports several languages of interest to DOD and IC. More importantly, new languages can be readily supported within weeks, using our language model training pipeline. ML can then characterize content/actors with bot-detection, psychological profiling, and biometrics. Geo-inferencing provides temporal, geo-fenced activity views.

FortisAI enables 24x7/365 ground-layer activity sensing for: over-watch; force protection; OPSEC; influence operations. FortisAI is being delivered to U.S. Army Pacific Command (USARPAC) as Alion-managed Gov-Cloud-based turnkey service and is also being transitioned into Army Cyber Command for PAI collections in FY22. FortisAI is commercial-off-the-shelf (COTS) software based on an open architecture that allows effective integration of third-party COTS analytics as needed to enhance the common operating picture for information operations.

**BIO:** Nanda Ramanujam, Ph.D., MBA, is managing director of AI Operations in the CTO office at Alion. He oversees strategy, product, and business development of PAI OSINT solutions. Previously, Dr. Ramanujam was CTO/chief strategy officer at other defense technology companies including DRS Technologies (Leonardo). His career at public companies and venture-backed startups has spanned photonic telecommunications, medical devices, 5G, strategy consulting, and venture capital. Dr. Ramanujam has a track record of identifying and successfully transitioning innovative commercial technologies into the defense market. He has an S.B. in electrical engineering (MIT), M.S. and Ph.D. in optics (University of Arizona), post-doctoral fellowship (MIT Research Laboratory of Electronics), and an MBA in strategy and finance (The Wharton School).

# **CROSS-DOMAIN SOLUTIONS**

# Cross-Domain Solutions

**Steve Wagner, Vice President, Enlighten IT Consulting, LLC •**

swagner@eitccorp.com

## ABSTRACT

Enlighten proposes utilizing the government-owned big data platform (BDP) as the unifying data operating system to collect, process, analyze, and share information across domains and disparate classification systems. The BDP is an accredited GOTS capability that is currently operating in production on NIPR, SIPR, and JWICS and storing and analyzing over 37-petabytes (PBs) of all domain data across the DOD. The BDP has been adopted by the joint community as the centerpiece of the unified platform, which enables the aggregation, correlation, and analysis of information across the services, leveraging data from Army, Air Force, Marines, USCYBERCOM, Navy, Coast Guard, DISA, and others.

The proposed use of the BDP to enhance the Army's ability to share information across domains and disparate classification systems would be enhanced by connecting to the established unified platform to incorporate data from all domains and services. The BDP capability leverages WOLFDOOR, the integrated, accredited bi-directional cross domain service at USCYBERCOM to provide real-time decision-making across disparate classification systems.

Today, Army users can utilize this cross-domain service to search up classification levels on both secret and top secret BDP instantiations to view FOUO or CUI data from their unclassified account. Similarly, top secret users can search down on both the secret and unclassified BDP instantiations to view and transport data to the high side. This capability is possible due to the decision by all the service leadership to leverage the same unified data operating system baseline and results in the requirement to only store operational data on one classification system versus historic cost prohibitive approaches of storing the same data on multiple classification fabrics.

Beyond the Army's BDP cloud environments, smaller on-premise instances of the BDP, known as lower echelon analytic platforms (LEAPs), are also required to enable data ingest, processing, storage, analysis and forwarding capabilities at key operational locations that are currently unable to transport data back to the enterprise due to either contested or low bandwidth networks.

LEAP can enable mission forces at key forward locations to have the same BDP functionality that is present on the Army's enterprise BDP Gabriel Nimbus cloud instantiation. This also allows for the utilization of the same enterprise BDP accreditation for the forward-located LEAPs to reduce overhead and increase operational efficiencies. The BDP is positioned to be the Army's aggregation point for all domain data. This data agnostic capability is already collecting PBs of data. Integrating this information would be an important step forward in operationalizing this data to increase the speed of decision making.

Joint All Domain Operations require large scale data aggregation and integration across hundreds of data sources and data types to increase speed and confidence in decision making. The government-owned BDP is already being leveraged today in operations to collect billions of events/day from global network sensors and is processing, analyzing, and sharing this information across the services to provide real time insight into locations, availability, vulnerabilities, and readiness of global mission critical infrastructure. The Army should use BDP in combination with strategically located LEAPs to aggregate additional Army data sets to effectively share information across domains and disparate classification systems.

# Integrated Cross-Domain Solutions

**Timothy Goben, BAE Systems Integrated Cross Domain Solutions, BAE Systems**

• [tim.goben@baesystems.com](mailto:tim.goben@baesystems.com)

## ABSTRACT

In today's enterprise environments, secure data sharing and collaboration across networks of multiple classification levels is essential. Data integrity becomes increasingly complex as threats evolve and security requirements become more stringent. Both BAE Systems' XTS Guard 7 (XTSG7) and XTS-Diode (XTSD) are NSA raise the bar (RTB) compliant and a National Cross Domain Services Management Office (NCDSMO) listed cross-domain solution. The XTS Guard 7 is certified for multi-directional automated data transfers between networks, domains, and electronic assets while the XTS-Diode enables a uni-directional transfer of data and serves as a HW enforced protocol break.

A single solution supports multiple data protocols (UDP/TCP, SFTP, SMTP, XML, Office, etc.) with a variety of content inspection filters to alleviate the challenges faced by customers. As described by the Cross-Domain Solutions problem set from 2021 TechNet Augusta, there is an increasing need for data to be shared across disparate, classified domains. BAE Systems is the only vendor to offer a diode solution that transfers data up to 10Gb/s across domains and can be paired with our XTS-Guard 7 to disseminate and filter data as it moves across the security boundaries. As a basic design principal of RTB, use of the BAE Systems XTS-Diode alone to move said data across boundaries for actions may be a reasonable solution.

The U.S. Army currently deploys 10Gb/s diodes in architectures on ranges for movement of data. BAE Systems is more than willing to test said solution to produce metrics that may meet U.S. Army requirements. XTS Guard 7 runs on STOP 8, the general-purpose operating system with security as its core focus, developed by BAE Systems. STOP 8 ensures the diversity of Guard deployment within a multi-guard cross-domain solution, specified in RTB design patterns.

The XTSG retains its own security policy for process separation, domain separation, and one-way data transfer. A mandatory role-based access control (RBAC) model uses security roles to designate permission levels, and a Bell-LaPadula/Biba (BL/B) model provides a classification element that specifies where a given process or data set can and cannot exist. The combined RBAC and BL/B assignment is referred to as a security label. With XTS Guard, the number of security domains that can be interconnected is limited only by hardware. XTS Guard Enterprise version offered today can handle up to 20 security enclaves on either 1U - 2U hardware, and it is approved for both SABI and TSABI data transfer operations.

In contrast, alternative solutions support far less domains or charge a significant fee to add domains. This hardware architecture presents the possibility of consolidating many different enterprise devices into just one enterprise guard system for large financial savings. Lastly, BAE Systems provides a small form factor ruggedized solution as well that can handle up to 10 domains in a single 2x4x6 chassis for field deployments and holds an R5 GMS ruggedization level. Please feel free to reach out to schedule a whiteboard meeting to discuss your program's requirements. 703.689.1465, [tim.goben@baesystems.com](mailto:tim.goben@baesystems.com)



## WHAT IS AFCEA?

AFCEA is a member-based, non-profit association for professionals that provides highly sought-after thought leadership, engagement and networking opportunities. We focus on cyber, command, control, communications, computers and intelligence to address national and international security challenges.

The association has more than 29,000 individual members, 140 chapters and 1,536 corporate members. For more information, visit [www.afcea.org](http://www.afcea.org)

