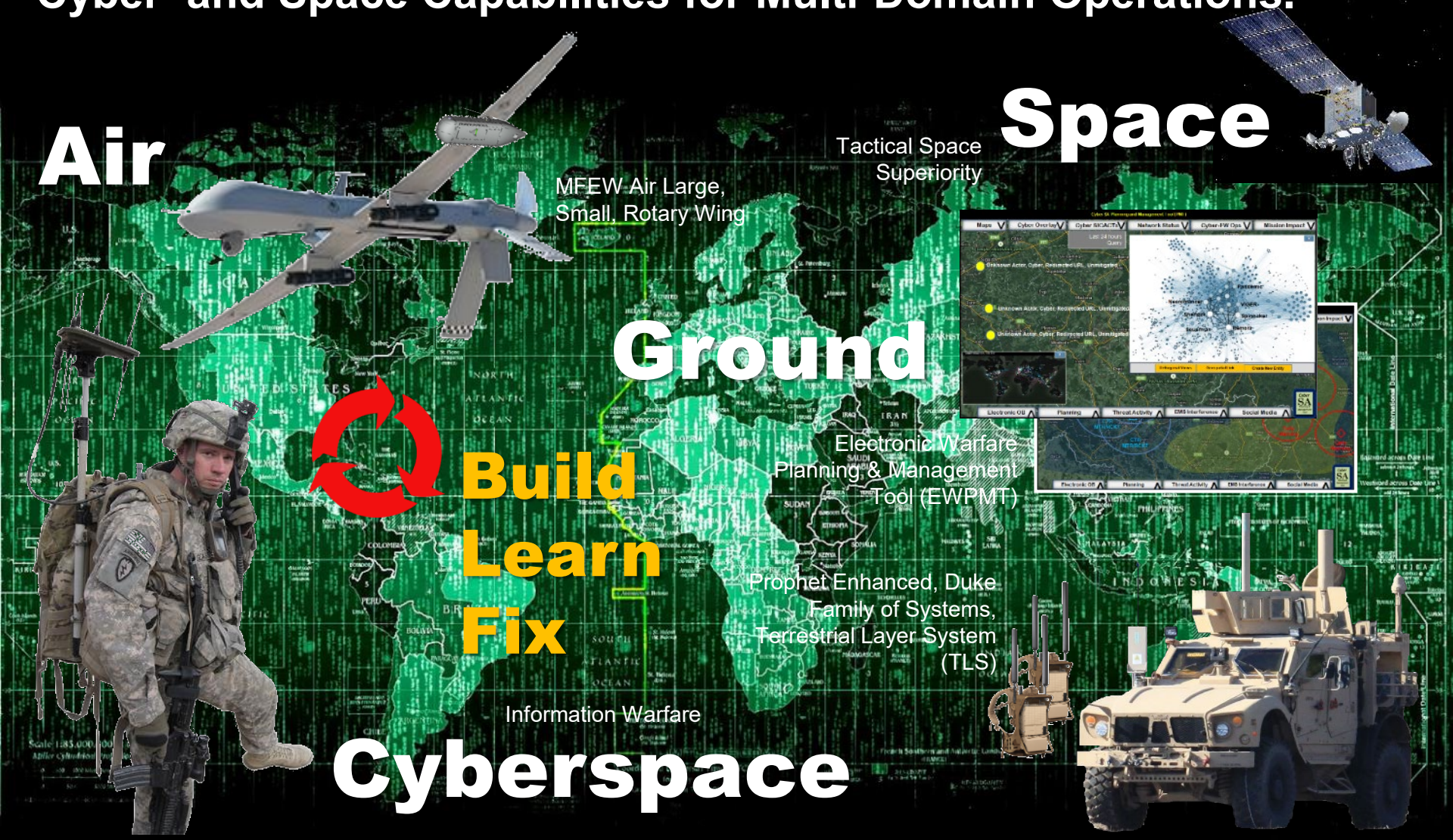
PM Electronic Warfare & Cyber

On the Road to 2028: Equipping the Force

23 AUG 2019

COL Kevin Finch
Project Manager
Electronic Warfare & Cyber
410-306-2180

Rapidly delivering Integrated Electronic Warfare, Intelligence, Cyber and Space Capabilities for Multi-Domain Operations.



Agile, adaptive programs that deliver now and pace the threat.

PM EW&C Portfolio

Prophet	Electronic Attack (EA)	EW Integration (EWI)	Information Warfare (IW)	Tactical Space Superiority (TSS)
				
• Prophet Enhanced • Terrestrial Layer System	• Mounted CREW - Duke • Dismounted CREW • Fixed Site CREW • Fixed Site EA • Multi-Function EW – Air	• EW Planning & Management Tool (EWPMT) • RF Interference Mitigation (RIM)	• Offensive Cyber Infrastructure • Weapon System / Tools • Defense Cyber Operations – Response Actions	• Space

Operational Capabilities

Ground SIGINT **Actionable Intelligence** **Situational Understanding** **Force Protection** **Theater Net-Centric Geo-location**	**Electronic Attack** Offensive / Defensive **Electronic Support** **Situational Awareness** **Force Protection - RCIED**	**Electromagnetic Battle Management** **Spectrum Management Operations** **Spectrum Compatibility**	**Offensive Cyberspace Operations** **Special User** **Low Quantity Fielding** **Development Operations** **Cyber Support to Corps & Below**	**Classified Capabilities**

Recent Accomplishments

- **Major Contract Awards:**
  - ~$1B multi-award IDIQ contract for development of Cyber capabilities
  - EWPMT CD4 Task Order
  - Prophet ceiling increase to support ESP kits and CEMA ONS
- **Expanding to support Joint requirements:**
  - IW project selected as Joint Common Access Program (JCAP)
  - Rapid Cyber Development Network expanding to other services
  - EWPMT being assessed as Joint EMBM solution
- **New Requirements:**
  - EWPMT Capability Drop 4
  - Multiple Requirement Definition Packages for Offensive Cyber
  - CPD for Space Capabilities
- **Summer "campaign of learning" for SIGINT/EW/Cyber - new Tactical EW System (TEWS) prototype**
  - Joint Warfighting Assessment (JWA) & Joint Operational Integration Assessment
  - National Training Center (September)
- **New Program! Approved MDD for Terrestrial Layer System (TLS)**
- **Transitioned full responsibility for CEMA & USAREUR ONS from RCCTO, PM EW&C is MDA**
- **Supporting transition of C5ISR OTA contract vehicle to PEO IEW&S**
- **Ongoing CREW support to CENTCOM and Coalition Loan Program**
- **Release of PM EW&C CMOSS standards and policy**

PM Electronic Warfare and Cyber Priorities

1. **<u>Build</u> new start Electronic Warfare/SIGINT and Cyber programs:**
   - Terrestrial Layer System Large (TLS-L)
   - Multi-Function Electronic Warfare Air Large (MFEW-AL)
   - Offensive Cyber Operations

2. **<u>Deliver</u> capabilities now to support Theater Operational Needs (ONS):**
   - Multiple theaters of operation
   - Dismounted Counter RCIED
   - Cyber Rapid Development/Operations (DEVOPS)
     - On the Path to Become POR

3. **<u>Execute</u> Programs of Record (POR):**
   - Electronic Warfare Planning and Management Tool (EWPMT)
   - Prophet Enhanced Modification and Fielding (POR B, Prophet ESP)
   - Offensive Cyber Operations
   - Counter Radio Controlled Improvised Explosive Device (CREW Duke)

4. **<u>Posture</u> to Pace the Threat**
   - Modular open architectures allow to adapt to changing threat
     - Interoperable (TLS, CWSB, MFEW-AL)
     - Easily integrated capabilities from 3rd parties

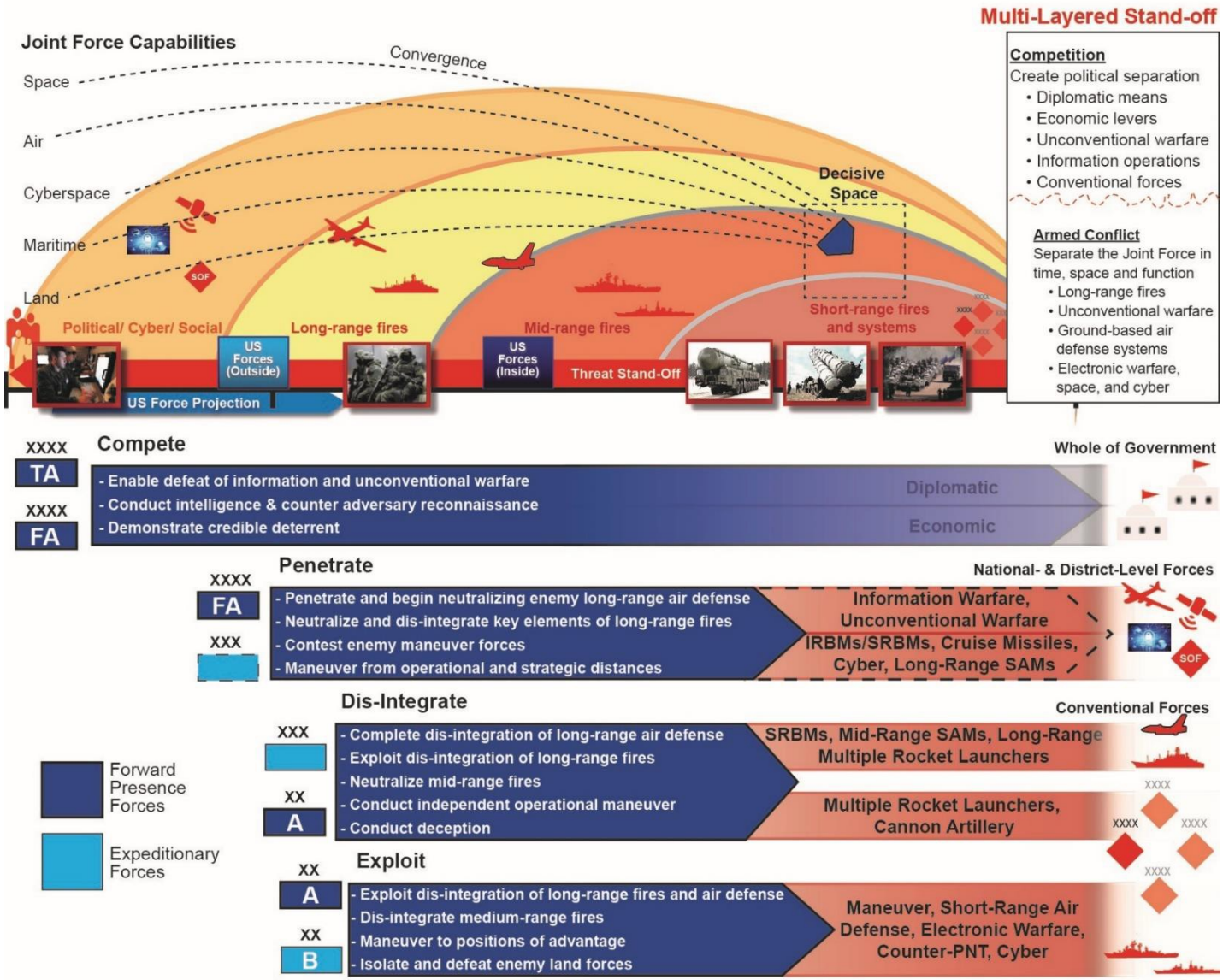
Deliver now…and pace the threat

The U.S. Army in Multi-Domain Operations
TRADOC PAM 525-3-1

Problem: Near peer adversaries generate multiple-layers of *stand-off* designated to separate the U.S. and its partners politically and the Joint force in space, time, and function. Adversaries are contesting all domains, the electromagnetic spectrum (EMS), and the information environment.

Solution: The Army fields an MDO-capable force that is designed to counter near peer adversaries by competing, penetrating, disintegrating, exploiting, and re-competing.

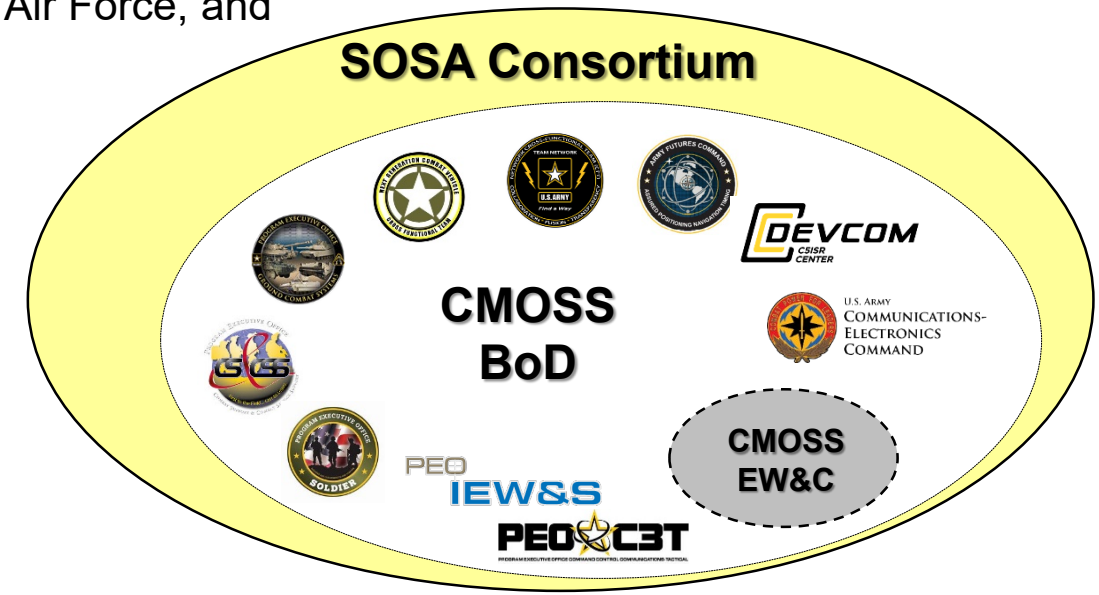
MDO Components: Army forces actively engaging across domains including (space & cyber), in the EMS and in the information environment. Convergence optimizes the employment of capabilities across all domains, the EMS, and the information environment to stimulate, see, and strike the enemy.



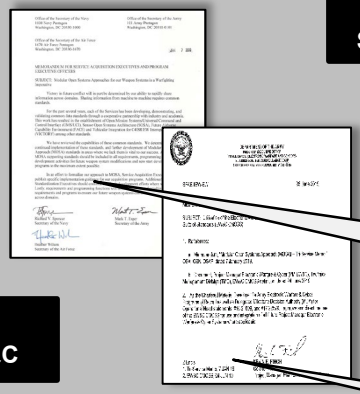
Modular Open Systems Approaches

- **WHY?** At the core, C4ISR/EW systems use many of the same technologies, but they are not always compatible between systems (e.g., amplifiers, filters, processors).
- **HOW?** CMOSS is being included in and managed under the SOSA initiative with Army, Air Force, and Navy participation.

- Reduces integration costs and risks
- Mitigates obsolescence
- Facilitates interoperability and reuse
- Accelerates fielding and deliveries



Modular Open Systems Approaches for our Weapon Systems



Tri-Service

PM EW&C

Utilization of Electronic Warfare & Cyber C4ISR/EW Modular Open Suite of Standards (EW&C CMOSS)

We determined the continued implementation of these standards, and further Development of ***Modular Open Systems Approach (MOSA)*** standards in areas where we lack them is vital to our success.

- Secretaries of the Army, Navy, & Air Force

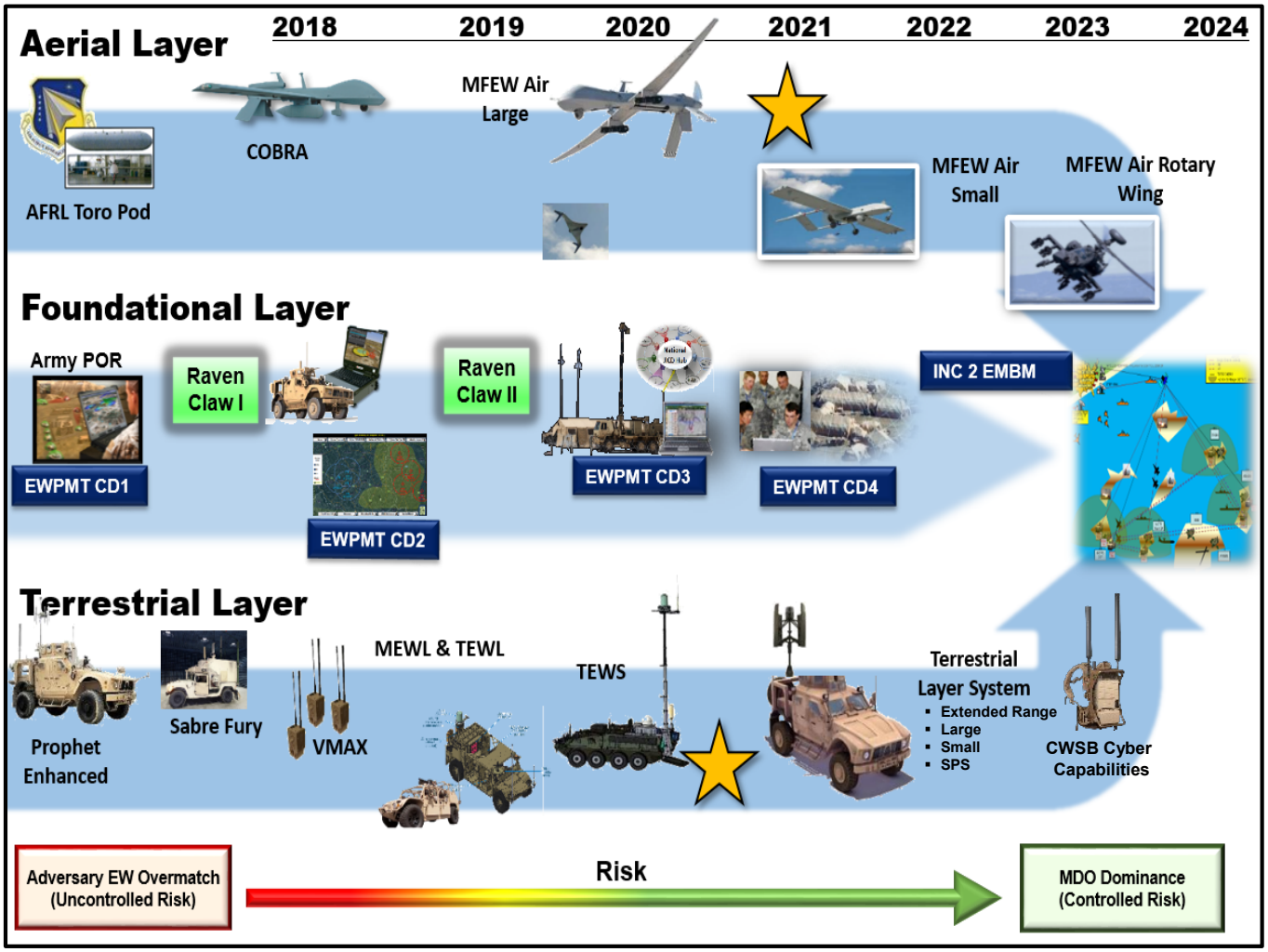
I approve and direct the use of the EW&C ***CMOSS*** for use and integration of all future Project Manager EW&C Systems where applicable.

- COL Kevin E. Finch, Project Manager, EW&C

Equipping the Force for Multi-Domain Operations

Design Tenants

- **Strategic, Operational, Tactical.** Layered approach to address Multi-Domain requirements.
- **Expeditionary.** Platforms to be based on supported maneuver unit.
- **Modular.** Open architecture enables future growth to pace the threat.
- **Defined Software Framework.** Allows rapid integration of signal "Libraries" instead of costly and time consuming integration of individual signals.
- **Commonality.** Similar and complementary look-and-feel for usability and reuse.
- **Automated.** Machine Learning for improved CEMA responsiveness and reduced Soldier workload
- **Rapid and Agile.** Early capability with multiple learning events and product improvements



Integrating the Best of Industry Across the Joint Force

On the Road to 2028: Delivering Integrated EW, SIGINT and Cyber at the Tactical Echelon

PM Electronic Warfare & Cyber

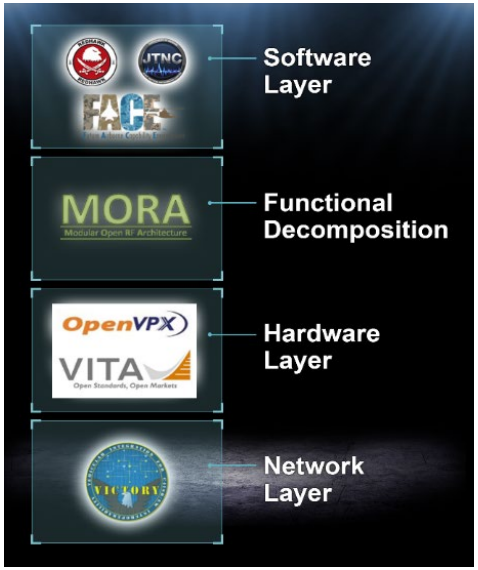
COL Kevin Finch
Project Manager
Electronic Warfare & Cyber
410-278-6210

Kenneth Strayer
Deputy Project Manager
Electronic Warfare & Cyber
410-278-6210

BACKUPS

What is CMOSS?

- CMOSS consists of a **suite of layered standards** that are individually useful and can be combined to form a holistic converged architecture
- CMOSS goals:
  - Provide pooled RF resources (e.g., antennas and amplifiers) for Communications, Electronic Warfare, and Signals Intelligence systems
  - Share processing resources (e.g., computers and displays) and data services (e.g., Position, Navigation, and Time) to reduce SWaP requirements
  - Facilitate rapid insertion of new capabilities into systems



Software Layer:
- Enables portability of software applications across hardware platforms
- Software framework selected based on mission area

Functional Decomposition:
- Allows for sharing of RF resources such as antennas and amplifiers
- Defines interfaces between RF functions and components
- Enables best of breed along with rapid component upgrades

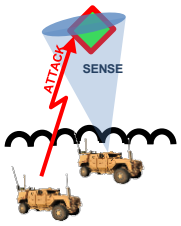
Hardware Layer:
- Enables capabilities to be fielded as cards in a common chassis
- Common form factor including physical, electrical, and environmental specifications

Network Layer:
- Provides connectivity within the platform and defines interfaces between capabilities
- Enables legacy systems to share services within the converged architecture

Army, Air Force, and Navy are collaborating under the SOSA Consortium to develop a holistic open architecture that leverages existing standards, maximizes economies of scale, and provides the flexibility to rapidly insert the latest capabilities

Terrestrial Layer System (TLS) Update

- TLS provides a Signals Intelligence (SIGINT), Electronic Warfare (EW), and Cyber-enabling integrated solution to support Multi-Domain Operations.
- Provides the maneuver commander with electronic attack and offensive cyber warfare options to deny, degrade, disrupt, or otherwise manipulate the targeted force.
- TLS employs technologically advanced systems with a modular open-system approach that can be more efficiently sustained and more effectively upgraded.
- TLS supports Army forces actively engaging across domains including (space & cyber), in the electromagnetic spectrum and in the information environment.



- Government intends to use C5 Consortium to award one or more Other Transaction Authority (OTA) agreements for TLS prototype and integration efforts.
  - Both a Request for White Paper (RWP) and a Tech Demo will be used as selection criteria for OTA award(s).
- Industry Day #2 conducted on 11 July to inform and prepare industry of upcoming solicitation.
- Successful outcome from OTA efforts may culminate with Production Contract Award planned for FY22.

Event/Action	Tentative Dates
Draft RWP Released	01 JUL 19
Industry Day	11 JUL 19
Official RWP Released	19 JUL 19
Tech Demos Requested	30 AUG 19
Anticipated OTA Award	01 APR 20

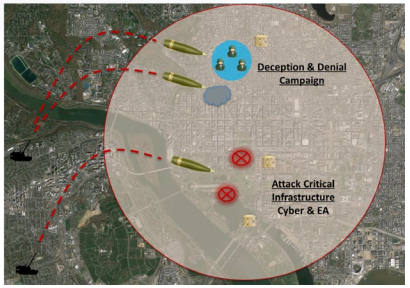
TLS - Extended Range (TLS ER) Request for Information (RFI)

- Seeking to inform technical approaches for a potential TLS ER solution in support of the Long Range Precision Fires and Increased Lethality at ranges between 40 and 1000 KM.
- Concepts/recommendations are requested for optimized approaches to integrating SIGINT, EW, and CO capabilities that can operate in existing formations for Division, Corps, and Army Service Component Commands.
- FEDBIZ OPS: RFI posted on 6 June 2019.
- NOTE: The TLS ER RFI is not connected with other current TLS acquisition efforts.

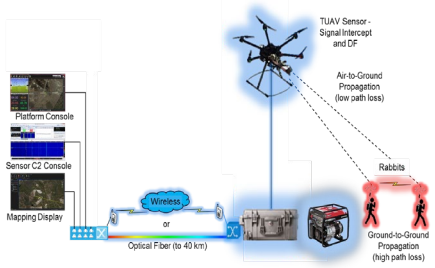
Notional Concepts:

Airborne or Air Delivered

Artillery Delivered



High Altitude



Hand Emplaced

Tethered UAS