DEFENSEDAILY'S

MODULAR OPEN SYSTEMS SUMMIT

Connecting Defense, Intelligence and Industry in the Digital Future

2018 Agenda

Tuesday | May 1

8:00 AM – 8:30 AM | Breakfast

Complimentary breakfast and coffee will be provided as you network with your other Defense Colleagues on the General Session floor. The Defense Daily Team will lead introductions for the day's activities and introduce our Speakers. Let the Sessions begin!

- Dan Parsons Editor, Defense & Open Architecture / Defense Daily /

8:30 AM – 9:15 AM| Morning Keynote

9:15 AM – 10:00 AM | Morning Plenary

10:00 AM – 11:00 AM | Morning Break - Exhibit Hall

10:00 AM – 10:15 AM | National Security Briefing 1

10:30 AM – 11:00 AM | National Security Briefing 2

11:00 AM – 12:00 PM | Combining Opens Systems Architecture and Technology Demonstrations to enable Acquisition Reform and meet Multi-Domain Battle Requirements (Bell Helicopter)

As the Joint Force adjusts Operating Concepts to deter or meet the demands of future warfare the Unites States must make fundamental changes to the DoD Acquisition Process. Acquisition reform is critical to fielding capability faster than potential peer adversaries and maintaining a premier fighting force. These reforms include combining technology demonstrations in vehicle systems and open architecture requirements for the hardware and software of mission systems. This allows the Joint Services to take advantage of the rapid pace of technology advancements and keep the warfighter ahead of adversaries in critical capabilities.

The combination of an open systems architecture in technology demonstrators and early prototypes facilitates the development of systems that are capable of growth in weight and power as well as mission systems capacities. This allows parallel development of capabilities with emerging requirements. This key component eliminates costly redundancy in the acquisition system, reduces program risk and delivers warfighters capability when they need it.

With the current rate of technology advancement, fiscal challenges and emerging adversaries, the USG cannot continue with the traditional acquisition methods. Open systems architecture combined with robust technology demonstrations and early prototyping presents some challenges and opportunities to the USG and industry. These challenges include cyber security, protection of proprietary information, funding availability and overcoming decades of inefficient acquisition methods. Close USG/Industry cooperation understanding and working thru these challenges will ensure success in future acquisition programs.

Learning Objectives:

- Enabling acquisition reform through USG/Industry cooperation in effective Technology Demonstration program management.
- Open system architecture challenges, data rights and potential impacts on acquisition reform.
- Overcoming challenges with the current DoD 5000 and rate of technology advancement (e.g. life cycle sustainment strategies for software intensive systems through technology insertion and software product upgrade).
- How open system architecture and technology demonstrations support rapid increase in capability reducing program cost and risk.

12:00 PM – 1:00 PM| Keynote Lunch

1:30 PM – 2:30 PM | Room #1: Ensuring Security of our Homeland against Unknown Threats

When it comes to protecting our homeland and ensuring security of our country's critical infrastructure, it is imperative for security technologies to be seamlessly compatible with each other. Customs and Border Protection, the Transportation Security Administration, and other components of the Department of Homeland Security are acquiring security systems that feature open system architecture, making it easier to operate different systems, avoid vendor lock, and increase competition for upgrades and enhancements to existing equipment.

- Steve Karoly Acting Assistant Administrator, Office of Requirements and Capabilities Analysis / Transportation Security Administration (TSA) /
- Mark J. Laustra Vice President, Global Business Development & Government Relations, Chairman, Security Manufacturers Coalition / Analogic Corp. /

1:30 PM – 2:30 PM | Breakout Session - Room 2

2:30 PM – 3:30 PM | Afternoon Break - Exhibit Hall

3:00 PM – 3:15 PM | 5 Things Federal Contractors Need to do to Get Cybersecurity Right

Part of the responsibility of the contractor that deploys IT solutions for the federal government includes resolving open security findings so that the system is cleared for operation. Though vulnerability scanning tools provide an excellent snapshot of the state of the environment, those with deep knowledge of the design and architecture of these systems are often able to find ways to work around some of the security controls if they choose to. If a control can be bypassed, what else is exposed? Why does this even happen and what can be done about it? In years of federal IT consulting, we have seen gaps that exist for many reasons; budget constraints, deadlines, contractual restrictions, competency challenges, and so on. Taking cybersecurity to a completely different level will require drastic changes in the federal contracting process, and we discuss five areas that need serious consideration.

Learning Objectives:

- Understand where IT security gaps exist in federal IT project implementations
- Identify what is needed to more adequately ensure the security of IT systems

3:15 PM – 3:30 PM | Complying with ITAR Requirements in a Modular Open System Architecture

Topic includes:

- ITAR requirements in open standards-based defense systems
- Sharing ITAR-controlled technical data in an open multi-vendor environment
- Defense services and dealing with foreign program partners and subcontractors in open systems
- Use of TAA's and other multi- party license authorizations
- Coordination of restrictions on ITAR-controlled technical data and IP data rights
- ITAR data security requirements

Learning Objectives:

- Understand the ITAR regulatory requirements that arise in open system operations
- Understand the legal risks and potential penalties for ITAR violations
- Practical recommendations for compliance and risk mitigation

3:30 PM – 4:30 PM | Breakout Session - Room 1

3:30 PM – 4:30 PM | Breakout Session - Room 2

5:00 PM – 7:00 PM | Evening Reception and Open Systems Award - Exhibit Floor

DEFENSEDAILY'S

MODULAR OPEN SYSTEMS SUMMIT

Connecting Defense, Intelligence and Industry in the Digital Future

Wednesday | May 2

8:00 AM – 8:30 AM | Breakfast

Complimentary breakfast and coffee will be provided as you network with your other Defense Colleagues on the General Session floor. The Defense Daily Team will lead introductions for the day's activities and introduce our Speakers.

8:30 AM – 9:15 AM | Morning Keynote

9:15 AM – 10:00 AM | Morning Plenary

10:00 AM – 11:00 AM | Morning Break - Exhibit Hall

10:00 AM – 10:15 AM | National Security Briefing 1

10:30 AM – 10:45 AM | National Security Briefing 2

11:00 AM – 12:00 PM | Breakout Session - Room 1

11:00 AM – 12:00 PM | Breakout Session - Room 2

12:00 PM – 1:30 PM | Keynote Lunch

1:30 PM – 2:30 PM | General Session

2:45 PM – 3:00 PM | Closing Comments