



DoD Systems Engineering Update

Kristen Baldwin

**Acting Deputy Assistant Secretary of Defense for
Systems Engineering**

**NDIA Systems Engineering Division Meeting
December 6, 2017**



DASD, Systems Engineering



**Acting Deputy Assistant Secretary of Defense
and Principal Deputy, Systems Engineering**
Kristen Baldwin

**Homeland Defense
Capability
Development**
Robin Hicks



Major Program Support
James Thompson



Engineering Enterprise
Robert Gold

*Supporting USD(AT&L) Decisions with
Independent Engineering Expertise*

- Engineering Assessment / Mentoring of Major Defense Programs
- Program Support Assessments
- Overarching Integrated Product Team and Defense Acquisition Board Support
- Systems Engineering Plans
- Systemic Root Cause Analysis
- Development Planning/Early SE
- Program Protection

*Leading Systems Engineering Practice
in DoD and Industry*

- Systems Engineering Policy and Guidance
- Technical Workforce Development
- Specialty Engineering (System Safety, Reliability and Maintainability, Quality, Manufacturing, Producibility, Human Systems Integration)
- Security, Anti-Tamper, Counterfeit Prevention
- Standardization
- Engineering Tools and Environments

Providing technical support and systems engineering leadership and oversight to USD(AT&L) in support of planned and ongoing acquisition programs



DoD Engineering Focus Areas



- **Grow and maintain engineering and technical leadership talent**
- **Mature engineering practices to implement modularity, agility, and innovation into systems**
- **Leverage advanced analytical and computing technologies and migrate to digital acquisition, engineering and manufacturing practice**
- **Address complex software development, integration, and sustainment challenges**
- **Establish practices for cyber-resilient aerospace and defense systems**
- **Enable trust and access to assured hardware and software**
- **Implement enterprise and mission integration management capabilities**



Major DASD(SE) Deliverables Planned for FY18 (1/2)



- **Policy and Guidance**

- Consolidate access to enterprise standards (Section 875)
- Issue updated Systems Engineering Plan (SEP) & Program Protection Plan (PPP) guidelines
- Implement Independent Technical Risk Assessment (ITRA) process & policy

- **Digital Engineering (DE)**

- Publish DoD DE strategy
- Oversee pilots, policy, and implementation actions

- **Modular Open Systems Approach (MOSA)**

- Define MOSA methods & guidelines

- **Software**

- Address Defense Science Board recommendations
- Explore software occupational career code
- Publish recommended competencies for software engineering

- **Mission Engineering/SoS Engineering**

- Mission Integration Management strategy to Congress
- Determine Research & Engineering (R&E) Mission Integration Structure and Roles
- Identify Competencies, Tools, and Training Needs

- **Workforce**

- Advance initiatives to address organic workforce needs
- Propose competencies for cybersecurity engineering
- Advanced Technical Degree Guidebook
- Recommend Production, Quality, and Manufacturing (PQM) career field restructure

- **Schedule**

- Update Integrated Master Plan/Integrated Master Schedule (IMP/IMS) Guidance

- **Sustainment Engineering**

- Develop a strategy to address sustainment engineering



Major DASD(SE) Deliverables Planned for FY18 (2/2)



- **Trusted Hardware (HW) and Software (SW) Assurance**
 - Realize Joint Federated Assurance Center (JFAC) Full Operational Capability (FoC)
 - Sustain Enterprise licenses for software assurance tools
 - Trusted & Assured Microelectronics Program and Strategy Report to Congress
- **Protection of Critical Technologies**
 - Joint Acquisition Protection and Exploitation Cell (JAPEC) DoD Instruction
- **Cyber Resilient Weapon Systems**
 - Produce tailored data protection standards for critical systems
 - Establish cyber resilient weapon systems Body of Knowledge (BoK)
 - Publish Cyber Appendix to DoD Risk, Issue, and Opportunity (RIO) Management Guide for Defense Acquisition Programs
- **Modeling and Simulation (M&S)**
 - Component and COCOM M&S gap analysis
 - DoD M&S Guidebook
- **Systems Engineering Research Center (SERC)**
 - Complete 5-year Comprehensive Review
 - Update 5-year Technical Plan
- **MITRE**
 - Complete 5-year Comprehensive Review
- **Counter-Unmanned Aircraft Systems (C-UAS) Technical Support**
 - Deliver Host-Nation Technology Report to Congress
 - Maintain compendium of technologies
 - Coordinate CONUS/OCONUS capability, interagency activities
- **Capability Development Working Group (CDWG)**
 - Homeland Capability Development with the Department of Homeland Security (DHS)



Opportunities for DoD and Industry Collaboration



- **Digital Engineering**

- Examine standardization of outputs from concept, requirements, architecture and design activities in DE to enable: 1) transition to manufacturing 2) transition to production, 3) transition to sustainment, and 4) tech data packages
- Investigate ability to conduct a competition via models; explore how industry might be converting model contents to documents for contractual compliance
- Continue deployment of tools, tool characterization, and use methods
- Engage with Semantic Web Technologies Foundation for Systems Engineering, a SERC, JPL, ESA (European Space Agency), INCOSE collaboration

- **Modeling and Simulation**

- Identify and address data collection, analysis, and sharing issues that are limiting development of more robust modeling and simulation capabilities, specifically a Common Data Environment for Modeling and Simulation

(Ref: SASC report 115-125, page 79, "Common Data Environment for Modeling and Simulation" <https://www.congress.gov/115/crpt/srpt125/CRPT-115srpt125.pdf>)



Opportunities for DoD and Industry Collaboration (continued)



- **Modular Open Systems Approach (MOSA)**
 - Work with industry to define practices for achieving the goals for MOSA outlined in the Acquisition Agility Act, including 1) assessment methods to determine whether MOSA has been applied to the maximum extent practicable and 2) methods or standards to apply MOSA to achieve particular benefits
- **Emphasizing Reliability & Maintainability (R&M) in Weapon System Design**
 - Explore methods to incentivize R&M performance on a development or production contract
 - Gain support from industry for the “R&M Body of Knowledge”
- **Sustainment Engineering**
 - Characterize sustainment engineering activities to support body of knowledge development



Opportunities for DoD and Industry Collaboration (continued)



- **System of Systems/Mission Engineering**
 - Engage with mission engineering competency activities
 - Explore role of industry in mission engineering and mission integration
 - Identify approaches for garnering inputs or otherwise getting participation from multiple industry partners across mission/capability areas to perform mission characterization/analysis
- **Workforce**
 - Assess benefits/opportunities of collaborating on the combined gov't/industry technical workforce and explore shared engineering workforce capability challenges/shortfalls
 - Support expansion of SE Capstone Marketplace
 - Help grow SERC Doctoral Fellows Program



Engineering Cyber Resilient Weapon Systems – Background



- **DoD Instruction 5000.02 Operation of the Defense Acquisition System, Enclosure 14, Cybersecurity in the Defense Acquisition System, holds the acquisition community responsible and accountable for cybersecurity in the defense acquisition system**
- **DASD(SE) is pursuing implementation of Enclosure 14 through five areas identified for further investigation:**
 1. Technical Performance Measures and Metrics
 2. Systems Engineering Technical Reviews
 3. Leveraging System Safety Practices
 4. Cyber Resilient Software
 5. DoD Risk, Issue, and Opportunity (RIO) Management Guide Update
- **NDIA held a 3-day Cyber Resilient Summit in April 2017; dialogue found government and industry have common systems engineering challenges:**
 - Emphasized need for consistency across communities
 - Discussed approaches to risk acceptance
 - Offered thoughts on implementing safeguards on manufacturing floor
 - Offered areas for improvements to methods, standards, processes, and techniques for cyber resilient & secure weapon systems
 - Thoughts on addressing sustainment challenges

DoDI 5000.02: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002_dodi_2015.pdf



Opportunities for DoD and Industry Collaboration (continued): Cyber Resilient Weapon Systems



- **Investigate engineering and design methods, standards to enable the system architecture and design to address, at a minimum, how the system:**
 - Manages access to and use of the system and system resources
 - Is structured to protect and preserve system functions or resources, (e.g., through segmentation, separation, isolation, or partitioning)
 - Maintains priority system functions under adverse conditions
 - Is configured to minimize exposure of vulnerabilities that could impact the mission, including through techniques such as design choice, component choice, security technical implementation guides, and patch management in the development environment (including integration and T&E), in production and throughout sustainment
 - Monitors, detects, and responds to security anomalies
 - Interfaces with DoD Information Network (DoDIN) or other external security services



Opportunities for DoD and Industry Collaboration (continued): Cyber Resilient Weapon Systems



- **Identify what is needed to establish security as a fundamental competency of systems engineering**
 - Explore how industry, academia, and government can work together to drive consistency across system security engineering activities using systems engineering practices
 - Identify how the DoD Risk, Issue, and Opportunity processes can help develop a culture in which engineers inform risk decisions by factoring in cybersecurity with all other elements of the system constraints
 - Investigate the use of Technical Performance Measures as a mechanism to conduct ongoing assessments of the cyber risks, issues, and opportunities and the likelihood of meeting system performance objectives. Insight will inform trade-off and risk acceptance decisions. [Build from the Technical Measurement Report, A Collaborative Project of PSM, INCOSE and Industry, December 2005]
- **Explore shared engineering workforce capability challenges/shortfalls**
 - Identify how to educate and train more engineers on the foundations, principles, and characteristics of security and resilience in Cyber Physical Systems; develop engineers who are able to translate Information Technology compliance and network resiliency requirements to inform weapon system resiliency
 - Identify mechanisms to develop an engineering culture able to translate cybersecurity needs in the technical risk process



Opportunities for DoD and Industry Collaboration (continued)



- **Systems Engineering Research**

- Participate in review of future DoD Systems Engineering Research Center (SERC) Technical Plan

- **Division Organization**

- Review NDIA SE Division organization (Committees and charters) to consider overlaps and gaps; ensure today's SE areas of interest are addressed
- Translate the results of organizational review into 2018 SE Conference call for papers and event plenary/track structure



Systems Engineering: Critical to Defense Acquisition



Defense Innovation Marketplace
<http://www.defenseinnovationmarketplace.mil>

DASD, Systems Engineering
<http://www.acq.osd.mil/se>