OSD Systems Engineering Status and Goals

Stephen Welby
Deputy Assistant Secretary of Defense for Systems Engineering

AIA Technical Operations Council (TOC)
May 1, 2013
Better Buying Power 2.0
A Guide to Help You Think

Achieve Affordable Programs
• Mandate affordability as a requirement
• Institute a system of investment planning to derive affordability caps
• Enforce affordability caps

Control Costs Throughout the Product Lifecycle
• Implement “should cost” based management
• Eliminate redundancy within warfighter portfolios
• Institute a system to measure the cost performance of programs and institutions and to assess the effectiveness of acquisition policies
• Build stronger partnerships with the requirements community to control costs
• Increase the incorporation of defense exportability features in initial designs

Incentivize Productivity & Innovation in Industry and Government
• Align profitability more tightly with Department goals
• Employ appropriate contract types
• Increase use of Fixed Price Incentive contracts in Low Rate Initial Production
• Better define value in “best value” competitions
• Only use LPTA when able to clearly define Technical Acceptability
• Institute a superior supplier incentive program
• Increase effective use of Performance-based Logistics
• Reduce backlog of DCAA Audits without compromising effectiveness
• Expand programs to leverage industry’s IR&D

Reduce Unproductive Processes and Bureaucracy
• Reduce frequency of higher headquarters level reviews
• Re-emphasize AE, PEO and PM responsibility, authority, and accountability
• Reduce cycle times while ensuring sound investment decisions

Promote Effective Competition
• Emphasize competition strategies and creating and maintaining competitive environments
• Enforce open system architectures and effectively manage technical data rights
• Increase small business roles and opportunities
• Use the Technology Development phase for true risk reduction

Improve Tradecraft in Acquisition of Services
• Assign senior managers for acquisition of services
• Adopt uniform services market segmentation
• Improve requirements definition/prevent requirements creep
• Increase small business participation, including through more effective use of market research
• Strengthen contract management outside the normal acquisition chain – installations, etc.
• Expand use of requirements review boards and tripwires

Improve the Professionalism of the Total Acquisition Workforce
• Establish higher standards for key leadership positions
• Establish stronger professional qualification requirements for all acquisition specialties
• Increase the recognition of excellence in acquisition management
• Continue to increase the cost consciousness of the acquisition workforce – change the culture

For additional information on Better Buying Power 2.0: http://bbp.dau.mil/
DASD, Systems Engineering Mission

Systems Engineering focuses on engineering excellence – the creative application of scientific principles:
- To design, develop, construct and operate complex systems
- To forecast their behavior under specific operating conditions
- To deliver their intended function while addressing economic efficiency, environmental stewardship and safety of life and property

**DASD(SE) Mission:** Develop and grow the Systems Engineering capability of the Department of Defense – through engineering policy, continuous engagement with component Systems Engineering organizations and through substantive technical engagement throughout the acquisition life cycle with major and selected acquisition programs.

A Robust Systems Engineering Capability Across the Department Requires Attention to Policy, People and Practice

**US Department of Defense is the World’s Largest Engineering Organization**
- **Over 99,000** Uniformed and Civilian Engineers
- **Over 39,000** in the Systems Engineering (SPRDE) Acquisition Workforce
DASD, Systems Engineering

Stephen Welby
Principal Deputy Kristen Baldwin

Systems Analysis
Kristen Baldwin (Acting)
Addressing Emerging Challenges on the Frontiers of Systems Engineering
Analysis of Complex Systems/Systems of Systems
Program Protection/Acquisition Cyber Security
University, FFRDC and Industry Engineering and Research
Modeling and Simulation

Major Program Support
James Thompson
Supporting USD(AT&L) Decisions with Independent Engineering Expertise
Engineering Assessment / Mentoring of Major Defense Programs
Program Support Reviews
OIPT / DAB / ITAB Support
Systems Engineering Plans
Systemic Root Cause Analysis

Mission Assurance
Nicholas Torelli
Leading Systems Engineering Practice in DoD and Industry
Systems Engineering Policy & Guidance
Development Planning/Early SE
Specialty Engineering (System Safety, Reliability and Maintainability Engineering, Quality, Manufacturing, Producibility, Human Systems Integration)
Counterfeit Prevention
Technical Workforce Development
Standardization

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

- FY 2012 SE Annual Report delivered to Congress
- Detailed review of DASD(SE) accomplishments in FY12
- Review of Service progress and plans implementing key pieces of WSARA to improve SE capabilities
- Detailed program by program assessments for 40+ MDAPs

GAO Report 13-103 Findings
DASD(SE) Performance

- Completed the development of systems engineering and development planning policy, guidance and performance measures
- Regularly completing MDAP document review and approval and program monitoring and assessments
- Led working group efforts to support Service initiatives to address systemic reliability issues in UAS and rotary wing portfolios
- Led workforce development initiatives to attract and retain a qualified SE workforce and support KLP implementation
- Positively impacted the requirements development and technical and reliability planning for:
  - Joint Lightweight Tactical Vehicle
  - Ground Combat Vehicle
  - Joint Strike Fighter
  - Remote Mine-hunting System
  - Gray Eagle and Global Hawk

Top Level FY13 DASD(SE) Goals

• Continue excellence in SE support to programs and acquisition decisions

• Improve consistent program protection plan (PPP) engagement with programs resulting in successful vulnerability mitigation strategies

• Advocate for and ensure SE workforce capacity and capability

• Provide depth to acquisition policy and processes with SE guidance, practices, and continuous learning opportunities

• Advance the state of engineering to meet challenges and enable DoD goals

• Maintain quality of technical insight in resource constrained environment
FY13 DASD(SE) Objectives

• **Engineering Program Support**
  – Provide engineering assessment / mentoring of major defense acquisition programs
  – Support acquisition leadership with independent engineering analysis and advice
  – Support, review and approve Systems Engineering Plans
  – Engage with programs in support of preliminary design review/critical design reviews (PDR/CDR) assessments
  – Institutionalize software assessment support capability
  – Develop an update to the DoD Risk Management Guide to implement a risk management approach for PMs
  – Program data analysis and benchmarking

• **Engineering Workforce**
  – Publish Human Capital Strategic Plan content for Engineering Non-Construction, SPRDE and PQM career fields
  – Oversee implementation of Lead Systems Engineer Key Leadership Position (KLP)
FY13 DASD(SE) Objectives

• **Engineering Policy and Guidance**
  – Promulgate revised engineering guidance in DoDI 5000 and publish an update to the Defense Acquisition Guidebook Chapter 4 – Systems Engineering
  – Oversee Value Engineering activities in support of Better Buying Power (BBP) 2.0
  – Publish Open Systems Architecture guidance in support of BBP 2.0
  – Finalize DAES reporting guidance for Reliability and Maintainability Engineering
  – Publish guidance on risk-based counterfeit prevention, in coordination with L&MR and DPAP, in support of FY12 NDAA Section 818 and FY13 NDAA Section 833

• **Technical Standards**
  – Oversee Government Industry Data Exchange Program (GIDEP) requirements update and implementation in support of FY12 NDAA Section 818 Counterfeit Prevention activities
FY13 DASD(SE) Objectives

- **Program Protection**
  - Conduct Anti-Tamper study to support exportability BBP 2.0 initiative
  - Update Software Assurance policy/guidance in compliance with FY13 NDAA Section 933
  - Implement AT&L strategy for Defense Industrial Board (DIB) Cyber Security/Safeguarding Unclassified information, and Supply Chain Risk Management in support of NDAA Section 941
  - Support acquisition program implementation of trusted microelectronics strategies in accordance with DoDI 5200.44 requirements for trusted ASICs and FPGA strategy
Defense Acquisition Guidebook (DAG)  
Chapter 4 Systems Engineering Update

- Improve guidance to fully reflect current policy and DASD(SE) initiatives:
  - Joint Capabilities Integration and Development System (JCIDS) (Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01H)
  - Process changes as a result of Better Buying Power
  - Systemic root cause analyses findings
  - Department-wide best practice; avoiding Service and domain-specific implementations

- Improve currency, consistency, usability, and readability—less theory, more utility

- Emphasize the role of Systems Engineering in providing balanced solutions (managing cost, schedule and risk) that deliver needed capability to the war fighter

- Make Chapter 4 an effective tool for the Program Manager and the Systems Engineering Practitioner

https://acc.dau.mil
Proposed DoD 5000.02 Update

- Decrease emphasis on “rules” and increase emphasis on process intent and thoughtful program planning
- Provide program structures and procedures tailored to the dominant characteristics of the product being acquired and to unique program circumstances, e.g., risk and urgency
- Added key decision points between Milestone A and Milestone B
- Institutionalize changes to statute and policy since the last issuance of DoD Instruction 5000.02
Program Protection Integrated in Policy

**DoDI 5000.02 Operation of the Defense Acquisition System**
- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD
- References DoDI 5200.39

**DoDI 5200.39 Critical Program Information (CPI) Protection Within the DoD**
- Assigns responsibility for Counterintelligence, Security, and System Engineering support for the ID and protection of CPI
- Expands definition of CPI to include degradation of mission effectiveness

**DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks**
- Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission critical functions or components

**DoDI 8500.01E Information Assurance**
- Establishes policy and assigns responsibilities to achieve DoD information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare

DoD Issuances Website: http://www.dtic.mil/whs/directives/corres/ins1.html
## What Are We Protecting?

### Technology
- **What**: Leading-edge research and technology
- **Who Identifies**: Technologists, System Engineers
- **ID Process**: CPI Identification
- **Threat Assessment**: Foreign collection threat informed by Intelligence and Counterintelligence assessments
- **Countermeasures**: AT, Classification, Export Controls, Security, Foreign Disclosure, and CI activities
- **Focus**: “Keep secret stuff in” by protecting any form of technology

### Components
- **What**: Mission-critical elements and components
- **Who Identifies**: System Engineers, Logisticians
- **ID Process**: Criticality Analysis
- **Threat Assessment**: DIA SCRM TAC
- **Countermeasures**: SCRM, SSE, Anti-counterfeits, software assurance, Trusted Foundry, etc.
- **Focus**: “Keep malicious stuff out” by protecting key mission components

### Information
- **What**: Information about applications, processes, capabilities and end-items
- **Who Identifies**: All
- **ID Process**: CPI identification, criticality analysis, and classification guidance
- **Threat Assessment**: Foreign collection threat informed by Intelligence and Counterintelligence assessments
- **Countermeasures**: Information Assurance, Classification, Export Controls, Security, etc.
- **Focus**: “Keep critical information from getting out” by protecting data

---

**Protecting Warfighting Capability Throughout the Life Cycle**
DoDI 5200.44
Trusted Systems and Networks

• Implements the DoD’s Trusted Systems and Networks (TSN) strategy

• Manage risk of mission-critical function and component compromise throughout lifecycle of key systems by utilizing
  – Criticality Analysis as the systems engineering process for risk identification
  – Countermeasures: Supply chain risk management, software assurance, secure design patterns
  – Intelligence analysis to inform program management

• Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)

• Document planning and accomplishments in program protection and information assurance activities
FY13 NDAA SEC. 941: REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS

- “The Secretary of Defense shall establish procedures that require each cleared defense contractor to report ... when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.”

Defense Industrial Base (DIB) Cyber Security

“The private sector, government, military, our allies - all share the same global infrastructure and we all share the responsibility to protect it.”

Secretary of Defense Leon E. Panetta
October 11, 2012

DoD efforts to advance cyber security in the DIB include:

- DIB Cyber Security/Information Assurance (CS/IA) Program, and its optional enhanced component the DIB Enhanced Cybersecurity Services (http://dibnet.dod.mil)
- Standards development in collaboration with Industry
- Reinforcing protection of technical information in acquisition activities
System Security Community Activities

- **NDIA “Guidebook for System Assurance”, Version 1.0, 2008**
  - Process/technology guidance to increase the level of system assurance through a planned, systematic set of multi-disciplinary activities

- **ISO/IEC 15026 – System and Software Engineering – Systems and Software Assurance**
  - Establishes common assurance concepts, vocabulary, integrity levels and life cycle activities

- **ISO/IEC 27036 – IT Security Techniques – Supplier Relationships**
  - Establishes techniques between acquirer and supplier for supply chain risk management

- **International Council on Systems Engineering (INCOSE) Handbook**
  - Working group to develop security engineering updates to INCOSE SE Handbook

- **NIST - System Security Engineering (SSE) 800-160 Special Pub (In Development)**
  - Aligns SSE with ISO/IEC15288 terminology, incorporates DoD best practices
  - DoD Appendix targets DoD community, includes Systems Engineering Technical Review (SETR) criteria

- **The Open Group (TOG)**
  - The Open Trusted Technology Provider Framework (O-TTPF) - open standard that codifies best practices across the entire lifecycle (targeted against counterfeit HW & malicious SW)
  - [http://www.opengroup.org/ogttf/](http://www.opengroup.org/ogttf/)
Data Vulnerability Tiger Team

- **USD(AT&L) Memorandum, February 7, 2013**
  - Established the Data Vulnerability Tiger Team
  - 60-day schedule
  - Review progress in protecting unclassified technical data
  - Identify further actions to take

- **Tiger Team actions**
  - Identify Focus Teams
  - Focus Teams will analyze gaps and recommend actions
  - Consolidate recommendations for USD(AT&L)
FY13 NDAA Section 933

FY13 NDAA SEC. 933: IMPROVEMENTS IN ASSURANCE OF COMPUTER SOFTWARE PROCURED BY THE DEPARTMENT OF DEFENSE

– USD(AT&L), in coordination with the DoD CIO… “shall develop and implement a baseline software assurance policy for the entire lifecycle of covered systems. Such policy shall be included as part of the strategy for trusted defense systems of the Department of Defense.”

– …“(2) require covered systems to identify and prioritize security vulnerabilities and, based on risk, determine appropriate remediation strategies for such security vulnerabilities;”
DoD SPRDE Workforce: Age Demographics

FY2007 Mean Age: 43.6 years
FY2008 Mean Age: 43.4 years
FY2009 Mean Age: 43.0 years
FY2010 Mean Age: 42.7 years
FY2011 Mean Age: 42.9 years
FY2012 Mean Age: 43.1 years

Source: AT&L Defense Acquisition Workforce Data Mart
SPRDE – Systems Planning, Research, Development and Engineering
### Engineering (Non-Construction) Functional Community by Occupational Series & Component

Total = 74,923

<table>
<thead>
<tr>
<th>Occupational Series</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0801-General Eng</td>
<td>14,571</td>
</tr>
<tr>
<td>0806-Materials Eng</td>
<td>814</td>
</tr>
<tr>
<td>0819-Environ Eng</td>
<td>2,048</td>
</tr>
<tr>
<td>0830-Mechanical Eng</td>
<td>2,149</td>
</tr>
<tr>
<td>0840-Nuclear Eng</td>
<td>3,361</td>
</tr>
<tr>
<td>0854-Computer Eng</td>
<td>4,033</td>
</tr>
<tr>
<td>0855-Electronics Eng</td>
<td>17,046</td>
</tr>
<tr>
<td>0851-Aerospace Eng</td>
<td>821</td>
</tr>
<tr>
<td>0853-Chemical Eng</td>
<td>1,158</td>
</tr>
<tr>
<td>0855-Industrial Eng</td>
<td>5,624</td>
</tr>
</tbody>
</table>

**Notes:**
1. 0840, 0854, 0855 designated “Mission Critical Occupations (MCOs)”
2. Does not include 0801A Acquisition Program Management Function

Source: DCPDS, June 30, 2012
Mission Critical Occupations: Age by Occupational Series

0840 - NUCLEAR ENGINEERING

0854 - COMPUTER ENGINEERING

0855 - ELECTRONICS ENGINEERING

Source: DCPDS via DRS, June 30, 2012

High number of young Engineers

Distribution Statement A – Approved for public release by OSR; SR#s 13-S-1115, 13-S-1634 and 13-S-1836 apply.
Are a majority of these Career Level 2s in 2 & 3-year intern programs? How many have industry experience?

What is being done to fill the gaps? Or is it necessary?

Data Source: CMIS data as of June 30 pulled on 9/18/2012
Population: Appropriated Fund excluding employees in SES like pay plans
0854 – Computer Engineer Career Level by Years of Service

Do these Career Level 3s have industry experience?

Is the ~10-yr departure a trend?

Data Source: CMIS data as of June 30 pulled on 9/18/2012
Population: Appropriated Fund excluding employees in SES like pay plans

Career Level 3: GS 13-15 or Equiv.
Career Level 2: GS 9-12 or Equiv.
Career Level 1: GS 1-8 or Equiv.
0855 – Electronics Engineer
Career Level by Years of Service

Do these Career Level 3s have industry experience?

Data Source: CMIS data as of June 30 pulled on 9/18/2012
Population: Appropriated Fund excluding employees in SES like pay plans
Key Leadership Position Initiative

- Directed by Sec 820 of PL 109-364 that requires “properly qualified” individuals in key positions on major defense acquisition programs
- Further implementation in USD(AT&L)’s 25 Aug 2010 memo, Government Performance of Critical Acquisition Functions
  - Identifies Program Lead Systems Engineer as a mandatory Key Leadership Position for all MDAP/MAIS programs (Acquisition Categories I and IA) when the function is required based on the phase or type of acquisition program
- Working with SPRDE FIPT on updating Systems Engineering competencies and determining Key Leadership Position characteristics

FIPT – Functional IPT
KLP – Key Leadership Position
SPRDE – Systems Planning, Research, Development and Engineering
Growing Great Engineers

• **Breadth**
  – Awareness of and appreciation for other functional areas
  – Understanding of system lifecycle and processes
  – Knowledge of other engineering disciplines and how they integrate into a system solution
  – Knowledge of product domains

• **Depth**
  – Extensive expertise and experience in one or more engineering disciplines and in one or more product domains

• **Leadership**
  – Ability to motivate and inspire individuals and teams
  – Comfort in dealing with complexity
  – Focus on underpinning decisions with data
  – Capability to make tough technical decisions
President’s Budget Request (PBR) 14 Impact on Federal STEM Education Programs

PBR Proposal:
End programs and shift resources to ED, NSF, and the Smithsonian, directed at 4 clear priorities.

FY 12 STEM Efforts

78 Different Programs
9 Agencies
$176.4 M

Department of Education
$100.3 M
Improve K-12 instruction

National Science Foundation (NSF)
$51.1 M
STEM undergraduate education and national strategy for fellowships

Smithsonian
$25.0 M
Develop infrastructure to support STEM instruction and engagement
SEC. 862. ENCOURAGEMENT OF CONTRACTOR SCIENCE, TECHNOLOGY, ENGINEERING, AND MATH (STEM) PROGRAMS.

(a) IN GENERAL.—The Under Secretary of Defense for Acquisition, Technology, and Logistics shall develop programs and incentives to ensure that Department of Defense contractors take appropriate steps to—

(1) enhance undergraduate, graduate, and doctoral programs in science, technology, engineering and math (in this section referred to as “STEM” disciplines);

(2) make investments, such as programming and curriculum development, in STEM programs within elementary and secondary schools;

(3) encourage employees to volunteer in Title I schools in order to enhance STEM education programs;

(4) make personnel available to advise and assist faculty at such colleges and universities in the performance of STEM research and disciplines critical to the functions of the Department of Defense;

(5) establish partnerships between the offeror and historically Black colleges and universities and minority institutions for the purpose of training students in scientific disciplines; or

(6) award scholarships and fellowships, and establish cooperative work-education programs in scientific disciplines; or

(7) conduct recruitment activities at historically black colleges and universities and other minority-serving institutions or offer internships or apprenticeships.

(b) IMPLEMENTATION.—Not later than 270 days after the date of the enactment of this Act, the Under Secretary shall submit to the congressional defense committees a report on the steps taken to implement the requirements of this section.
Summary

• FY13 continues to be shaped by budget uncertainty
• Criticality of our Systems Engineering mission work has grown
  – Our work will be even more essential in facing budget challenges
• We are making an impact
  – Strong support for System Engineering mission across the Department
• Dedicated, professional and committed SE staff
• Focused on working smarter, as a more tightly integrated team across OSD and the Services
  – Continue to make a difference for the warfighter and the taxpayer
Systems Engineering: Critical to Acquisition Success

Innovation, Speed, and Agility

http://www.acq.osd.mil/se