



DoD Systems Engineering Update

Mr. Nicholas Torelli
Director, Mission Assurance
Office of the Deputy Assistant Secretary of Defense for
Systems Engineering

RAM V
October 16, 2012



Agenda



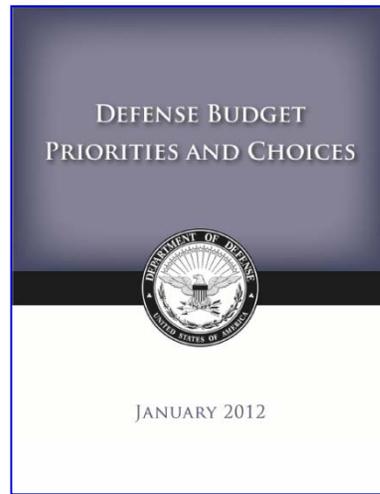
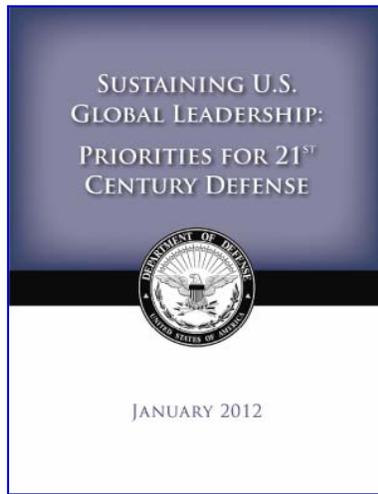
- **Discuss DASD(SE) efforts and mission**
- **Review key events and actions from the last year**
- **Q&A**



Some Context Up Front: Key Elements of Defense Strategic Guidance



- The military will be smaller and leaner, but it will be agile, flexible, ready and technologically advanced.
- Rebalance our global posture and presence to emphasize Asia-Pacific and the Middle East.
- Build innovative partnerships and strengthen key alliances and partnerships elsewhere in the world.
- Ensure that we can quickly confront and defeat aggression from any adversary – anytime, anywhere.
- Protect and prioritize key investments in technology and new capabilities, as well as our capacity to grow, adapt and mobilize as needed.





Department of Defense



Our Mission:

- Protect our National Security*
- Provide the military forces needed to deter war and prevail in conflict*

- Over 1.4 million active duty men and women*
- Over 1.1 million Guard & Reserves*
- Over 718,000 civilians*



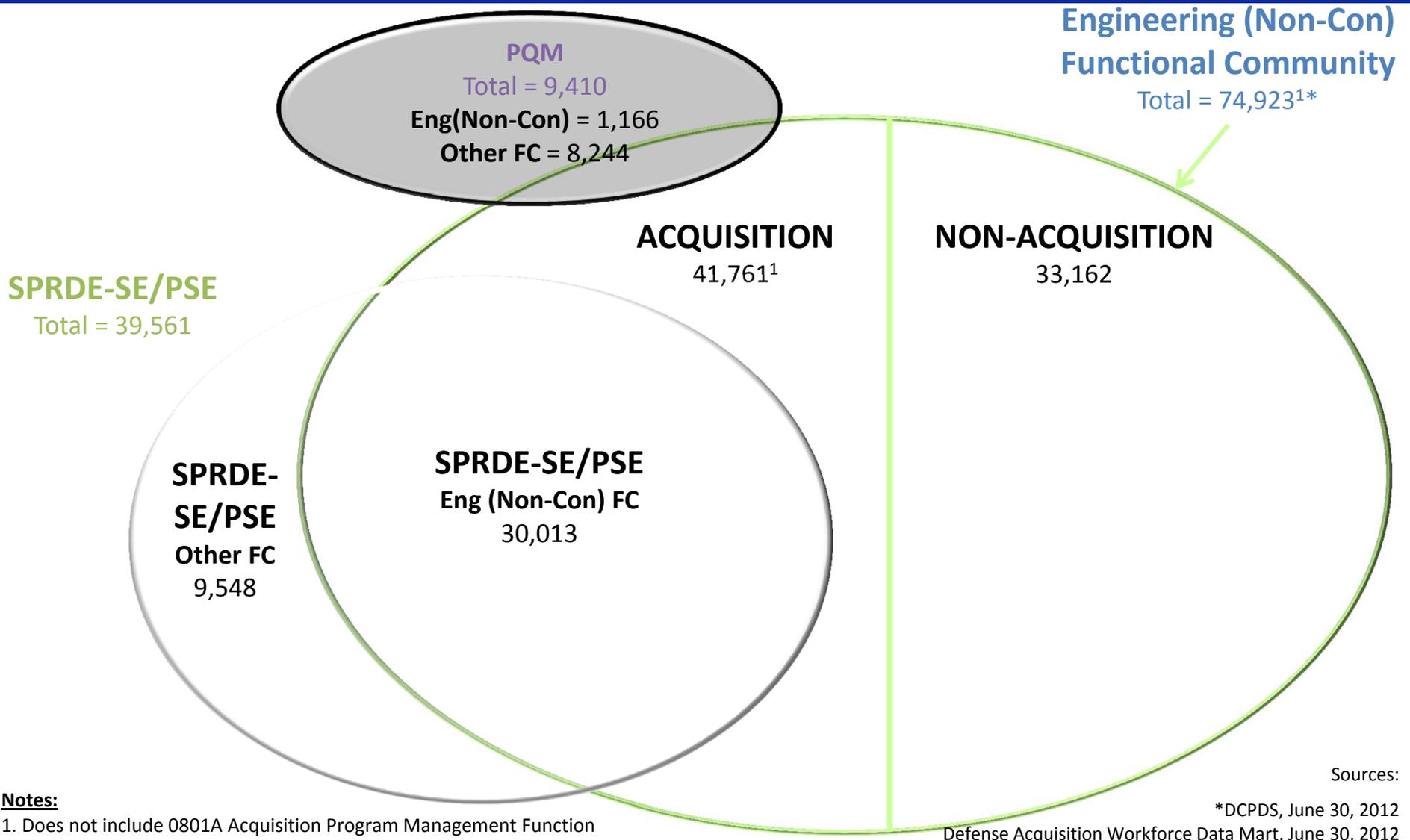
DoD Engineering Enterprise



- *World's Largest Engineering Organization*
- *Over 99,000 Uniformed and Civilian Engineers*
- *Over 39,000 Acquisition Corps Certified Systems Engineers (SPRDE)*



Engineering (Non-Construction) Functional Community Acquisition Engineers



Notes:

1. Does not include 0801A Acquisition Program Management Function

Sources:

*DCPDS, June 30, 2012

Defense Acquisition Workforce Data Mart, June 30, 2012



DASD (Systems Engineering) 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

We apply best engineering practices to:

- Support and advocate for DoD Component initiatives
- Help program managers identify and mitigate risks
- Shape technical planning and management
- Provide technical insight to OSD stakeholders
- Identify systemic issues for resolution above the program level





DASD, Systems Engineering




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 and Industry Engineering Research
- Modeling and Simulation
- Systems Engineering FFRDC Oversight



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 (HSI))
- 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



Program Engagement



- **Engineering Assessment / Mentoring of Major Defense Programs**
- **Technical Reviews**
- **AT&L Decision Forums**
- **Systems Engineering Plans**
- **Systemic Root Cause Analysis**
- **Support Acquisition Leadership with Independent Engineering Analysis and Advice**



Our Focus: Supporting Knowledge-Based Decision Making



Policy and Practice



- **Supporting the Current Practice**
 - Department-wide Systems Engineering Policy and Guidance
 - Specialty Engineering
 - System Safety, Reliability and Maintainability Engineering, Quality, Manufacturing, Producibility, Human Systems Integration

- **Addressing Emerging Challenges**
 - Complex Systems/Systems of Systems
 - Program Protection/Acquisition Cyber-Security
 - University and Industry Engineering Research
 - Modeling and Simulation Support to Acquisition
 - Systems Engineering Federally Funded R&D Centers (FFRDC) Oversight

Our Focus: Policy, People and Practice



DASD(SE) Top-Level FY12 Goals



Strengthen our *program engagement*, across full product spectrum, using expert technical teams to support informed, affordable decisions

- Increase early engagement in AoA's and RFPs
- Increase use of quantitative data (new SEP format) in program oversight
- Meet commitment to USD(AT&L) to comprehensively support PDR and CDR
- Maintain program support review tempo and quality while using less resources

Implement comprehensive *program protection planning*

- As a part of the trusted defense systems strategy

Implement clear, effective *reliability and manufacturing policy*

- Establish and promulgate guidance and support for these specialty disciplines

Conduct detailed review/update of *SPRDE curriculum*

- Dovetail into DAU statutory requirement to review Acquisition Curriculum

Assess and Strengthen *Workforce Systems Engineering Competencies*

Measure and improve Department-wide *Systems Engineering performance*

- Establish collection of performance metrics, benchmarking



DoDI 5134.16, Deputy Assistant Secretary of Defense for Systems Engineering



Implementing statutory authorities provided under WSARA:

- **Performing continuous technical engagement, oversight, and review of Service acquisition programs' SE and Development Planning capabilities**
 - Continuous engagement with Services' acquisition enterprises
 - Sharing best practices across the department
- **Directly advising USD(AT&L) on SE and Development Planning (including Defense Business Systems and National Intelligence Programs)**
 - Active participant in MDAP and MAIS major milestone decision making
- **Reviewing and approving MDAP and MAIS Systems Engineering Plans (SEPs)**
- **Developing SE, Development Planning, Manufacturing, and Reliability and Maintainability policy and guidance**
- **Influencing Pre-MDD and MS A activities (CAPE and JROC)**
- **Participating in AoA guidance development and study oversight**

<http://www.dtic.mil/whs/directives/corres/pdf/513416p.pdf>

WSARA – Weapon Systems Acquisition Reform Act of 2009



Annual Report to Congress



DEPARTMENT OF DEFENSE
Developmental Test and Evaluation
and Systems Engineering
FY 2011 Annual Report



MARCH 2012


Edward R. Greer
Deputy Assistant Secretary of Defense
Developmental Test and Evaluation


Stephen P. Welby
Deputy Assistant Secretary of Defense
Systems Engineering

Preparation of this report cost the Department of Defense a total of approximately \$959,000 in Fiscal Years 2011–2012.
Generated on 2012Mar19 1409 RefID: 9-37B8F44
WHS Report Control Symbol DD-AT&L(A)2258

- **FY2011 SE and DT&E Annual Report to Congress delivered to Congress and GAO on 6 April 2012**
- **Detailed review of DASD(SE) Accomplishments in FY11**
- **Review of FY11 Service progress and plans implementing WSARA to improve SE capabilities**
- **Overall SE Workforce review, including FY12 Budget Impacts on SE Workforce**
- **Detailed program by program SE assessments for 40+ MDAPs**



Defense Acquisition Guidebook

Chapter 4 (DAGC4) Rewrite



- Use a product-centered approach, where the product is the weapon system or capability under development
- Thread policy, activities/processes, and product together
Policy (Direction / Requirement) → Process (How) → Product (What)
- Do not restate policy, rather clarify intent of policy and identify expectations
- Do not invent guidance to fill a gap in policy and remove preferences
- Map to Services' practices
- Minimal links
- Reduce the overall page count
- Include the emerging acquisition models

Provide the thinnest layer of guidance to get the job done



New DAGC4 Framework



Overarching Themes:

- Provide balanced approach in delivering a capability to the war fighter
- Support program success through systematically increasing maturity and reducing risk over the acquisition lifecycle

1. Introduction (Overview)

- Systems Engineering Definition
- Why It's Important

2. Systems Engineering Activities in the Life Cycle

- By Phase Description of Key Activities
- Technical Reviews
- Emerging Acquisition Models

3. Systems Engineering Processes

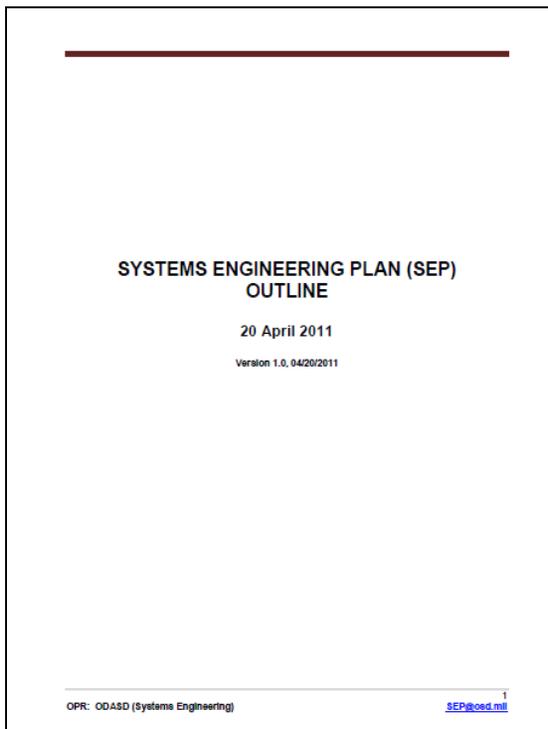
- Description of Each Process
- Design Considerations
- Specialty Engineering



Fully Implementing the 2011 Revised Systems Engineering Plan



- April 2011 SEP Outline directs programs to present their strategy for identifying, prioritizing, and selecting metrics for monitoring and tracking program SE activities and performance



- Provide an overview of measurement planning and metrics selection process
- Include approach to monitor execution-to-plan and identification of roles, responsibilities, and authorities
- Minimum set of TPMs and intermediate goals and plan to achieve them with as-of dates.
- Examples include TPMs in areas of software, reliability, manufacturing, integration, and test

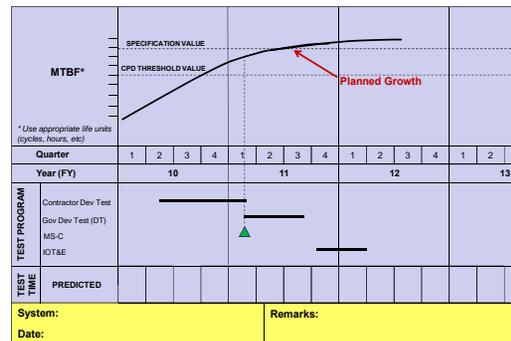


Figure 3.6-1 Reliability Growth Curve (sample)

Name	Spec	Status	Margin	Trend	S L
Aerodynamic drag (counts)	< 222	220	2.0		Y
Thermal utilization (kW)	< 60	55	5.0		G
Electrical power utilization (kVA)	< 201	123	78		G
Operating weight (lb)	< 99,000	97,001	1,999		G
Range (nmi)	> 1,000	1,111	111		G
Average flyaway unit cost (number)	< 1.5	1.3	0.20		G

Table 3.6-2 TPMs (sample)

Program will use metrics to measure progress.



Reliability and Maintainability DTM 11-003 Key Policy Attributes



- **Mandates specific reliability planning in the SEP and TEMP:**
 - Submission of a RAM-Cost Rationale Report (SEP)
 - Comprehensive R&M planning (SEP)
 - Reliability Growth Curves (SEP and TEMP)
- **Mandates identification of reliability contract requirements in the TDS and AS:**
 - Translation of AoA sustainment characteristics and Sustainment KPP thresholds into R&M design requirements and contract specifications
 - Identification of systematic processes that the contractor will be required to use to demonstrate achievement of these design requirements
- **Directs PMs and OTAs to assess the likelihood of reliability requirement achievement during IOTE and report this to the MDA at MS C**
- **Establishes specific reliability monitoring and reporting throughout the acquisition process as part of established technical reviews and assessments and in the DAES**



Major Initiatives: Increased Priority for Program Protection



- **Threat: Nation-state, terrorist, criminal, or rogue developer who:**
 - Gain control of systems through supply chain opportunities
 - Exploit vulnerabilities remotely
- **Vulnerabilities**
 - All systems, networks, and applications
 - Intentionally implanted logic
 - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- **Traditional Consequences: Loss of critical data and technology**
- **Emerging Consequences: Exploitation of manufacturing and supply chain**
- **Either can result in corruption; loss of confidence in critical warfighting capability**

Today's acquisition environment drives the increased emphasis:

<u>Then</u>		<u>Now</u>
Stand-alone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers
CPI (technologies)	>>>	CPI and critical components



Counterfeits Focus in FY12 National Defense Authorization Act (NDAA)



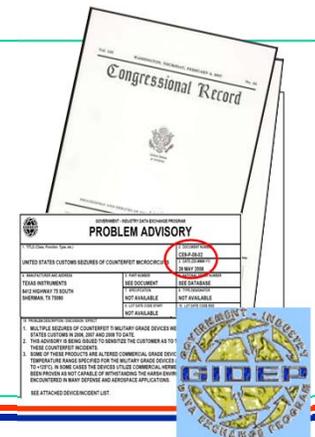
Focus—Detection and Avoidance of Counterfeit Electronic Parts

Tenets:

- Directs DoD to *assess current anti-counterfeiting practices* and implement “risk-based” policies to address counterfeit
- Requires DoD and contractors whenever possible to buy electronic parts from the Original Component Manufacturer (OCM) or its authorized distributor(s)
- Directs DoD to *establish a “Trusted Supplier” program* to certify organizations that comply with industry standards on anti-counterfeiting
- Institutes cost recovery for counterfeit items
- *Re-affirms mandatory reporting (GIDEP) for incidents internal and external to DoD*
- Requires the Secretary of Homeland Security to establish a methodology for the enhanced inspection of electronic parts after consulting with the Secretary of Defense as to the sources of counterfeit parts in the defense supply chain

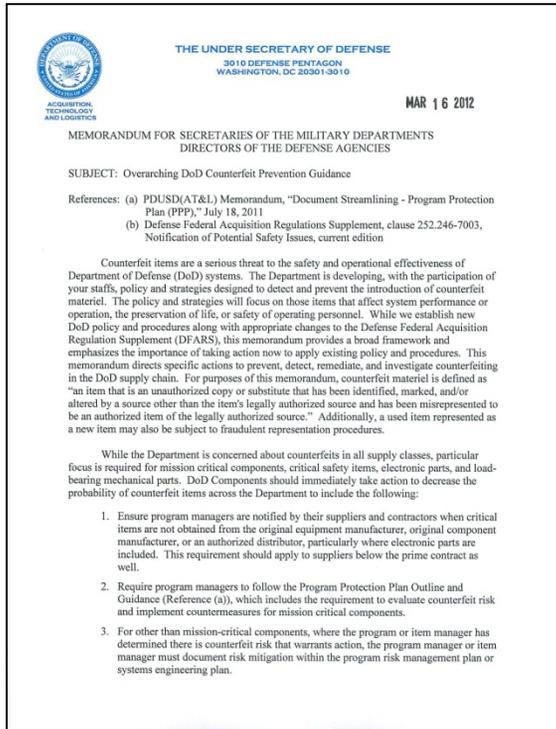
Specific Actions:

- *Establish DoD-wide definition*
- *Issue anti-counterfeit mitigation guidance*
- *Issue remedial action guidance*
- *Create reporting process (GIDEP)*
- *Develop process to analyze and act on reports*
- *Incorporate in DFAR anti-counterfeit language*





USD(AT&L) Memorandum: Overarching Anti-Counterfeit Prevention Guidance



THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

MAR 16 2012

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Overarching DoD Counterfeit Prevention Guidance

References: (a) PDUSD(AT&L) Memorandum, "Document Streamlining - Program Protection Plan (PPP)," July 18, 2011
(b) Defense Federal Acquisition Regulations Supplement, clause 252.246-7003, Notification of Potential Safety Issues, current edition

Counterfeit items are a serious threat to the safety and operational effectiveness of Department of Defense (DoD) systems. The Department is developing, with the participation of your staffs, policy and strategies designed to detect and prevent the introduction of counterfeit materiel. The policy and strategies will focus on those items that affect system performance or operation, the preservation of life, or safety of operating personnel. While we establish new DoD policy and procedures along with appropriate changes to the Defense Federal Acquisition Regulation Supplement (DFARS), this memorandum provides a broad framework and emphasizes the importance of taking action now to apply existing policy and procedures. This memorandum directs specific actions to prevent, detect, remediate, and investigate counterfeiting in the DoD supply chain. For purposes of this memorandum, counterfeit materiel is defined as "an item that is an unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source." Additionally, a used item represented as a new item may also be subject to fraudulent representation procedures.

While the Department is concerned about counterfeits in all supply classes, particular focus is required for mission critical components, critical safety items, electronic parts, and load-bearing mechanical parts. DoD Components should immediately take action to decrease the probability of counterfeit items across the Department to include the following:

1. Ensure program managers are notified by their suppliers and contractors when critical items are not obtained from the original equipment manufacturer, original component manufacturer, or an authorized distributor, particularly where electronic parts are included. This requirement should apply to suppliers below the prime contract as well.
2. Require program managers to follow the Program Protection Plan Outline and Guidance (Reference (a)), which includes the requirement to evaluate counterfeit risk and implement countermeasures for mission critical components.
3. For other than mission-critical components, where the program or item manager has determined there is counterfeit risk that warrants action, the program manager or item manager must document risk mitigation within the program risk management plan or systems engineering plan.

8 clause 252.246-7003, "Notification of potential safety issues for parts identified as critical safety items; subassemblies integral to a system; or overhaul services for systems and parts integral to a system. This clause covers non-conformances and deficiencies that could affect systems or subsystems, assemblies, or components. Follow the procedures at section 252.246-7003 for the handling of notifications of potential safety issues."

Identify appropriate industry standards for parts and components used in contracting requirements as well as requirements flow down to appropriate suppliers.

Identify parts for items not received from an original manufacturer, or authorized distributor to assess counterfeit potential. These requirements apply to suppliers below the prime contract. Report suspected or confirmed counterfeit items to the Industry Data Exchange Program (GIDEP) reporting repository.

8. Report suspected or confirmed counterfeit items discovered by DoD activities in GIDEP using the Product Quality Deficiency Reporting process as appropriate.
9. Investigate suspected counterfeit incidents discovered or reported, and report incidents confirmed as counterfeit to the appropriate criminal authorities. In the case of suspected counterfeits, the parts should be held until resolution of the potential non-conformance is complete. If items are confirmed to be counterfeit, they should not be returned to the actual or a potential supplier at any time prior to criminal authorities' release for disposition.
10. Develop and provide training to DoD personnel involved with the development, acquisition and procurement, supply, maintenance, and protection of weapon systems on proper measures to address counterfeiting.

Your support in this critical area will ensure the safety and mission performance of our warfighting systems. My point of contact is Mr. Gerry Brown, ODASD(SCI), at 571-372-5259.

Frank Kendall
Acting

- Addresses an area of critical concern while Department policy is in coordination
- Provides definition
- Emphasizes
 - Risk-based approach
 - Leverages Program Protection Plan and non-conforming processes
 - Directs use of existing contracting clauses and data elements to ensure traceability and reporting on critical items for contractors and subcontractors
 - Use of anti-counterfeiting standards
 - Disposal of counterfeit items
 - Training



Reporting and Information Sharing



- **GIDEP (Government-Industry Data Exchange Program) is the official repository connecting Government, Industry, Law Enforcement (internal and external) for counterfeit data**
- **Weapon System Managers and FMS program offices are responsible for sharing counterfeit information with affected customer countries**
- **International Traffic in Arms Regulations (ITAR) exemption required for partner country GIDEP access**
- **Official country requests to US State Department can influence potential change to GIDEP data access limitations**





Standards



- **Defense Standardization Council (DSC) recognized that enterprise-wide approaches were needed for certain systems engineering disciplines**
- **DSC directed the Defense Standardization Program Office (DSPO) to form working groups to assess existing systems engineering technical documentation, identify requirements gaps, and make recommendations**
- **Working groups focused on standards for specific areas:**
 - Systems Engineering and Technical Reviews and Audits
 - Configuration Management
 - Manufacturing and Quality
 - Logistics Support Analysis



DoD Workforce Development



- **Contributing to the DoD Strategic Workforce Plan in support of DASD(SE)'s responsibility for the Engineering (non-construction) Functional Community Manager**
- **Managing Service and Agency Personnel as part of the SPRDE-SE/SPRDE-PSE and PQM Acquisition Workforce**
- **Refining Key Leadership Position (KLP) competency and experience requirements for Lead Systems Engineer**
- **Participating with the Systems Engineering Research Center (SERC) on several personnel-related research topics**
- **Supporting DoD STEM (Science, Technology, Engineering and Mathematics) Executive Board**



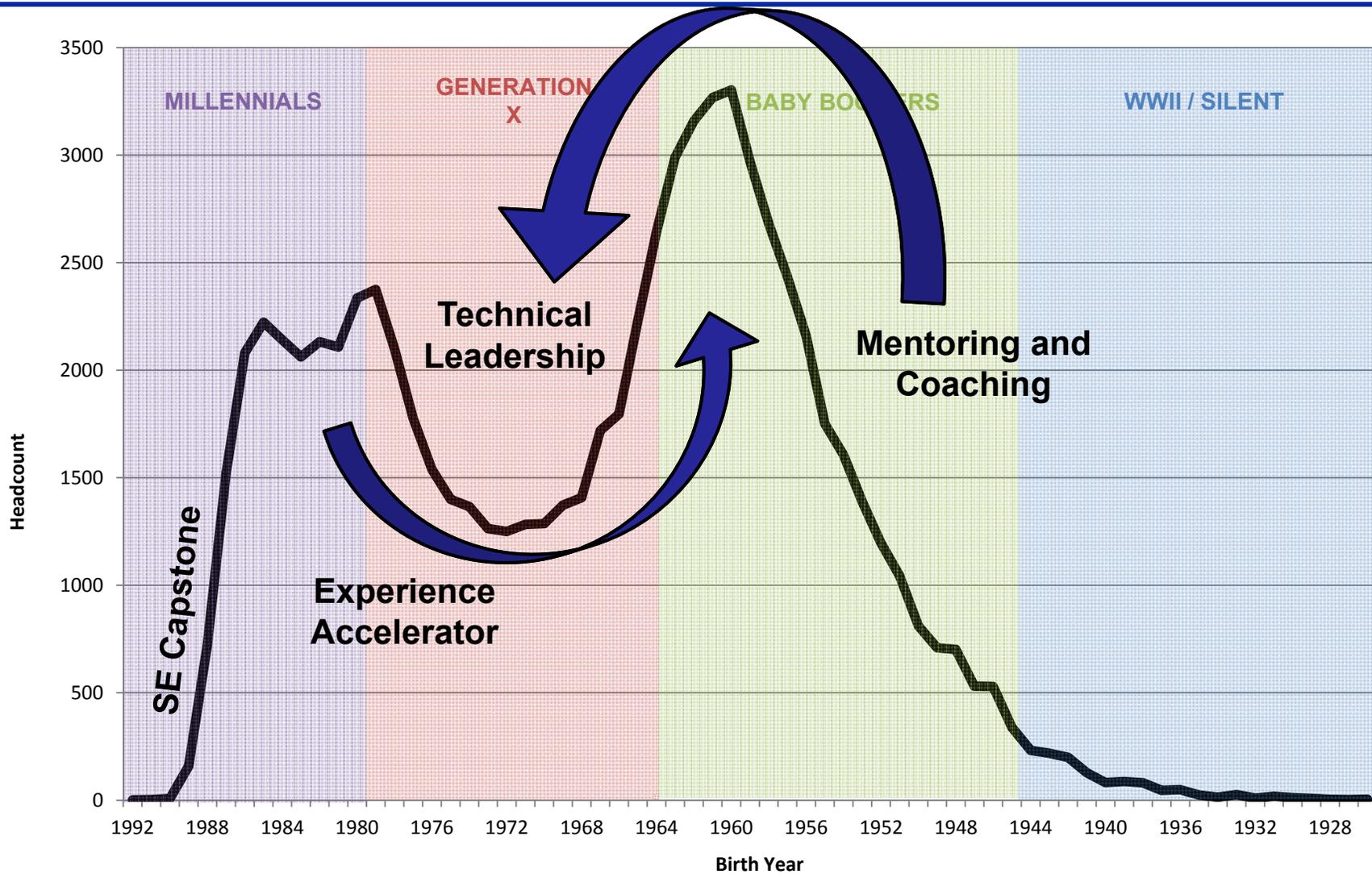
Growing Great Engineers



- **Depth**
 - Extensive expertise and experiences in one or more engineering disciplines and in one or more product domains
- **Breadth**
 - Awareness of and appreciation for other functional areas
 - Understanding of system life cycle and processes
 - Knowledge of other engineering disciplines and how they integrate into a system solution
 - Knowledge of 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



Engineering Challenges

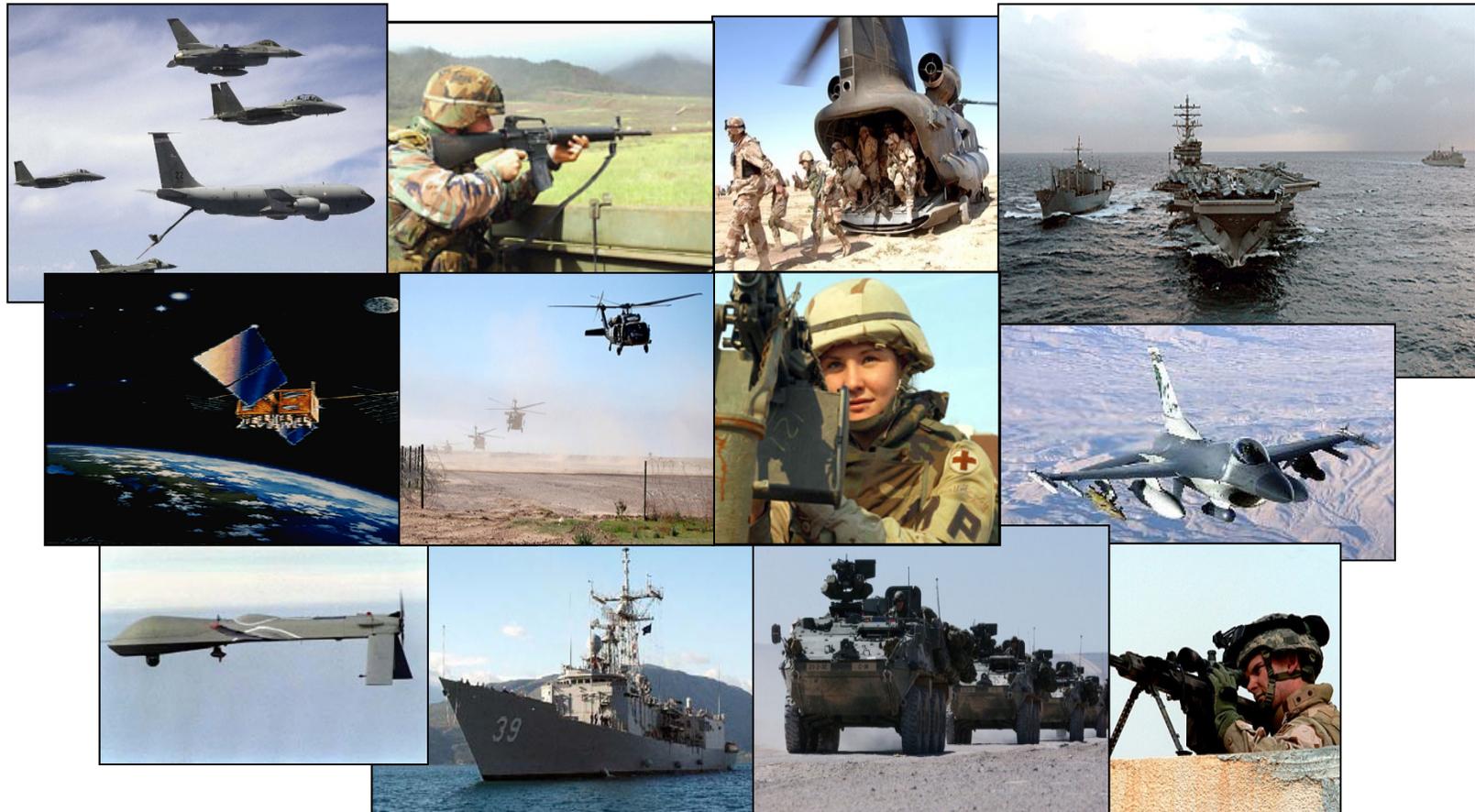


Source: AT&L Acquisition Workforce DataMart, Dec 2011

*Excluded: 222 personnel with unknown Birth Year



Systems Engineering: Critical to Program Success



Innovation, Speed, and Agility

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