



DMSMS in DoD Acquisition: Opportunities and Challenges

Mr. Stephen P. Welby

**Deputy Assistant Secretary of Defense
for Systems Engineering (DASD(SE)), OUSD(AT&L)**

**Diminishing Manufacturing Sources and Material Shortages
(DMSMS) 2013 Conference**



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

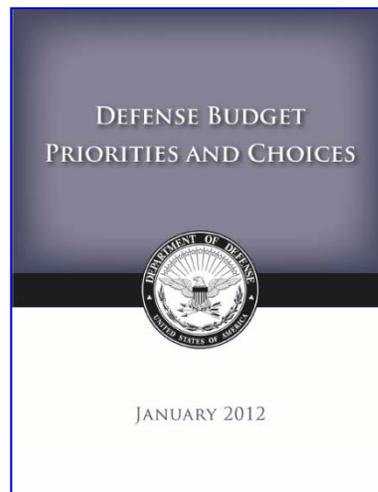
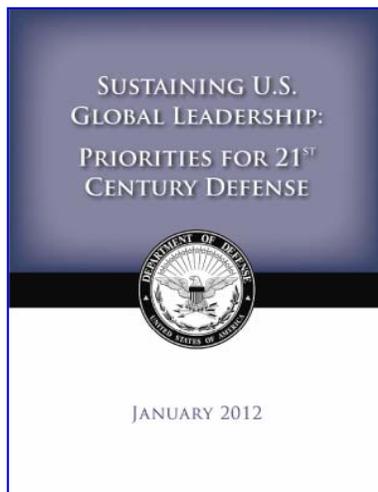
- ***US Department of Defense is the World's Largest Engineering Organization***
- ***Over 99,000 Uniformed and Civilian Engineers***
- ***Over 39,000 in the Engineering (ENG) Acquisition Workforce***



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 regions.
- 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.





2013 DoD Leadership Focus: Challenges, Choices, Opportunities



Chuck Hagel
24th Secretary of Defense

- The challenges posed by a changing strategic landscape and new budget constraints;
- The choices we have in responding to these challenges; and
- The opportunities that exist to fundamentally reshape the defense enterprise to better reflect 21st century realities.



Current DMSMS Challenges



- **Likely impact of current fiscal environment:**
 - Fewer new-start development programs
 - More Service Life Extension Programs (SLEP)
- **Accelerating technology life cycles means fewer sources for “pin-compatible” replacement parts**
- **Driving SLEP cost and risk:**
 - Loss of OEM sources
 - Obsolete parts
 - Loss of component pedigree
 - Loss of key manufacturing expertise

DMSMS - Diminishing Manufacturing Sources and Material Shortages



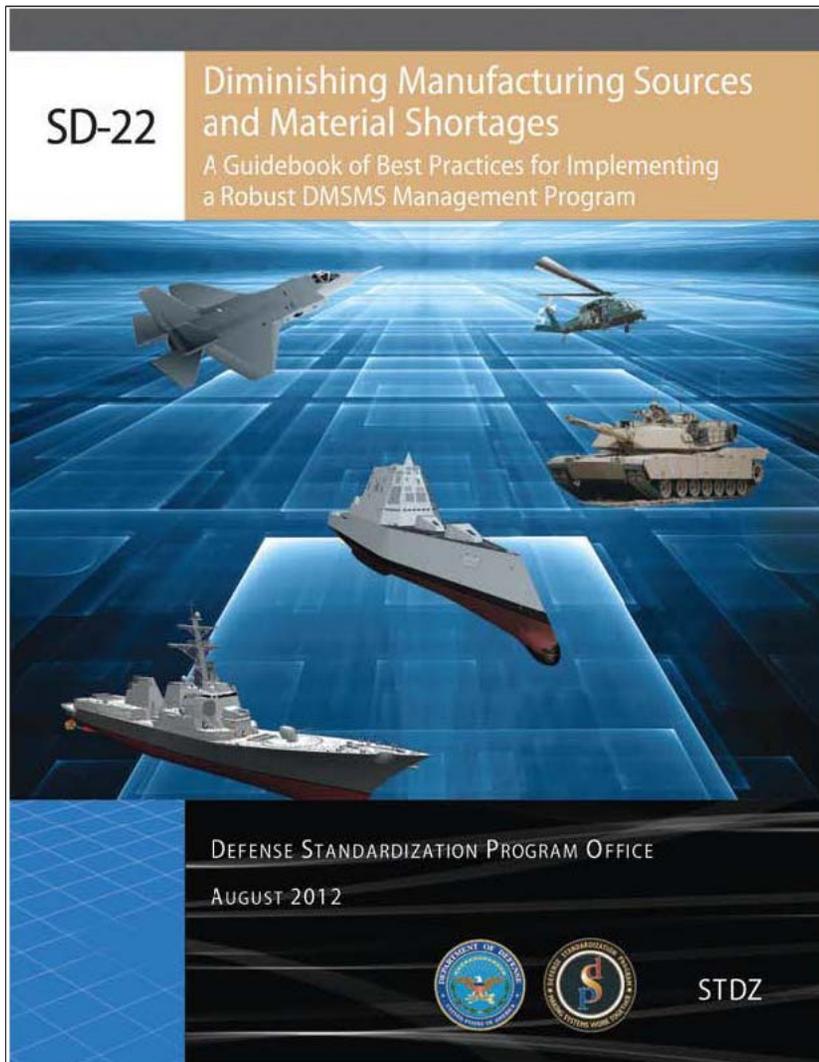
DMSMS Program Strategy



- **Eliminate DMSMS-related production schedule impacts**
 - **Eliminate DMSMS-related degradations to readiness**
 - **Minimize the scope of DMSMS-driven out-of-cycle redesigns when they cannot be completely eliminated**
- ... in a cost effective manner consistent with Better Buying Power (BBP) 2.0 initiatives**



DMSMS Planning



- **DMSMS Considerations in Design**
 - Are we appropriately trading DMSMS concerns with other design considerations?
 - Are DMSMS management activities during O&S adequately considered in upfront design activities?
 - Are DMSMS considerations adequately covered in technical reviews and engineering plans?
- **Potential design concepts to minimize DMSMS risk**
 - Technology and component selection
 - Parts management
 - Use of COTS assemblies
 - Open systems design



Resilient Design

- **The only constant for DoD systems is change:**
 - Evolving threats
 - Strategic and Tactical Innovation
 - Rapid technological change
 - Increased Defense leverage of commercial systems
 - Resource and demand uncertainty
- **These factors all demand increased resilience – the ability to explicitly design military systems to have capacity to adapt and adjust to maintain relevance and operational advantage in an environment of change**

**One method to address obsolescence risk during design is
Open System Architecture**



Defining Open Systems Architecture



What: *A technical architecture that leverages technical standards to support a modular, loosely coupled and highly cohesive system structure*

How: *Customer definition and ownership of product architecture; publication of key interfaces within the system*

Why: *Enables Open, Competitive Business Model – allowing components to be added, modified, replaced, removed or supported by different vendors throughout the life cycle – driving opportunities to enhance competition and innovation*



DoD Interest in Open Systems Architecture



- **Drives risk-prudent competition**
- **Enables Business Architectures that mirror Technical Architectures**
- **Provides a constant battle rhythm of competition**
- **Levels playing field; reduces barriers to market entry**
- **Addresses obsolescence risk**
- **Promises wider access to innovation**



Leveraging Open Systems to Address DMSMS



Establish an Environment for Change

- Be clear about intent to compete/recompete
- Establish a flexible contracting approach
- Incentivize good behavior among contributing contractors

Focus Systems Engineering for Openness

- Develop common architectures across a product line or across related product families
- Functionally decompose legacy capabilities



Leverage and Exercise Data Rights

- Assess current and needed data rights
- Be a better customer: confirm that data rights restrictions are correct and assert data rights
- Use government purpose rights (GPR) for next competition

Explore Business Architectures and Sound Competition Approaches

- Create alternatives
- Inject OSA through technical insertions
- Consider alternative integrations concepts
- Insure incentives align with desired behaviors
- Reward reuse



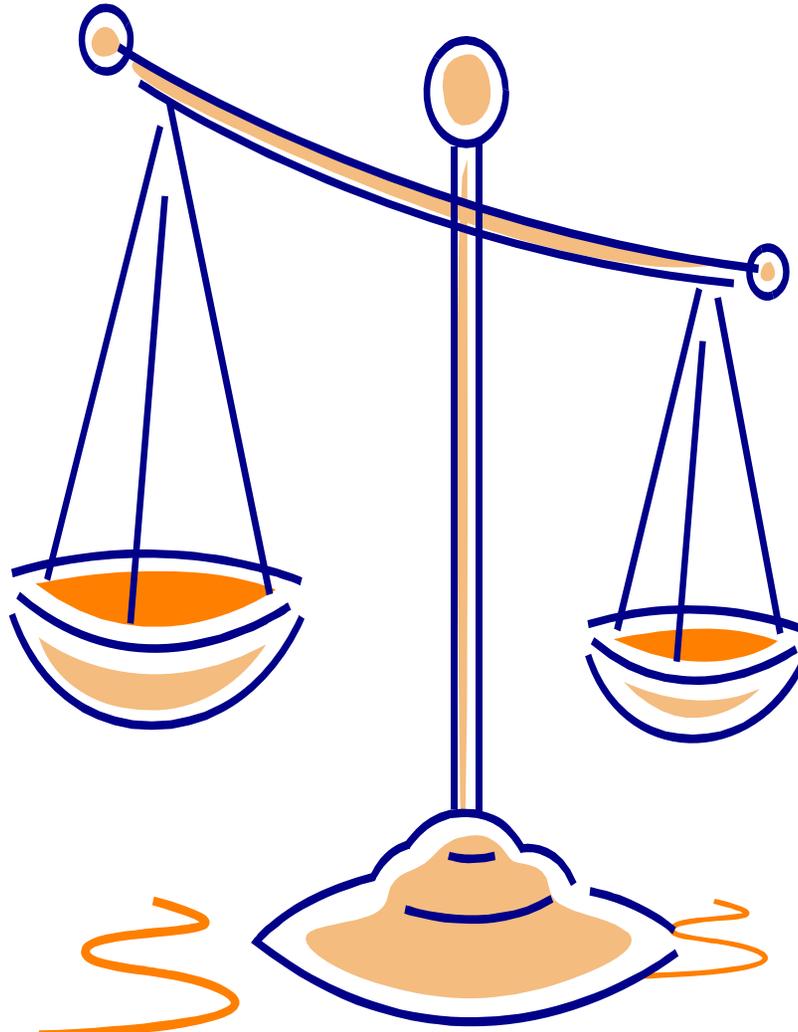
Technical Data, Computer Software, and Intellectual Property Rights



- **Data rights are considered up-front when developing an acquisition strategy; if critical data and software are not be specified for delivery, they may be unavailable (or unaffordable) years later for use on a program during its sustainment phase.**
- **Some Technical Data Rights Strategy considerations:**
 - Data deliverables included in the RFPs and subsequent contracts
 - Data rights, including the responses to the contractor's data assertion lists
 - Data management approach including how the data will be delivered, accessed, maintained, and protected



Balancing Goals



Customer

- Cost of Data Rights
- Typical Engineering Deliverables

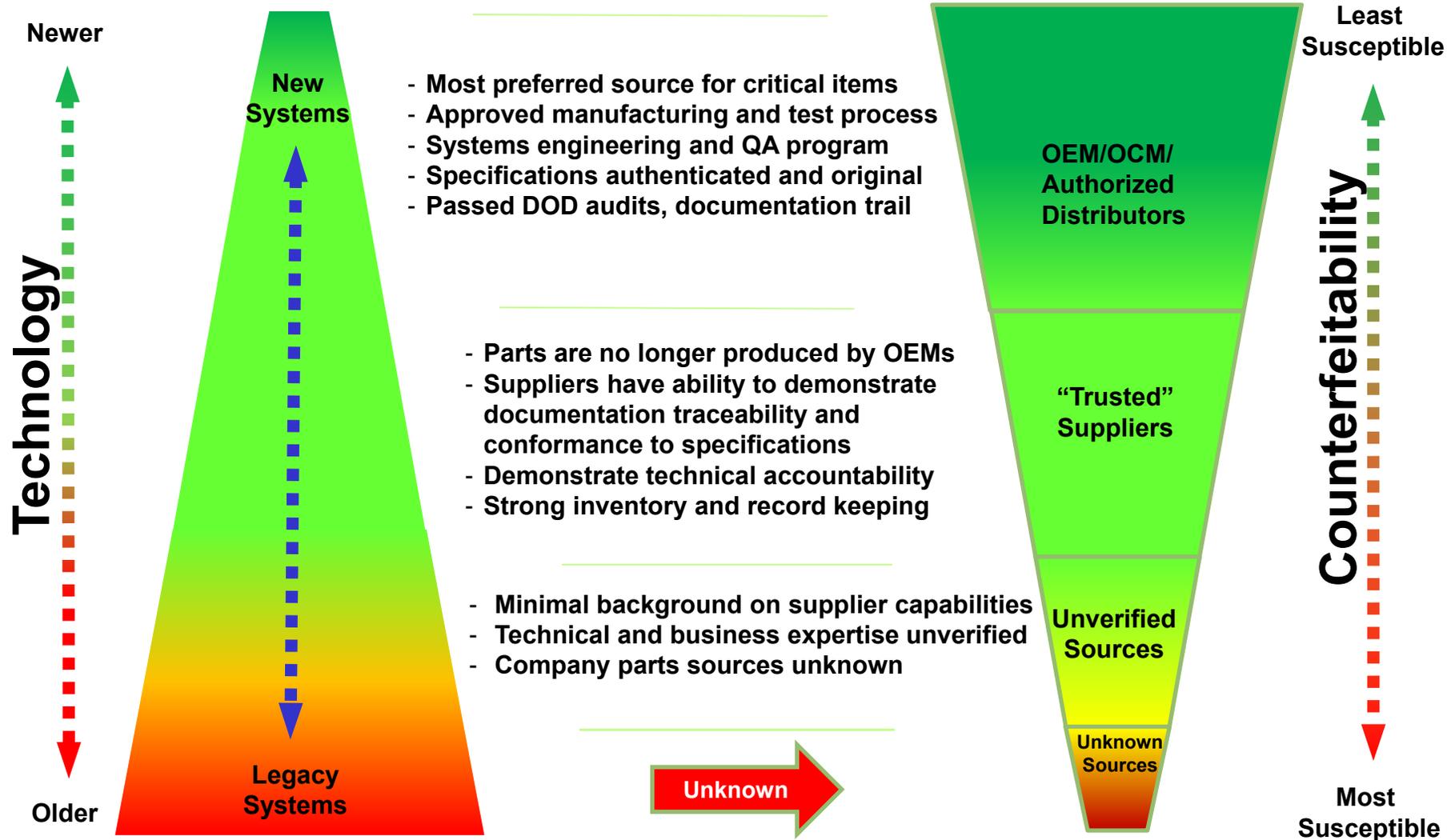
Vendor

- Competitive Advantage
- Financial Return on Research Investment

DMSMS considerations during design must be driven by a value-focused business case.



Profile of Counterfeit Risk



Prolonged use of aging systems creates opportunities for counterfeit parts to enter the supply chain



DoD Counterfeit Prevention Policy (DoDI 4140.67)

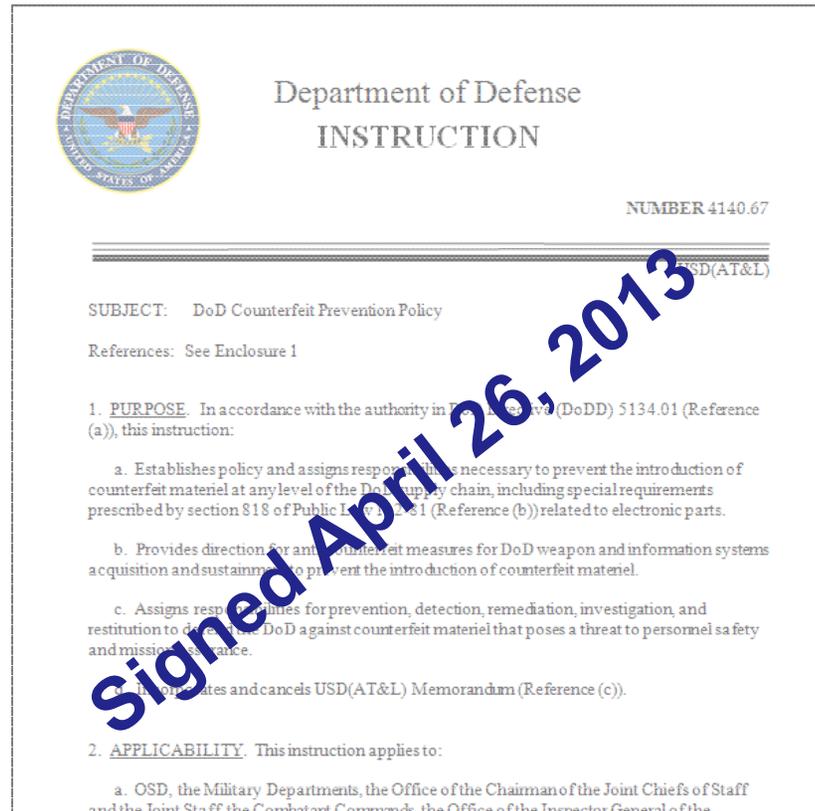


Purpose:

- Establishes policy
- Assigns responsibilities
- Provides definitions

It is DoD Policy to:

- Employ a risk-based approach
- Apply early prevention and detection procedures
- Document all occurrences in GIDEP
- Notify criminal investigative organizations
- Seek restitution when confirmed
- Provide education and training



Counterfeit Materiel Defined as:

“An item that is an unauthorized copy or substitute that has been identified, marked, 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.”

<http://www.dtic.mil/whs/directives/corres/pdf/414067p.pdf>

Responsibilities:

ASD(L&MR):

- Principal point of contact for anti-counterfeit improvements

ASD(R&E):

- Risk-based procedures to identify critical materiel
- Quality assurance policy
- Supplier qualification criteria
- GIDEP management

DPAP

- Procurement policies

DoD Components

- Identify critical materiel
- Procure from suppliers meeting appropriate criteria
- Conduct materiel testing
- Report in Government – Industry Data Exchange Program (GIDEP)



Proposed Acquisition Rule Changes

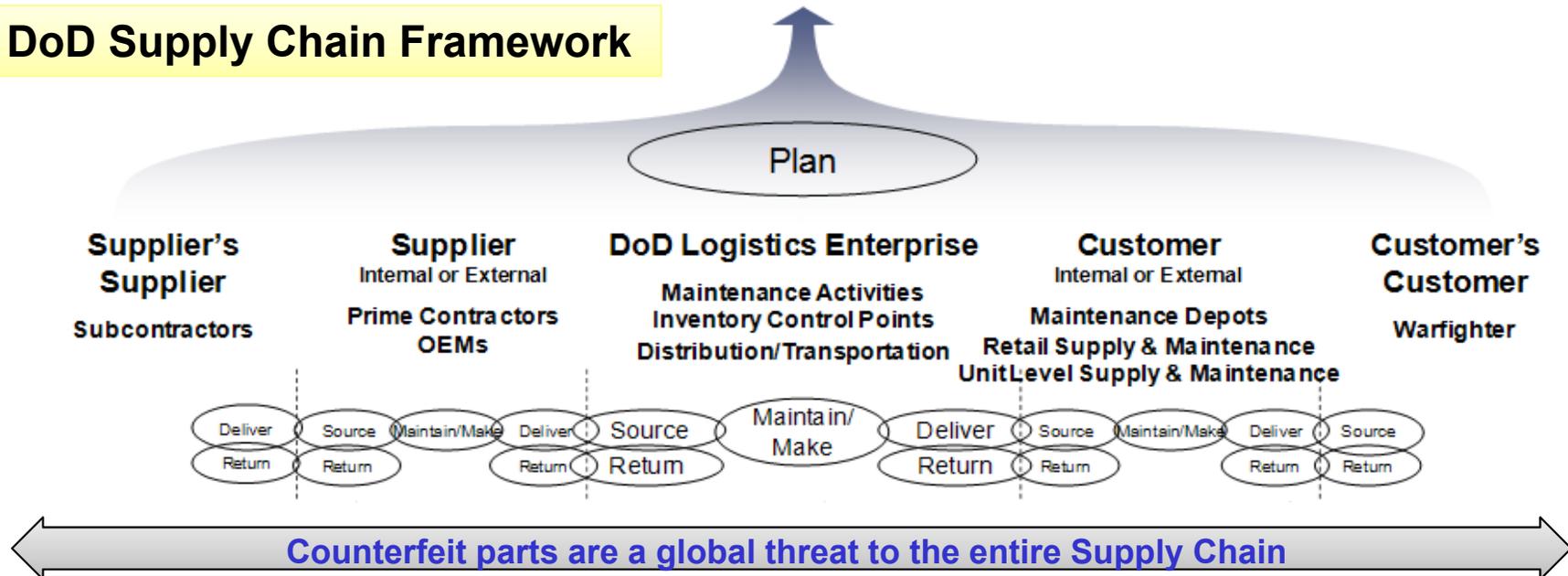


- **DFARS case (2012-D055) “Detection and Avoidance of Counterfeit Electronic Parts”**
 - Implements provisions of FY12 NDAA §818 to (a) add definitions specific to counterfeit parts, (b) define contractors' responsibilities, and (c) clarify the Government's role.
 - Implements FY13 NDAA §833 regarding allowability.
 - Anticipate publication as a final rule in 2014.
- **FAR case (2013-002) “Expanded Reporting of Non-conforming Items”**
 - Expands Government and contractor requirements for reporting of non-conforming supplies. Partial implementation of FY12 NDAA §818.
 - Anticipate publication as a proposed rule in 2014.
- **FAR case (2012-032), “Higher Level Contract Quality Requirements”**
 - Revises acquisition planning and quality assurance requirements to ensure the performance of higher level quality assurance for critical items.
 - Anticipate publication as a proposed rule in the next few months.



Supply Chain Implications

DoD Supply Chain Framework



Anti-Counterfeit Touch Points

- Plan: Collaboration with Trusted Suppliers
- Source: Reaches all levels of the supply chain
- Make: Demands traceability of all critical parts
- Deliver: Standards and practice
- Return: Prevent counterfeit reentry into the supply chain



Reporting and Information Sharing



- **Government – Industry Data Exchange Program (GIDEP) is the official repository connecting Government, Industry, Law Enforcement (internal and external) for counterfeit data.**
- **Weapon System Managers and Foreign Military Sales program offices are responsible for sharing counterfeit information with affected customer countries.**
- **International Traffic in Arms Regulations (ITAR) exemptions are required for partner country GIDEP access.**





Defense Standardization Update



- **Defense Standardization Council identified key, initial areas where standards are needed to restore discipline and consistency**
- **Focus is on supporting Department needs by leveraging voluntary consensus standards**
- **Future focus: Identifying key areas where additional standards can drive acquisition effectiveness and efficiency**



Challenges to the DoD Engineering Enterprise



- Lay solid foundations...create opportunities
- Envision multiple futures...enable flexible choices
- Design and build systems with focus on lifecycle cost
- Protect our critical defense “intellectual property”
- Focus on “**3 Ps**” of the DoD Engineering Enterprise: **Policy, Practice and, most importantly, People**



Systems Engineering: Critical to Defense Acquisition



Innovation, Speed, Agility
<http://www.acq.osd.mil/se>