

# DoD Counterfeit Mitigation Update



Presented to: PSMC's Spring Meeting, Apr 24, 2012

OUSD/AT&L  
Defense Procurement & Acquisition Policy

# Today's Objectives

- Discuss Federal Government anti-counterfeit approach
- Discuss DoD specific implementation
- Discuss how Automatic Identification Technologies and Information Technology can provide accurate traceability

# Challenges in Anti-Counterfeiting

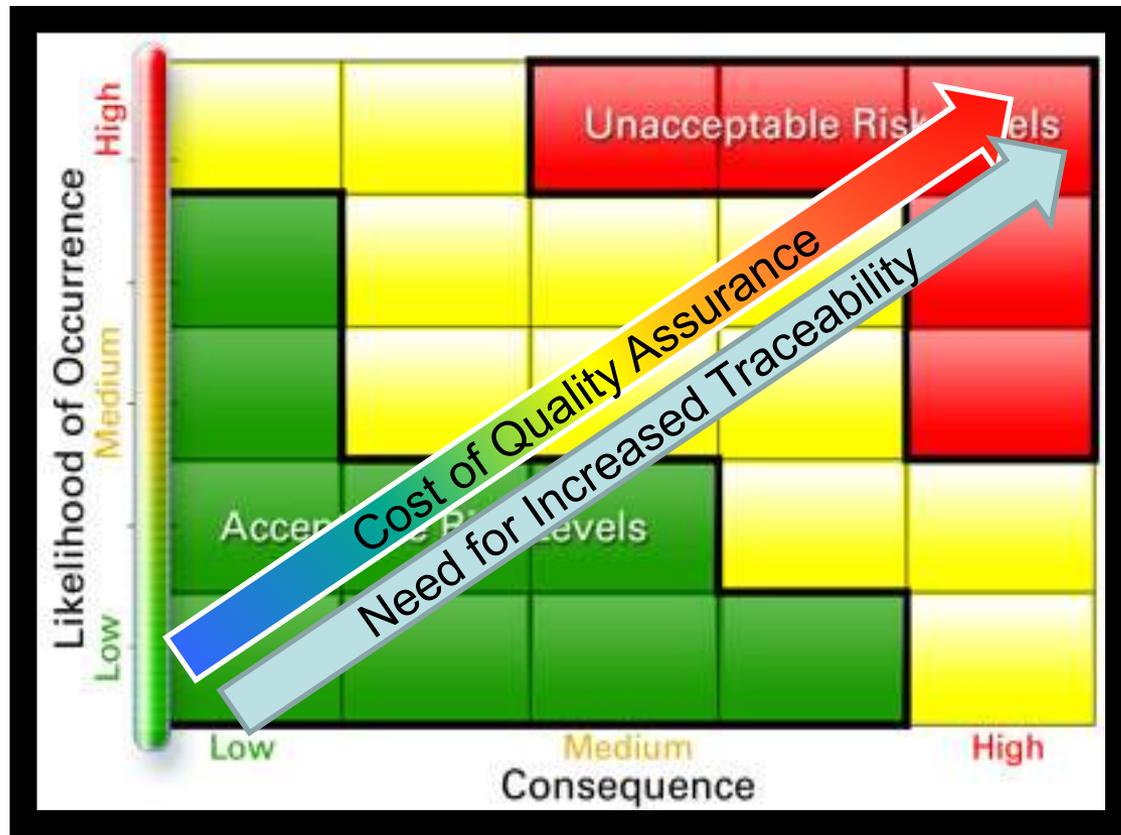
- Risk assessment is a key process to determine where to apply efforts to identify and stop counterfeiting of items.
- Terminology is a challenge and must be commonly applied through standards.
- How do we enhance quality assurance requirements based on risk?
- Relationships between Prime Contractors and Sub-Contractors (including small businesses) are key to the success of identification of suspect and confirmed counterfeit items.
- What about the commercial item conundrum?
- Who is ultimately responsible for the counterfeit item and what is their exposure?
  - Customer?
  - Prime Contractor?
  - Subcontractor?

# Federal Effort Involving AT&L

- Government-Wide Anti-Counterfeiting Working Group
  - Convened by OMB Intellectual Property Enforcement Coordinator (IPEC) to recommend common Federal approach with NASA, DoD and GSA as tri-chairs
    - US DoD Co-Chair
      - US DoD Working Group
        - Regulation
        - Risk Management
        - Traceability/identification/reporting
  - Established objectives and published objectives in Feb 2011 in IPEC Annual Report
  - Final Report in OMB Clearance – Publication April/May?

# Foundational Principle: “Identify Counterfeit Risk and Manage It”

- Risk Management is Part of Program Management
- Counterfeiting Is One Of Many Program Risks



# Traceability and Reporting

- Aren't there current processes and procedures that provide some traceability?
  - Product Lifecycle Management (PLM)
  - Government and Industry Data Exchange Program (GIDEP)
  - Product Data Reporting and Evaluation Program (PDREP)
  - Item Unique Identification (IUID)
- What is the level of tolerance of counterfeit items. What is the standard? What is acceptable?
- Can't Industry police itself and develop/leverage QA controls to meet a specified level of traceability.
  - Lacking a standards-based approach requirements customer demands would be unique to the customer
  - If left to the company each would develop their own procedures
  - How would the customer select among disparate approaches?

# Tailoring Traceability Based on Risk at the Item Level by Program

Likelihood	Near Certainty ~90%	Certificate of Authenticity ●	Process Audit/Review ●	Auditable Part History ●	Legally Authorized Source ●	Legally Authorized Source
	Highly Likely ~70%	Receipt Visual Inspection	Process Audit/Review ●	Verification Testing ●	Legally Authorized Source	Legally Authorized Source
	Likely ~50%	●	Receipt Visual Inspection ●	Authorized Supplier	Authorized Supplier ●	Auditable Part History
	Low Likelihood ~30%	● ●		Certificate of Authenticity	Verification Testing ●	Verification Testing
	Not Likely ~10%	● ●		Receipt Visual Inspection ●	Certificate of Authenticity ●	Certificate of Authenticity
	<b>Risk Categories:</b>	Negligible	Minor	Moderate	Serious	Critical
Impact of Non-Mitigated Counterfeit Item						

● Item Risk Mapped

High
  Medium
  Low

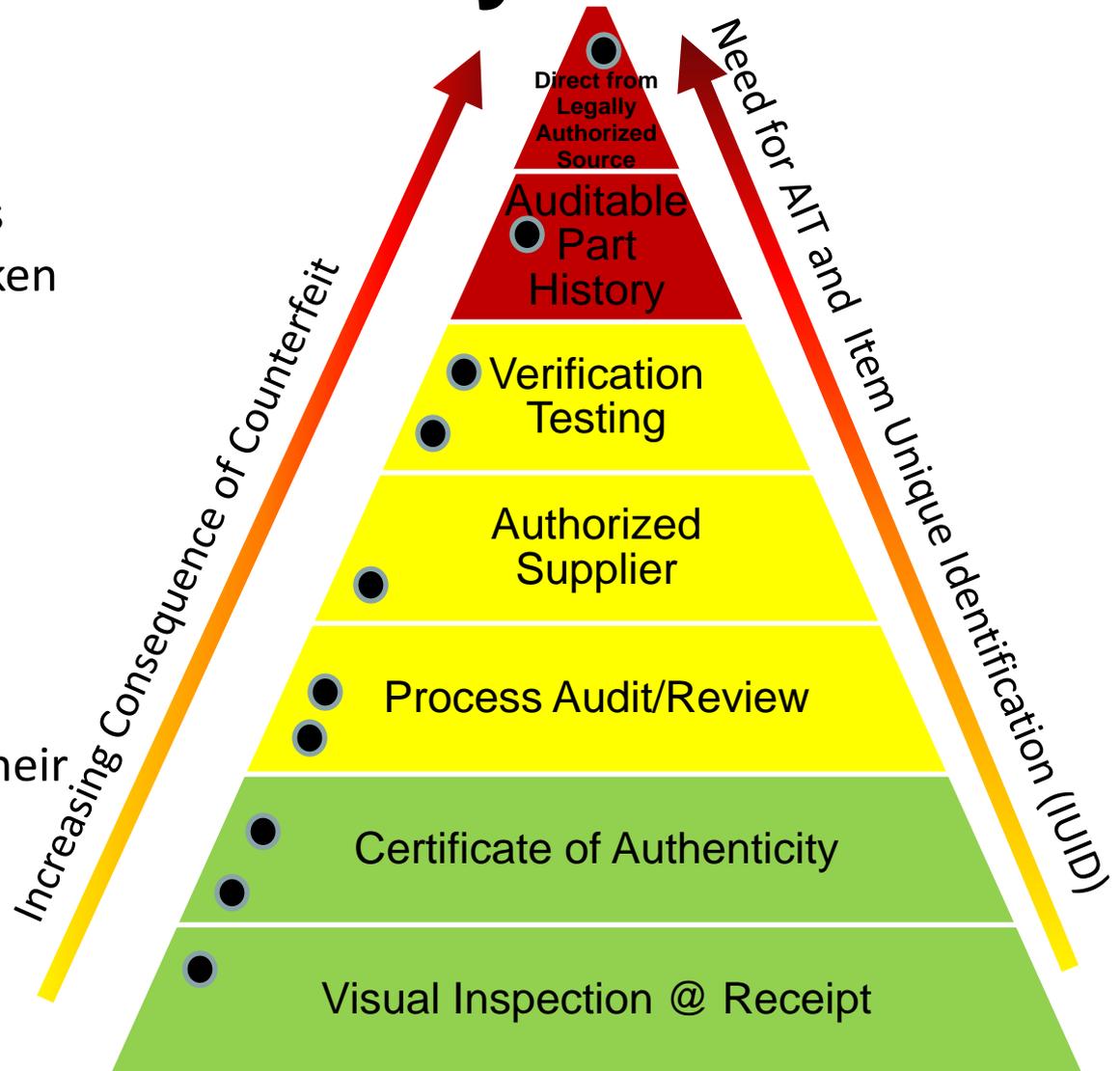
Reference: Risk Management Guide For DoD Acquisition, Sixth Edition (Version 1.0), August 2006

# Traceability Hierarchy

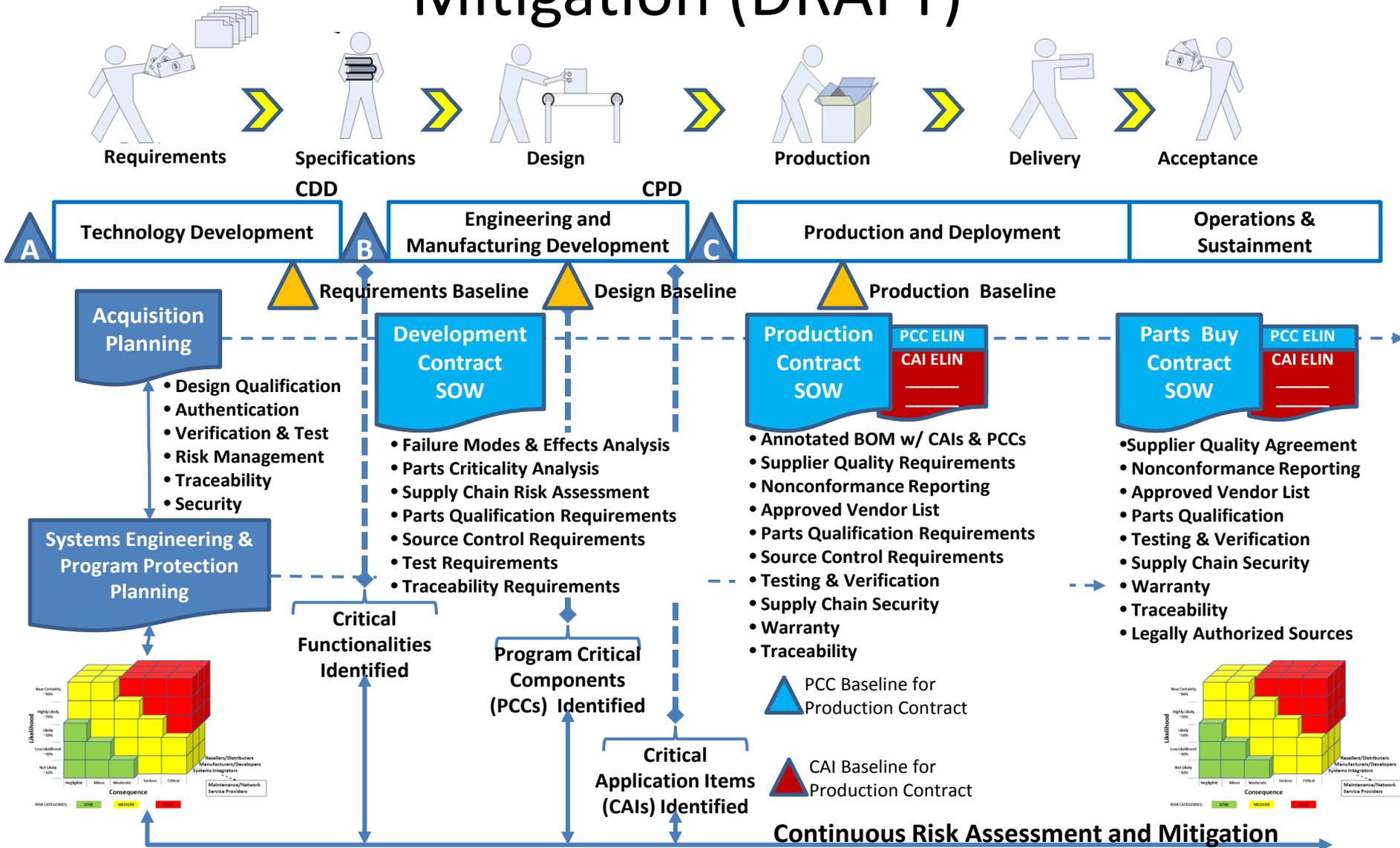
As the risk of Counterfeiting increases along with the consequence – more rigorous countermeasures must be taken throughout the supply chain.

Based on the Program/Item Management designation of “Susceptibility to Counterfeiting” – additional traceability measures will be required of contractors and their suppliers as shown in this diagram.

● Item Risk Mapped to Traceability Level



# Lifecycle Acquisition Counterfeiting Risk Mitigation (DRAFT)



# Jan 2010 Dept of Commerce Report

Focus—Defense electronics industrial base

## Findings:

- Supply Chain directly impacted by counterfeit electronics
- Lack of dialogue between all organizations in US supply chain
- Lack of traceability/insufficient accountability
- Limited recordkeeping on counterfeit incidents
- Need stricter testing protocols and quality control practices for inventory
- Most organizations don't know who to contact in the government on counterfeit
- Little policy in place to prevent counterfeit parts from infiltrating their supply chain

## Recommendations:

- Provide clear, written guidance on counterfeit parts
- Implement stricter testing protocols/quality control processes
- Establish procedures for detecting and reporting counterfeits
- Establish trusted supplier lists
- Modify contract requirements
- Maintain database

# March 2010 GAO Report



Focus—Defense supplier base, counterfeit parts

## Findings:

- No Department-wide definition of counterfeit
- No current policy or specific processes for detecting and preventing counterfeit parts
- Limited procurement and quality control practices to prevent and detect counterfeit parts
- No databases to track and report counterfeit parts

## Recommendations:

- Create consistent definition of counterfeit parts
- Establish and disseminate guidance/policy on counterfeit to all DOD components and defense contractors
- Establish consistent practices for preventing, detecting, reporting, and disposing of counterfeit parts
- Leverage existing DOD components and industry anti-counterfeit initiatives and practices
- Analyze the knowledge and data collected to best target and refine counterfeit-part risk-mitigation strategies

# FY2012 NDAA Section 818

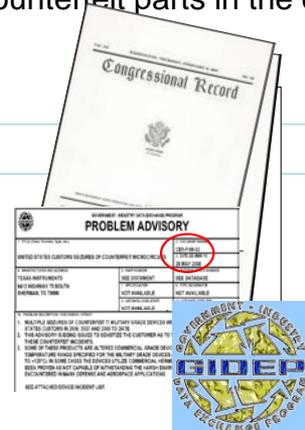
Focus—Detection and Avoidance of Counterfeit Electronic Parts

Tenets:

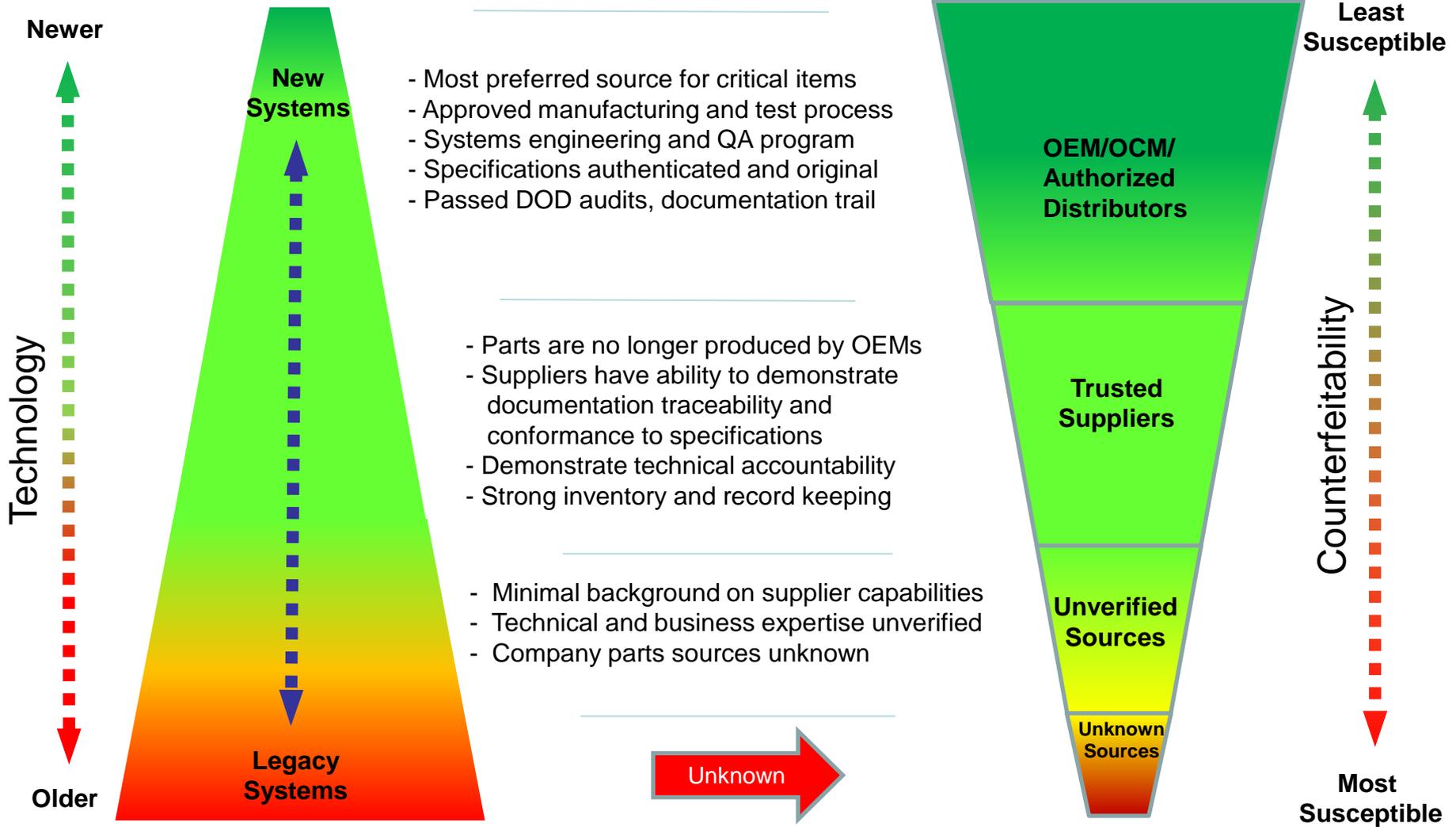
- Directs DOD to assess current anti-counterfeiting practices and implement “risk-based” policies to address counterfeit
- Requires DOD and contractors whenever possible to buy electronic parts from the Original Component Manufacturer (OCM) or its authorized distributor(s)
- Directs DOD to establish 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



# Profile of Counterfeit Risk

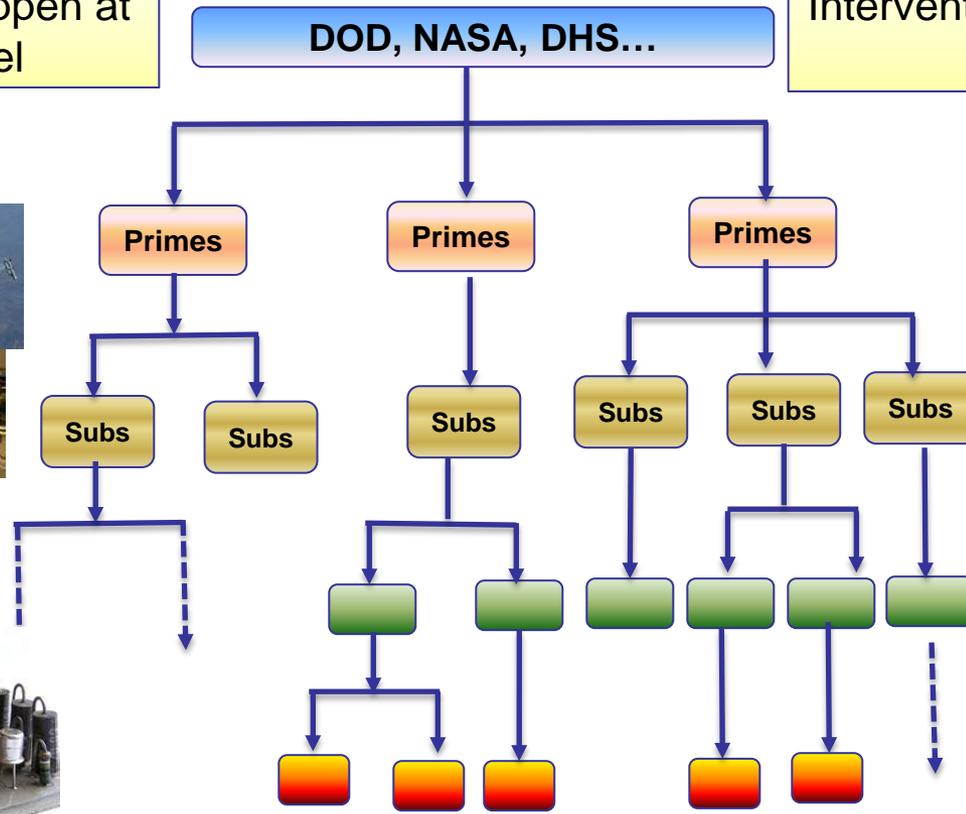


Prolonged use of aging systems creates opportunities for counterfeit parts to enter the supply chain

# Intrusion and Intervention

Intrusion...can happen at any level

Intervention...requires more than just contract action

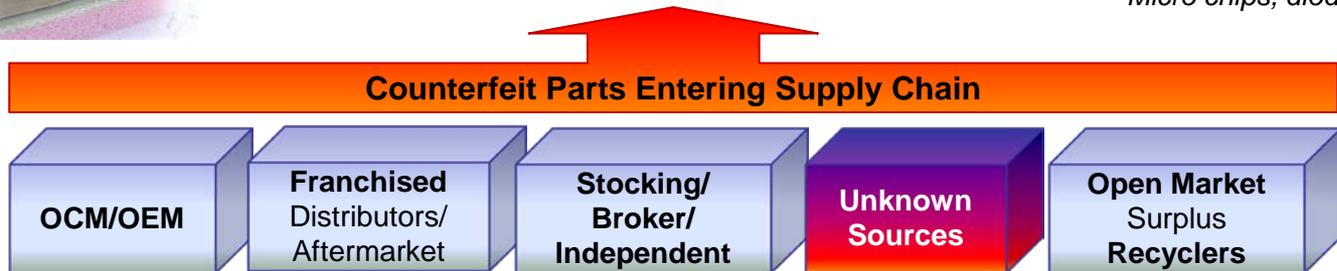


Systems  
Titan IV, GPS, F-16 etc.

Sub-Systems  
Flight Avionics, Propulsion,  
Electro-Mechanical Valves,  
Guidance Computer, INS, etc.

Components  
Power Distribution Assembly,  
Data Recorder, Antenna Assembly,  
etc.

Sub-Components  
Graphic Cards, Circuit boards,  
Micro chips, diodes, capacitors, etc.



# FY2010 - FY2014 Focus

## Department-wide

- Publish counterfeit materiel policy
- Establish counterfeit center of excellence (analysis, metrics, trend reporting)
- Develop and implement modifications to data exchange/reporting system (GIDEP)
- Collaborate with industry to develop recommended approaches and solution sets
- Expand training

## Defense Logistics Agency

- Establish additional distributor qualification lists for electronics and non-electronic products
- Tighten controls on component traceability & certification process
- Expand use of the DLA contractor review list
- Increase testing for new sources & “at risk” items
- Increase quality assurance capability ( inspections & testing) at Strategic Distribution Points
- Conduct more thorough investigations & trend analysis of reported deficiencies
- Institute specific procedures for disposition of counterfeit materiel
- Institute R&D programs ( CAGE Code Hopping, Counterfeit targets, DNA & UID marking techniques)

## Military Services

- Increase component testing—critical and non-critical
- Supplement DoD counterfeit policy
- Increase supplier facility and process audits for critical components
- Institute counterfeit control plans in supply and repair centers
- Develop counterfeit metrics and analysis centers
- Expand counterfeit training for contract specialist and artisans

# Memorandum from Acting USD/AT&L Overarching Anti Counterfeit Guidance

- Addresses an area of critical concern while DoDI is in coordination
- Provides definition
- Emphasizes
  - Risk-based approach
  - 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



Acting Under Secretary of  
Defense for AT&L

# So what does this have to do with AIT and Item Unique Identification (IUID)?

- Could methods of AIT be used to identify and provide traceability for authentic parts throughout their lifecycle?
  - AIT requires some sophistication to apply particular where fraud is used such as remarking parts as new
  - More efficient data gathering and connection to part information for confirmation and alerts (e.g. GIDEP)
  - Traceability to item level connected to information about the item (e.g., acceptance location, prior registration in DoD IUID Registry, previous disposition from inventory)
    - IUID integrated in Component business processes
  - For a few high-end closed loop applications consider additional technologies (e.g, nanotubes, DNA marking)

# Objectives for AIT as an Anti-counterfeiting strategy

- Develop identification processes to rebaseline items introduced years and even decades ago after authentication AND increase traceability in new production
- Not limited to electronics – could be load bearing parts, electro-mechanical, food, pharmaceuticals, and others
- Solutions should comply with existing DoD architectures and leverage existing and proposed AIT investments
- Work appropriately at the echelons of the DoD supply chain
- Cannot be easy for the counterfeiters to defeat
- Must support DoD supply chain objectives for decreasing response times, lowering costs, and supporting warfighter readiness globally

# Next Steps

- Think about solution sets which can provide end to end anti-counterfeiting protection, particularly for high risk items
- Play Red Team – if you were a counterfeiter, how would you defeat the protection?
- Does it meet the criteria on the previous slide?
- If so, stay tuned for further discussions