Addressing Counterfeits & Non-Conforming Components

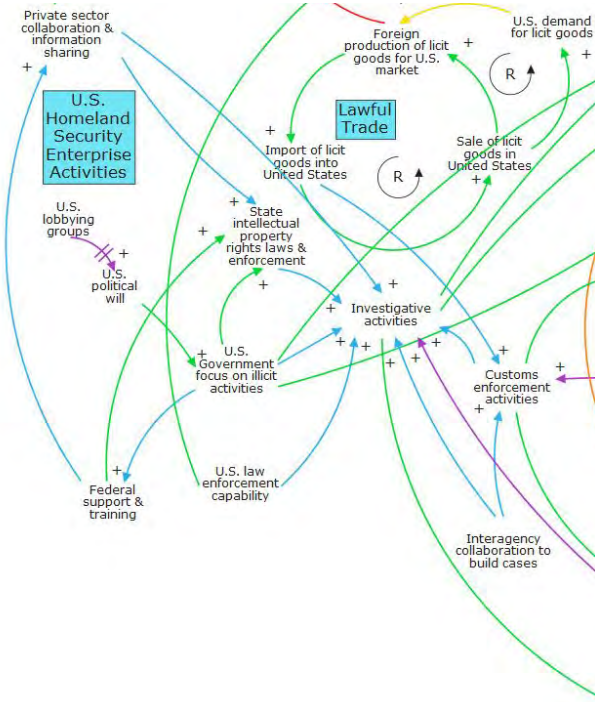
Joe Jarzombek,

Director for Software and Supply Chain Assurance

Stakeholder Engagement & Cyber Infrastructure Resilience

Homeland Security

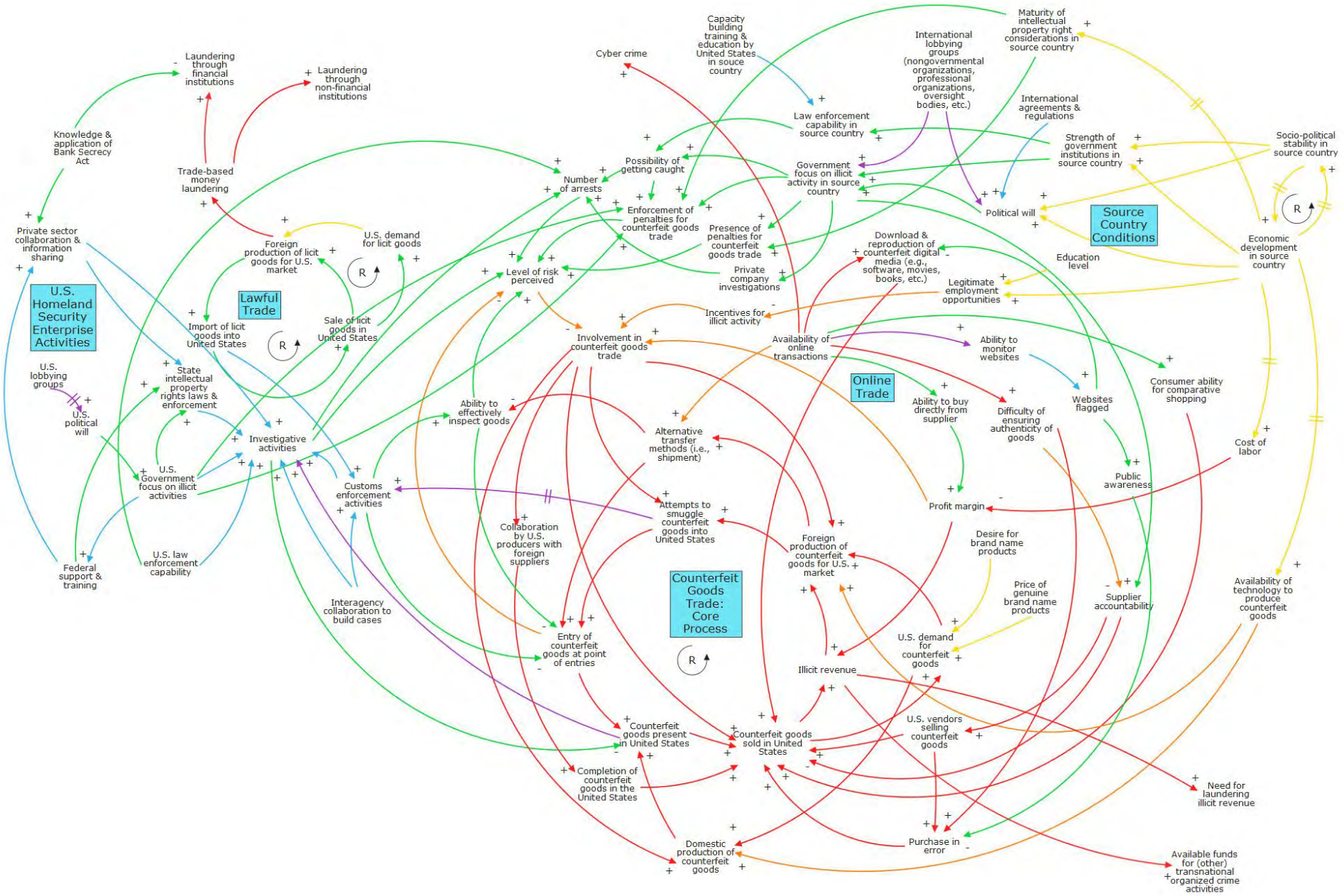
Supply Chain Risk Management and Software Assurance Imperatives



Increased risk from supply chain due to:

- **Increasing dependence on commercial ICT for mission critical systems**
- **Increasing reliance on globally-sourced IT hardware, software, and services**
  - **Varying levels of development & outsourcing controls**
  - **Lack of transparency**
  - **Varying levels of acquisition 'due-diligence"**
- **Residual risk passed to end-user enterprise**
  - **Counterfeit products**
  - **Tainted products with malware, exploitable weaknesses and vulnerabilities**
- **Growing technological sophistication among our adversaries**
  - **Internet enables adversaries to probe, penetrate, and attack us remotely**
  - **Supply chain attacks can exploit products & processes throughout the lifecycle**

Homeland Security



Homeland Security

Framing the Problem

- The USG and industry partners are working toward solutions to reduce the risk of counterfeit information and communications technology (ICT).
- Numerous efforts are underway to prevent, test, identify, and track counterfeit ICT. Today's presentations will demonstrate some of the leading counterfeit studies, approaches, reporting, and information gathering activities across government and industry.
- Using today's presentations as a foundation, the afternoon discussion should focus on how best to share data and lessons learned, as well as how to create scalable approaches for the detection and reporting of counterfeits.

Homeland Security

Framing the Problem

- A ‘counterfeit’ is a non-genuine hardware part or software.
- Non-genuine refers to:
  - Unauthorized copy
  - Not conforming to the design, model, or performance standards prescribed by the original manufacturer
  - Produced by an unauthorized contractor
  - Off-specification, defective, or used original component sold as new or working
  - Incorrect or false markings or documentation

Shantou (China) warehouse: Boards stacked, waiting for chip removal. Credit: Tom Sharpe, SMT Corp

Opportunity for malicious logic or backdoor insertion at untrusted manufacturing sites.

Counterfeits often fail more quickly or frequently than genuine parts, impacting reliability and brand name.

Homeland Security

Framing the Problem

Department of Commerce (DOC), Bureau of Industry and Security (BIS) Counterfeit Electronics Survey

Type of Company		Encountered Counterfeits	No Counterfeit Incidents	Total	% Encountered Counterfeits
OCMs	Discrete Electronic Components	18	21	**39**	**46%**
	Microcircuits	24	20	**44**	**55%**
Distributors	Authorized Distributors	10	35	**45**	**22%**
	Unauthorized Distributors	44	9	**53**	**83%**
Board Assemblers		**11**	**21**	**32**	**34%**
Prime/Sub Contractors		31	90	**121**	**26%**
Total		**138**	**196**	**334**	**41%**

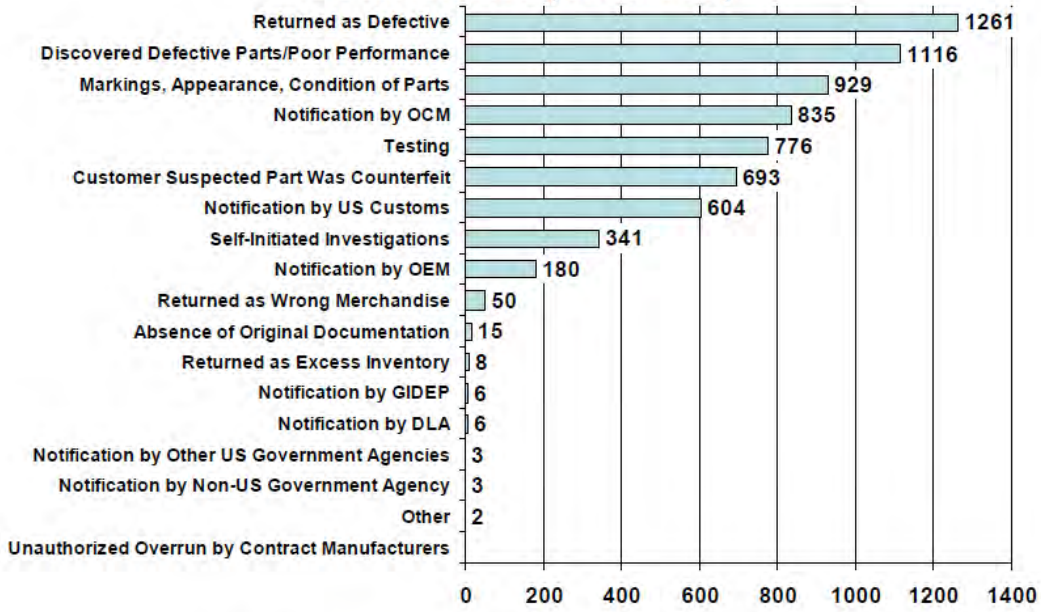
[1] DOC, BIS OTE, *Defense Industrial Base Assessment: Counterfeit Electronics,* p. 165, January 2010. (http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf)

Homeland Security

Framing the Problem

Identifying and Tracking Counterfeits

Figure VII-14: How Companies Are Uncovering Counterfeits (2008 est.)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

DOC, BIS OTE, *Defense Industrial Base Assessment: Counterfeit Electronics,* p. 176, January 2010. (http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf)

Figure VII-17: Percent of Companies/Organizations Who Encountered Counterfeits and Maintained a Tracking Database

OCMs	52%
Authorized Distributors	30%
Unauthorized Distributors	66%
Circuit Board Assemblers	18%
Prime/Sub Contractors	32%
Department of Defense	21%

Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

DOC, BIS OTE, *Defense Industrial Base Assessment: Counterfeit Electronics,* p. 179, January 2010. (http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf)

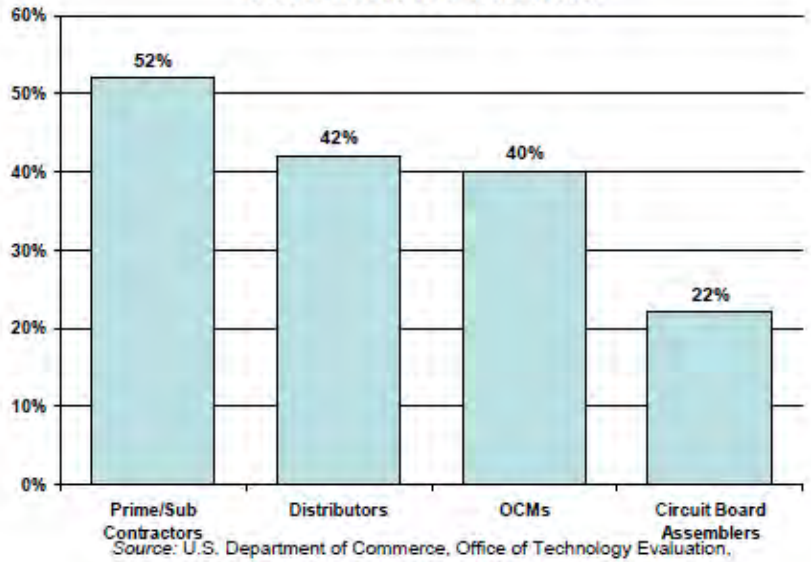
Homeland Security

Framing the Problem

Reporting

Figure VII-24: Top Authorities Notified After Counterfeit Incidents	
None at All	51%
Government-Industry Data Exchange Program (GIDEP)	14%
Defense Logistics Agency (DLA)	11%
State/Local Authorities	8%
Customs & Border Protection	7%
Federal Bureau of Investigation (FBI)	6%
Defense-Related Investigative Services (e.g., DCIS, NCIS, etc.)	5%
Federal Aviation Administration (FAA)	5%
*** Only includes those companies with counterfeit incidents**	
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.	

Figure VII-25: Percent of Companies That Know What Authorities to Contact When They Encounter Counterfeit Products



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

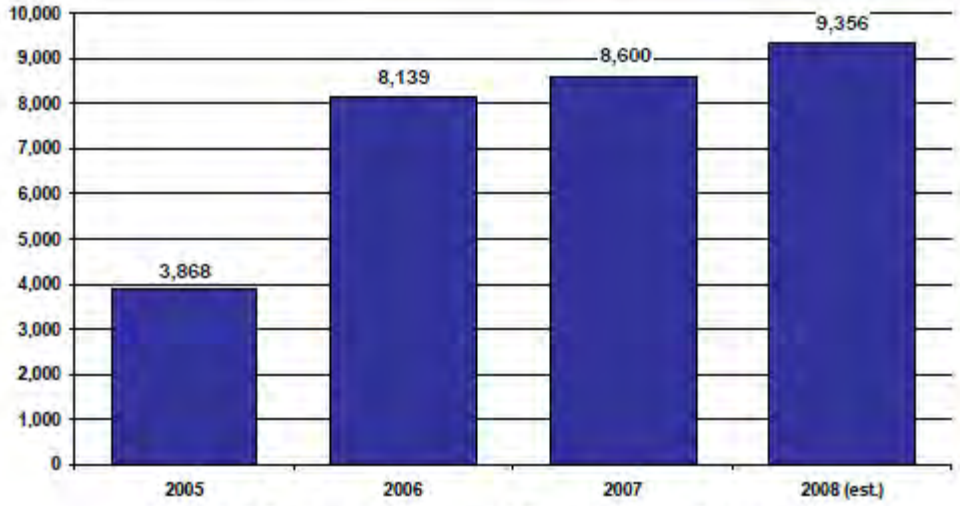
[1] DOC, BIS OTE, *Defense Industrial Base Assessment: Counterfeit Electronics,* p. 186, January 2010. (http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf)

Homeland Security

Framing the Problem

Incidents Identified and Incidents Reported

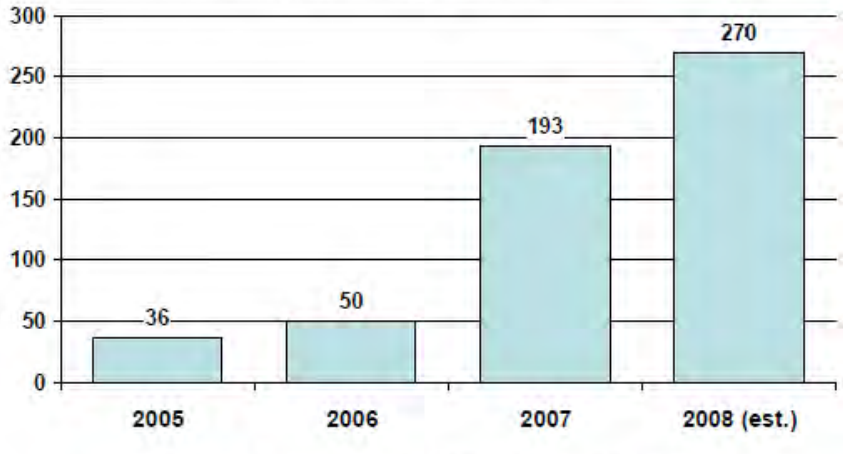
Figure VII-7: Total Counterfeit Incidents: OCMs, Distributors, Board Assemblers, Prime/Sub Contractors 2005 - 2008



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

DOC, BIS OTE, *Defense Industrial Base Assessment: Counterfeit Electronics,* p. 170, January 2010. (http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf)

Figure VII-23: Number of Incidents Reported to Government Authorities



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

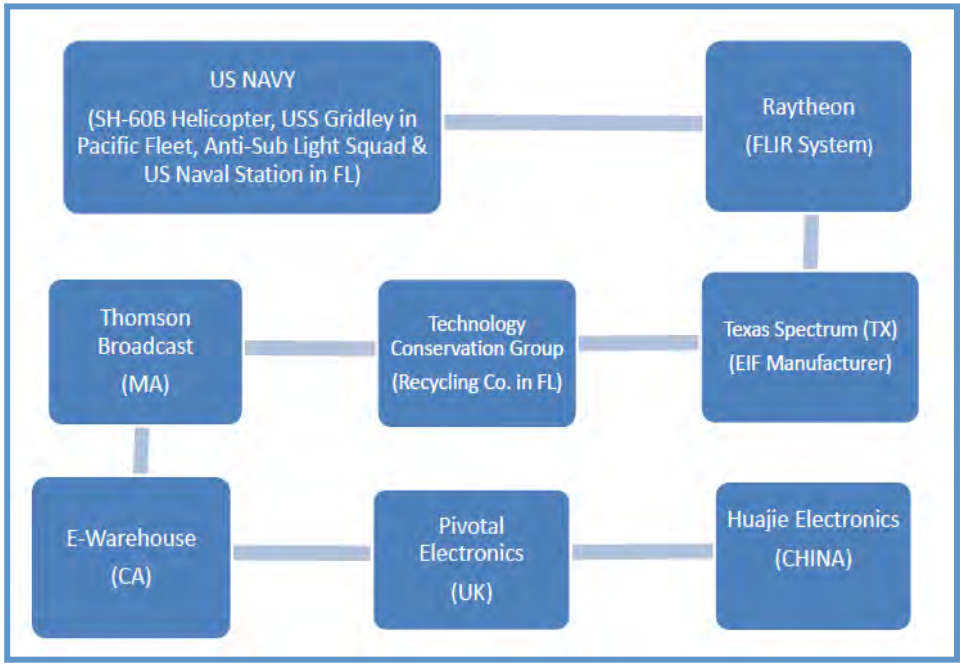
DOC, BIS OTE, *Defense Industrial Base Assessment: Counterfeit Electronics,* p. 185, January 2010. (http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf)

Homeland Security

Framing the Problem

Counterfeit Examples in the Department of Defense

- Counterfeit memory chips from China sold to L-3 Communications which were built-into the C-27J plane of the Air Force.
- Counterfeit parts were used in Electromagnetic Interference Filters (EIF) intended for the Navy's SH-60B helicopters.
- Cisco lost more than $27 million in assets due to one person who manufactured counterfeit electronic parts and then inserted them into Cisco's supply chain.



Supply Chain for Suspect Counterfeit Parts in FLIR for U.S. Navy SH 60B Helicopter

In 2008, North American law enforcement identified over $78 million in counterfeit Cisco products across global supply chains.

Homeland Security

Framing the Problem

Types of Counterfeit Databases

1. **Government-Industry Data Exchange Program (GIDEP)**: Cooperative activity between USG and industry participants to reduce resource expenditures by sharing technical information.
2. **Joint Deficiency Reporting System (JDRS):** Cross-service, web-enabled automated tracking system across the Aeronautical Enterprise. designed to initiate, process and track deficiency reports from the Warfighter through the investigation process.
3. **ERAI, Inc:** Privately held global information services organization that monitors, investigates and reports issues affecting the global semiconductor supply chain.

Homeland Security

Community Perspective on the Scalable Detection and Prevention of Counterfeits

Joe Jarzombek, Director for Software and Supply Chain Assurance

Stakeholder Engagement & Cyber Infrastructure Resilience

Homeland Security

Agenda

- Purpose
- Scope
- Initial Research & Findings
- Assumptions for Today's Discussion
- Proposed Methodology
- Framing the Problem
- Focus Areas
- Key Questions
- Next Steps

Homeland Security

Purpose

- The USG and industry partners need a scalable means to detect and report ICT supply chain risks attributable to counterfeits, defects, and tainted components (i.e. non-conforming parts).
- The purpose of this brief is to:
  - Establish a baseline of current practices and capabilities to inform community discussion, and
  - Propose a series of activities that ultimately lead to the automation of detecting and reporting non-conforming parts.

Homeland Security

Scope

- The initial research was limited to a number of organizations with easily accessible, transparent counterfeit and anti-counterfeit-related management programs.
- Our research included the following entities:
  - Federal Departments and Agencies:
    - Air Force, NASA, Navy, DHS (CBP), DoE, DoC
  - Professional Association and Standards Organization:
    - SAE International
    - Semiconductor Industry Association (SIA)
  - Commercial, Academic and Government Organization:
    - University of Connecticut: Center for Hardware, Assurance, Security and Engineering (CHASE)
    - Syracuse Research Corporation (SRC)

Homeland Security

Initial Research and Findings

- D/A's counterfeit management programs vary in approach and maturity.
- There is a heavy emphasis on counterfeit databases that are not used to their fullest potential (e.g., GIDEP).
- Variation of counterfeit definitions and characterization of counterfeits across the USG complicates the issue (e.g., many quality assurance procedures reflect existing counterfeit standards, but are not explicitly counterfeit guidance).
- The level of sophistication of testing counterfeits varies across D/As.
- The verification of data input of counterfeit databases is unclear.
- Not all counterfeit approaches examined have uniform reporting procedures.
- The majority of D/As prioritize the inspection of suspect counterfeit items based on mission criticality.

Assumptions for Discussion

- Focusing efforts on addressing all non-conforming components by default addresses maliciously-tainted components.
- Additional taxonomies around non-conforming parts may be available in government, industry, and academic fields that were not used in this presentation.
- Additional research may be necessary to understand the totality of counterfeit management approaches.
- There is currently no standardized and scalable detecting-and-reporting mechanism or procedure for non-conforming ICT parts.

Homeland Security

Methodology

1. Understand the depth and breadth of counterfeit and anti-counterfeit management approaches across the USG and industry.
2. Build aggregated taxonomies from the review.
3. Define risk characteristics or 'observables' of non-conforming (counterfeit, defective, and tainted) components and mechanisms for specifying conforming/authentic components (including packaging)
4. Catalogue testing and detection capabilities, as well as various means to assert or determine authenticity or conformance of components (i.e. anti-counterfeiting).
5. Identify gaps in tools and automation capabilities or opportunities for technology improvements.

Homeland Security

Framing the Problem

Taxonomy for Conforming & Non-Conforming Parts

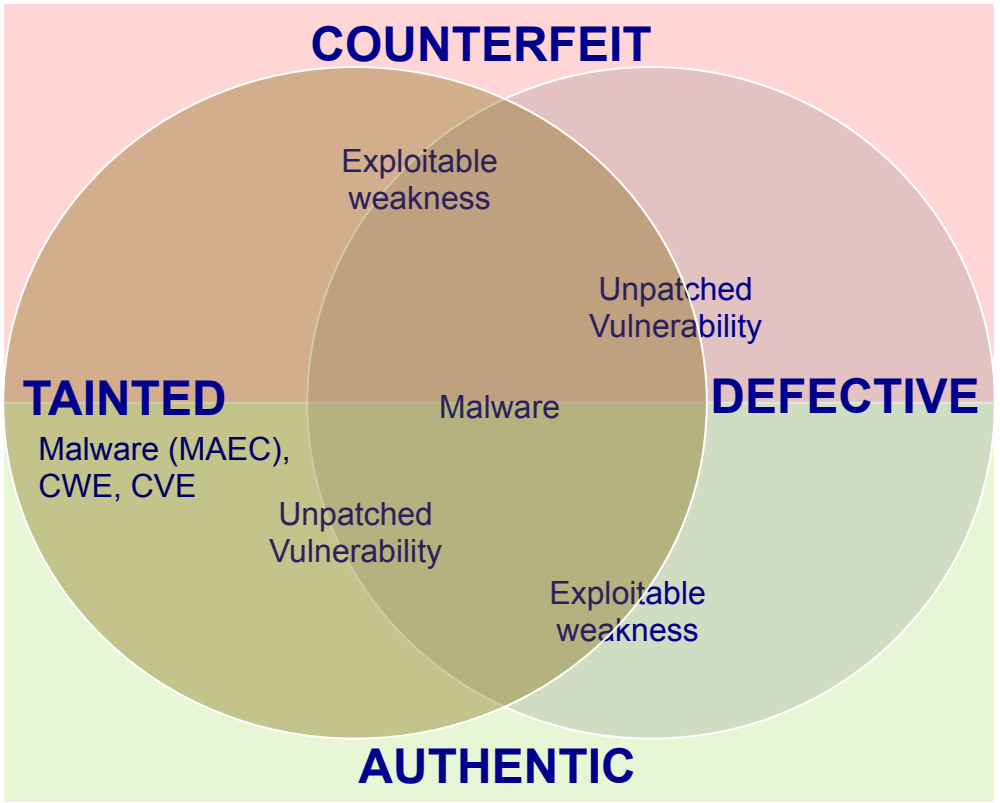
Catalogue Methods for Detection, Testing, and Anti-Counterfeiting

Build Taxonomies for determining:

- Authentic components
- Counterfeit components
- Defective components
- Tainted components containing
  - Malware (MAEC)
  - Exploitable Weaknesses (CWE)
  - Known vulnerabilities (CVE)

Define Observables

To 'scale' detection & reporting of Counterfeits, leverage Security Automation such as CybOX, STIX, & CAPEC



Components can become tainted intentionally or unintentionally throughout the supply chain, SDLC, and in Ops & sustainment

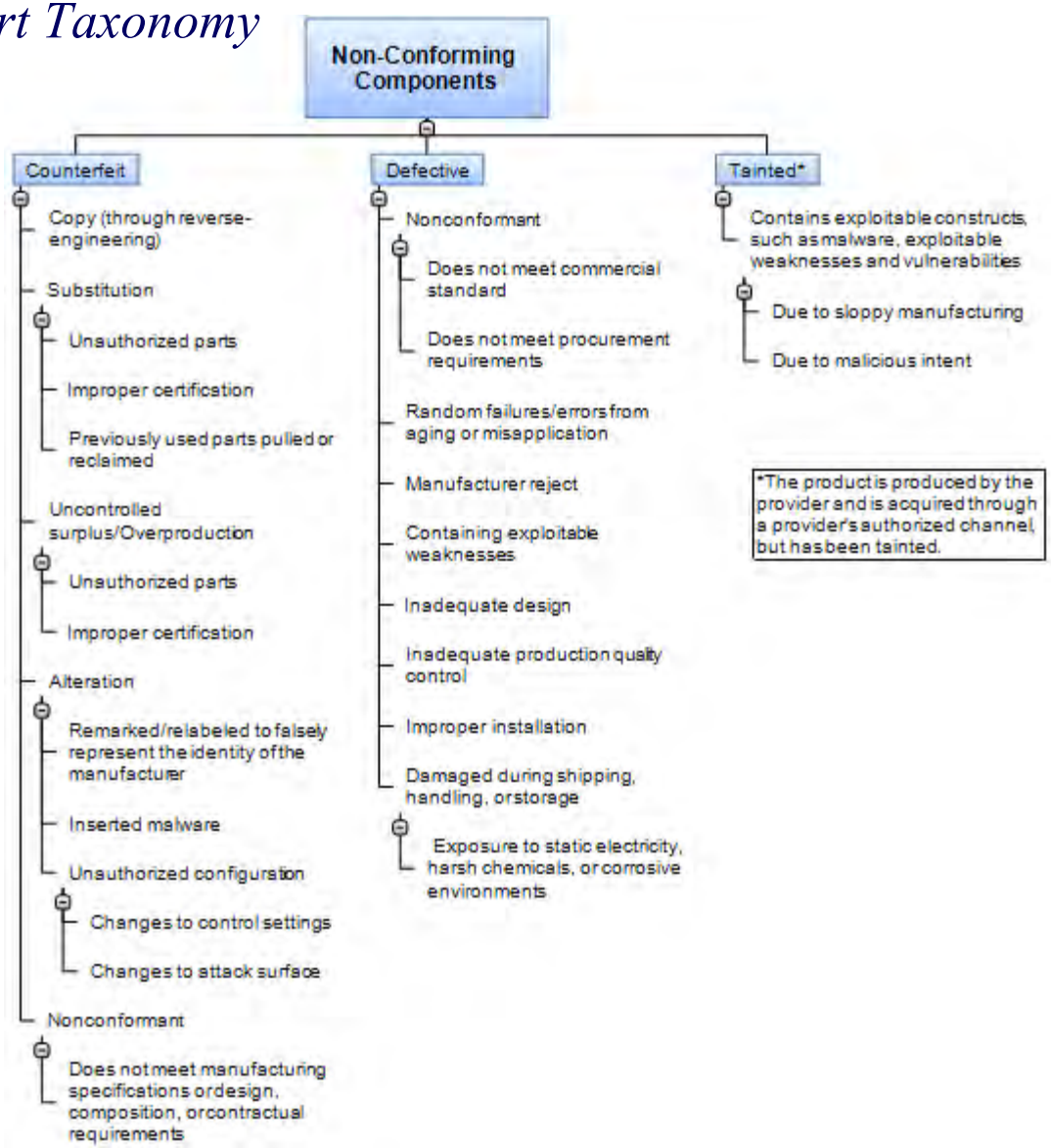
*Text demonstrates *examples* of overlap

Homeland Security

Focus Area #1: Build Taxonomies

Non-Conforming Part Taxonomy

A standardized taxonomy is the first step towards creating scalable methods for detecting and reporting non-conforming components.

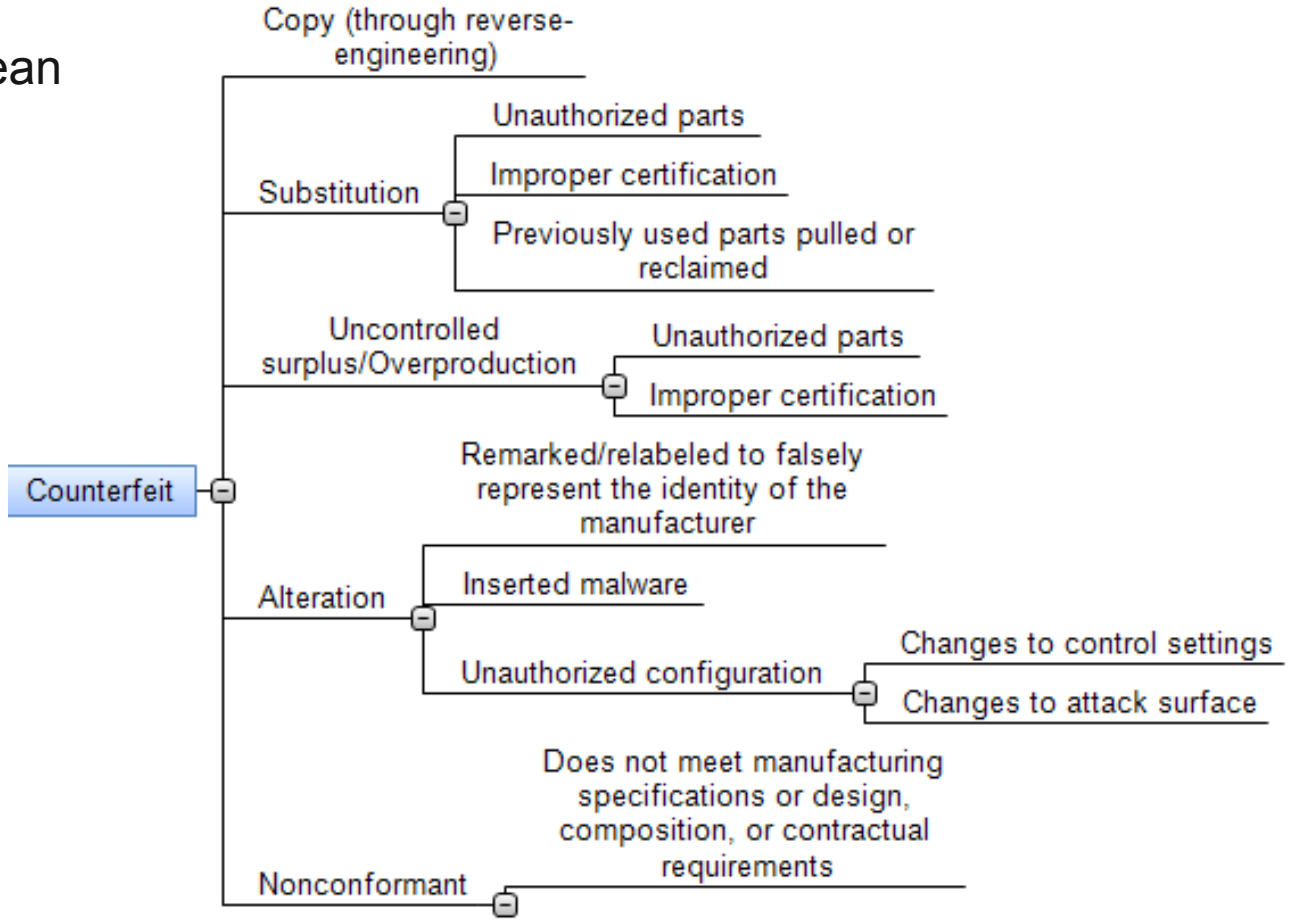


Homeland Security

Focus Area #1: Build Taxonomies

Counterfeit Taxonomy

What do we mean when we say 'counterfeit'?

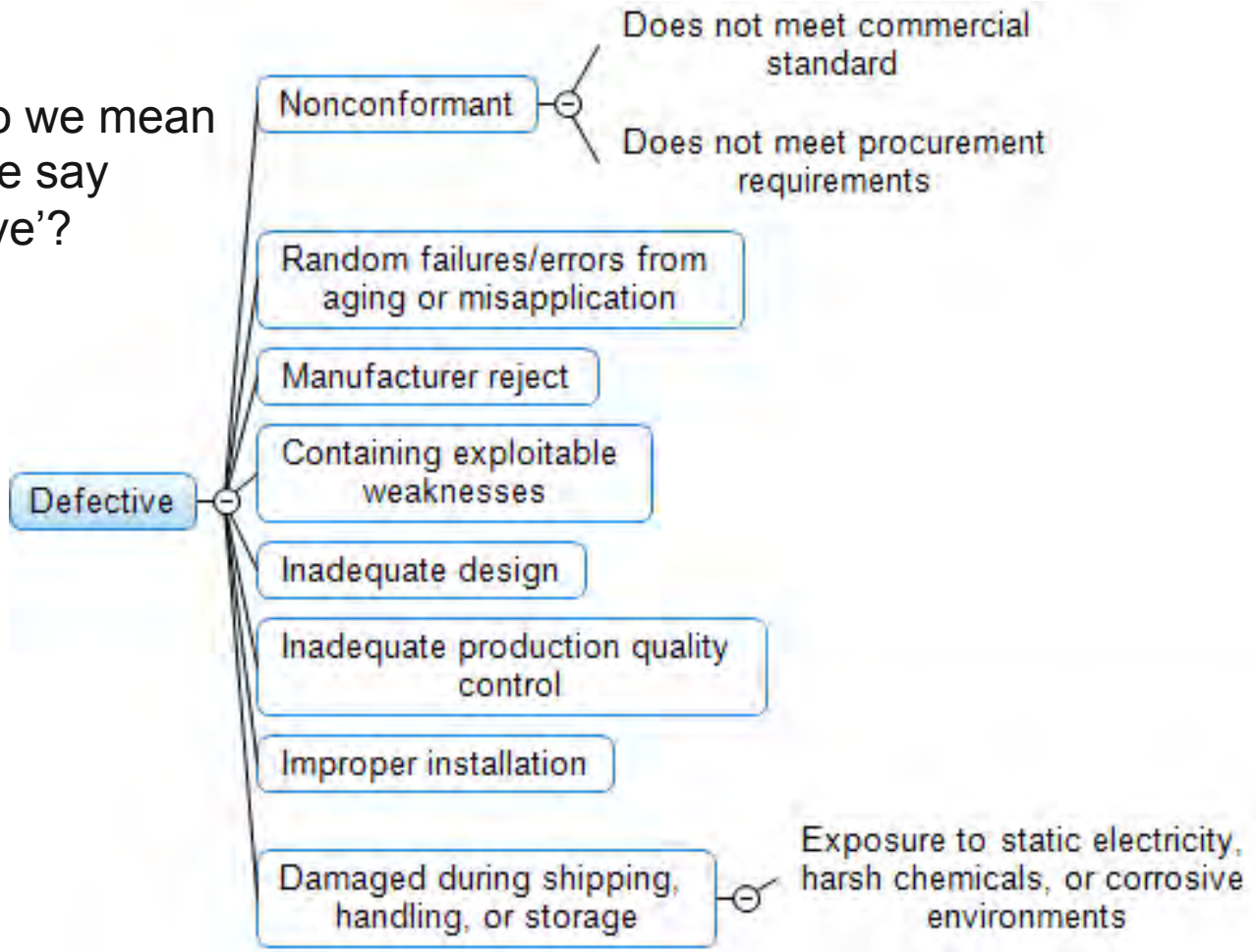


Homeland Security

Focus Area #1: Build Taxonomies

Defective Component Taxonomy

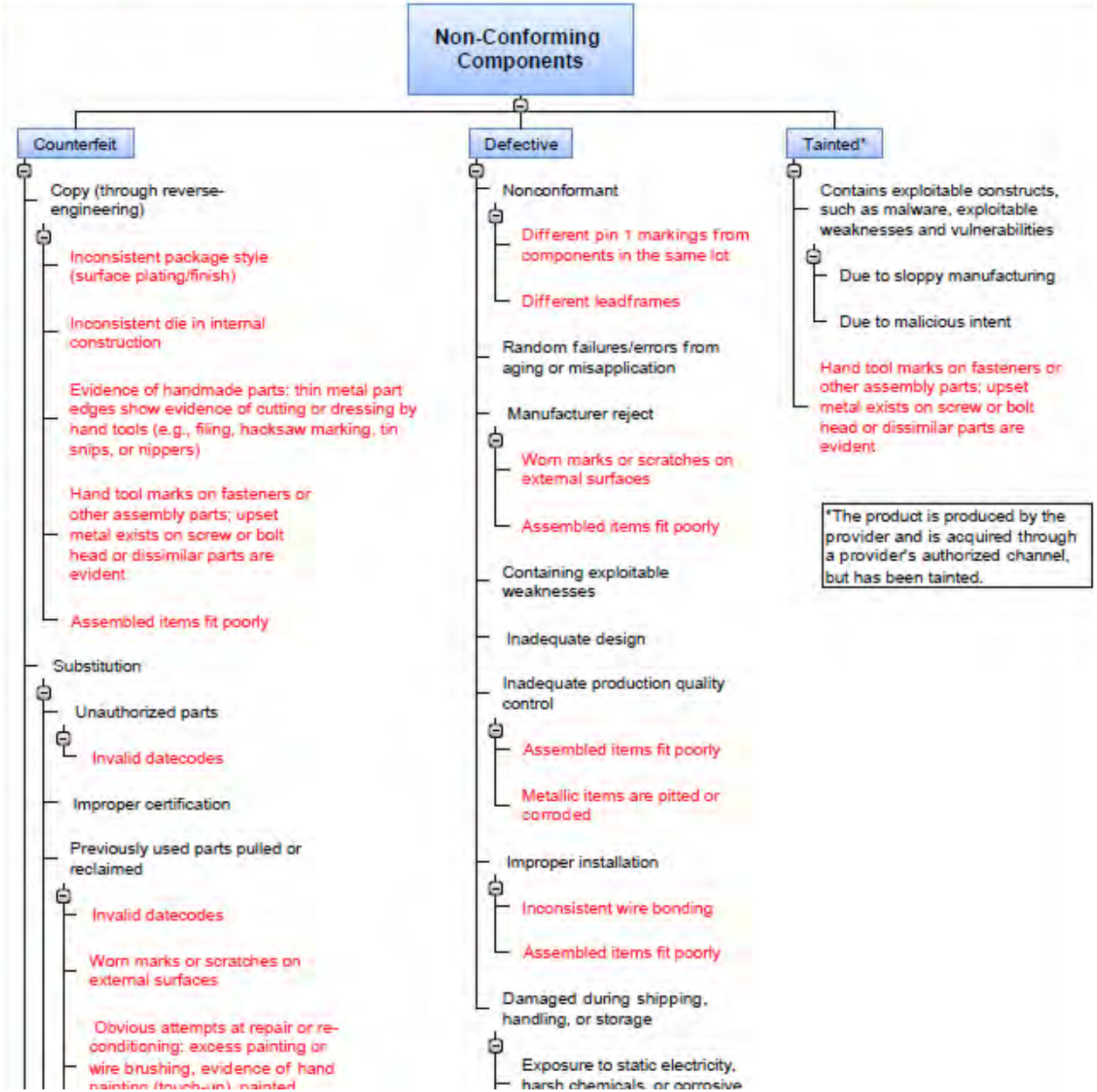
What do we mean when we say 'defective'?



Homeland Security

Focus Area #2: Define Observables

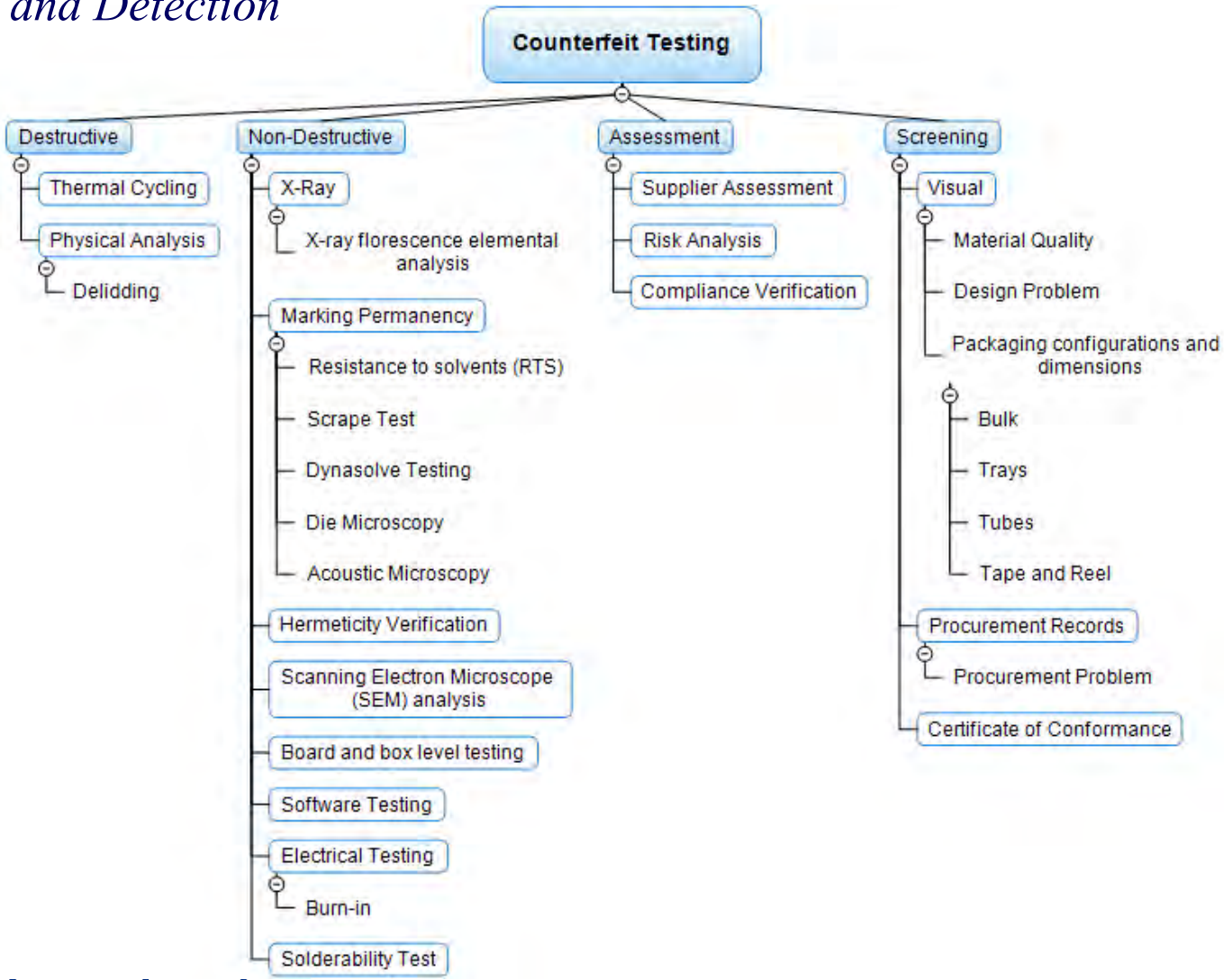
The second step is to associate 'observables' with each of the descriptive terms. The chart is demonstrative, not meant to be comprehensive.



Homeland Security

Focus Area #3: Catalogue Methods

Testing and Detection



Homeland Security

Focus Area #3: Catalogue Methods

Testing and Detection: NanoTEM MegaRel HI-REL Study1

MegaRel
A NanoTEM Company

Characterization Overview – Tiered Inspection

- level of inspection shown by icon in top right corner

Homeland Security

Focus Area #3: Catalogue Methods

Anti-Counterfeiting

1. When using an 'Aftermarket Manufacturer' rather than the Original Component Manufacturers (OCM),
   - Manufacturer is authorized by the OCM to produce and sell replacement parts, usually due to an OCM decision to discontinue production of a part.
   - Parts supplied are produced from materials that have been transferred from the OCM or produced using OCM tooling and IP.
   - Parts must have been properly stored until use and are subsequently assembled, tested, and qualified.
   - Parts must be labeled or otherwise identified to ensure that the "as shipped" aftermarket manufactured part should not be mistaken for the part made by the OCM.

Homeland Security

Focus Area #3: Catalogue Methods

Anti-Counterfeiting

2. Parts are received in a homogenous lot that are:
   - Received in a single shipment
   - Marked or otherwise identified with identical lot, batch, run, and identification information (e.g., dates codes, lot codes, serial numbers)
   - Identical in appearance to the unaided eye (parts and packaging)
   - Appear to have been subjected to the same handling, packaging, and/or storage conditions; and
   - Have maintained their physical placement relative to each other (i.e., have never been separated based on evidence such as source, packaging, labeling).

Homeland Security

Focus Area #3: Catalogue Methods

Anti-Counterfeiting

3. Use of authorized brokers
4. Product Identification/Authentication Request Form to authenticate suspect products during acquisition or already in the USG supply chain (e.g., used by the Semiconductor Industry Association)
5. Certification of Origin of Product: Confirmation by the Seller that it is either the Original Equipment Manufacturer (OEM), Original Component Manufacturer (OCM), or a franchised or authorized distributor of the OEM/ OCM for the product procured. (SRC Inc.)
6. Provision that the supplier further warrants that OEM/OCM General Provisions and requirements flow down to any tier of subcontractors and suppliers (SRC Inc.)

Focus Area #3: Catalogue Methods

Anti-Counterfeiting

7. ESD bagged/handling based on ANSI/ESD S20.20 standard instead of open unshielded boxes with integrated circuits in tubes or reels (not ESD-bagged).
8. Use IDEA and filtered ERAI member companies
9. List of all outsourced locations where value added processes are performed (lead straightening, testing, solder dipping, marking, packaging, etc.)
10. Deoxyribonucleic Acid (DNA) marking of authentic products

Homeland Security

Focus Area #3: Catalogue Methods

Anti-Counterfeiting

- Open Group Standard: O-TTPS *Mitigating Maliciously Tainted and Counterfeit Products*

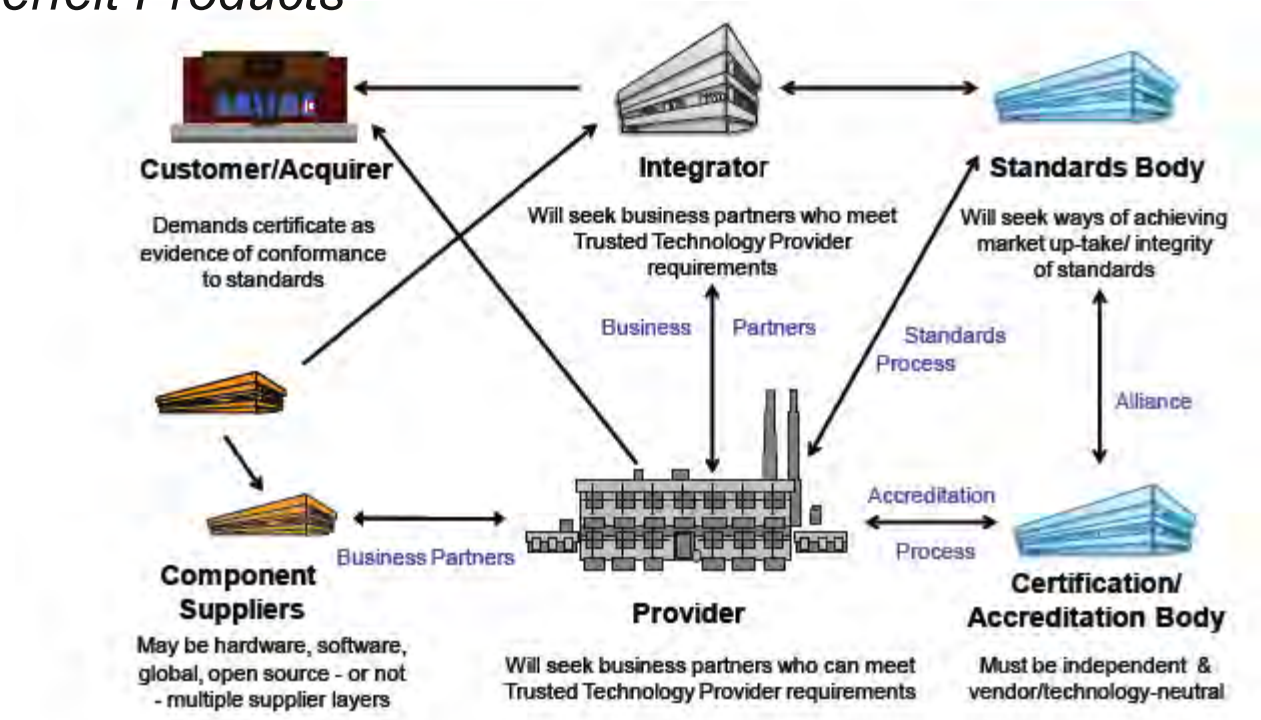


Figure 1: Constituents

Homeland Security

Software & Supply Chain Assurance focus on: Conforming & Non-Conforming Components

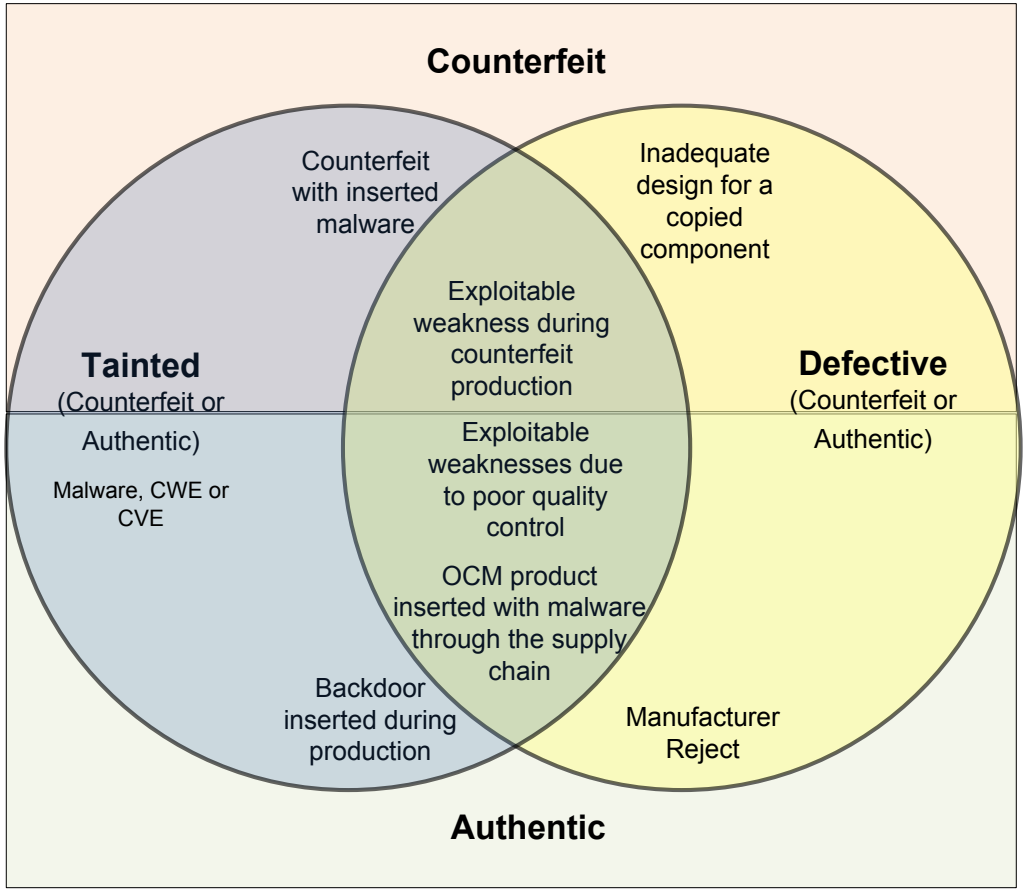
Catalogue Methods for Detection, Testing, and Anti-Counterfeiting

Build Taxonomies for determining:

- Authentic components
- Counterfeit components
- Defective components
- Tainted components containing
  - Malware (MAEC)
  - Exploitable Weaknesses (CWE)
  - Known vulnerabilities (CVE)

Define Observables

Leverage Security Automation such as CybOX, STIX, & CAPEC



Homeland Security

*Text demonstrates *examples* of overlap

Key Questions for Discussion

1. ***Standardization:*** Does the USG need to have a standard definition for what constitutes a counterfeit product and authentic component, or should the definition vary by application?
2. ***Scope:*** What is missing from the taxonomies presented above?
3. ***Prioritization:*** Is there value in prioritizing the list from least to most risky and/or their utility in terms of impact on the user?
4. ***R&D:*** What are gaps in tools and automation capabilities or opportunities for technology improvements?
5. ***Lessons Learned:*** Can we leverage lessons learned from identifying & preventing defects for identifying & preventing counterfeits?

Homeland Security

Next Steps

- Receive feedback on the Focus Areas (taxonomies and catalogue of methods).
- Formalize taxonomies for conforming and non-conforming parts
- Build/maintain catalogue of detection & anti-counterfeiting methods
- Test ability to create automated tools for observables (leveraging CybOX, STIX, and CAPEC) and identify gaps in existing security automation enumerations and languages
- Specify new language schema that covers counterfeits, authentic components, and defects (not addressed in CybOX, STIX, or CAPEC)
- Ensure “XXXX-as-a-Service” supply chain risks are addressed in moving to the Cloud for software, IT, platform, and data services.

Homeland Security

Technology Gaps in Realizing Scalability

For Obsolete/Active Parts:

- Long test time (up to 8 hours for a single chip) that leads to the sampling from the batch of components
- Existing detection process incurs human errors and inaccuracy during test
- Lack of automation leads to the requirement of SMEs
- Discrepancies in findings from different labs
- Lack of high confidence level in tests or consideration of risk during testing
- Lack of continuous monitoring for counterfeit trends and threats
- Designing new test equipment (portable) to securing borders

Homeland Security

Technology Gaps in Realizing Scalability

For New Parts:

- Industry has yet to include security, reliability, anti-counterfeiting, and trust into their design flow
- Research requirements:
  - Securing supply chain
  - Securing design and test process
  - Designing new mechanisms for securing ICs against all counterfeit types (recycling, over-produced, cloned, etc.)
  - Designing new test equipment (portable) to securing boarders
  - Verifying the trustworthiness of integrated circuits

Homeland Security

Homeland Security