INNOVATION DRIVES FORWARD




Counterfeit Parts Awareness and the Oshkosh Defense Avoidance System

Presentation Courtesy of Lockheed Martin

OSHKOSH DEFENSE

Part 1 – Background and Awareness

Part 2 – Avoidance

Part 3 – Detection

Part 4 – Mitigation

Part 5 – Disposition

Part 6 – Oshkosh Counterfeit Detection and Avoidance System

Reference: Significant portions of material in this presentation are taken from counterfeit prevention classes available through Defense Acquisition University and from a Counterfeit Parts Prevention presentation distributed by Lockheed Martin

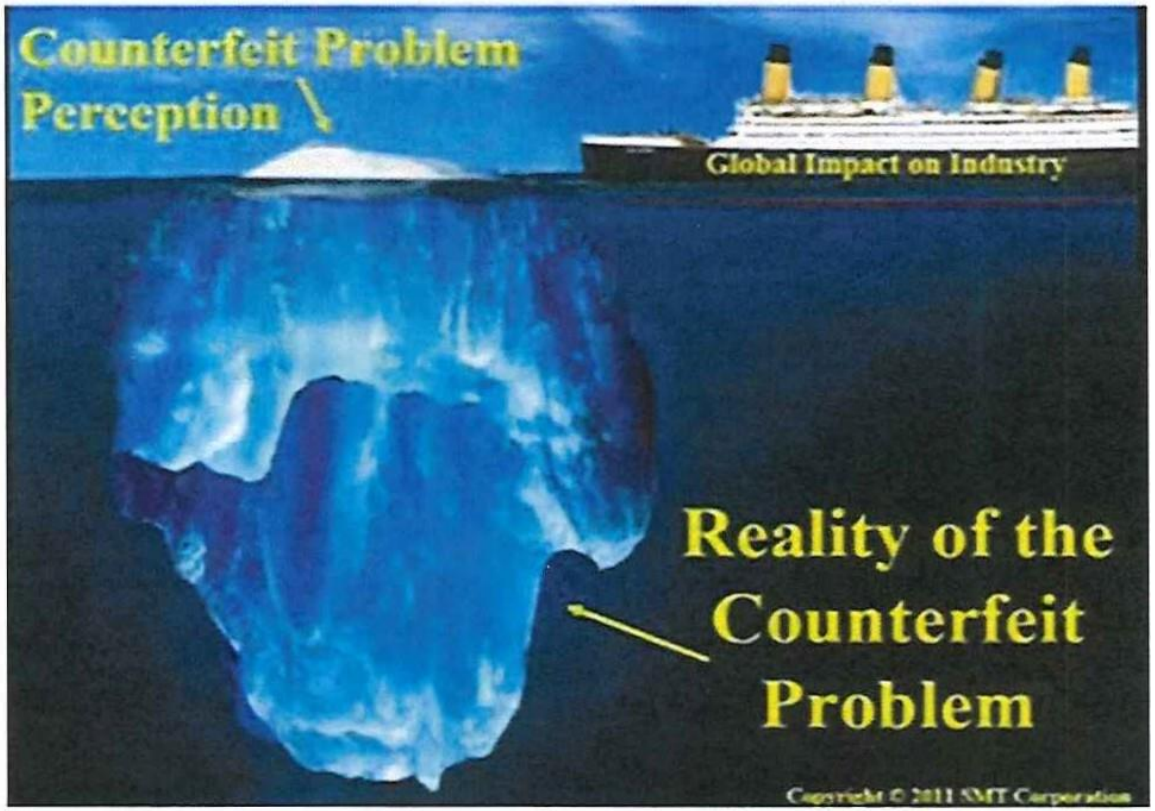
OSHKOSH DEFENSE

Counterfeit

Background and Awareness

OSHKOSH DEFENSE

What is Counterfeit?



Counterfeit items often have the appearance of being genuine but are later revealed that they were not…

- Manufactured by the original component or material manufacturer
- Built to the same quality standards or tested as rigorously as a genuine item

Many types of counterfeits are very difficult to detect visually and can be made such that they "seem" to be functional and pass early levels of testing.

OSHKOSH DEFENSE

Definitions

Nonconforming
According to the DoD Instruction 7050.05 a product (or component) that has not been manufactured, assembled, tested or inspected in accordance with the terms of a contract, specifications, or drawings. Nonconforming material is not necessarily suspect or counterfeit.

Suspect
According to SAE Aerospace Standard AS5553, a part is suspect when there is indication by visual inspection, performance, or testing that the part may have been misrepresented as something it is not; including evidence of misrepresentation in related documentation.

Counterfeit
DoD Instruction 4140.01, DoD Supply Chain Management Policy, defines counterfeit as a material whose identity or characteristics have been deliberately misrepresented, falsified, or altered without legal right to do so.

Counterfeit Electronic Part
According to DFARS 252.246-7007, an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

Counterfeiting is a Business

- Counterfeit business is estimated to be $225 billion and more than 750,000 jobs worldwide.
- Consumer Electronics constituted more than 8% of the $196 million seized by US customs.
- US companies suffer $9 billion in trade losses due to international copyright piracy

Source: International Anticounter Coalition

It is difficult to get firm statistics on how wide spread counterfeiting is because often times it is not reported. Items are often returned through the supply chain for refund or replacement or simply disposed of instead of being investigated.

OSHKOSH DEFENSE

Counterfeit Risks for DoD Supply Chain

- The most common Counterfeiting of DoD items identified to date is in **electronics, microcircuits and semi-conductors**; however, counterfeit drugs, metals and other materials including rubber, fasteners and O-rings are known to have been delivered to DoD.
- Counterfeiters may also take an entirely different part and mark it to appear to be the item purchased.

- Items with Diminishing Manufacturing Sources and Material Shortages (DMSMS) are at particular risk
  - Mainly reported with **electronics, microelectronics and components**, but can affect all areas of supply, material and equipment
  - Shortage of authorized items or manufacturers indicate risk
  - Re-marking other items or refurbishing used items are common methods used by counterfeiters to capitalize on this risk

OSHKOSH DEFENSE

Counterfeit parts are in the supply chain

- Three in California were indicted during a NAVY NCIS Sting operation for selling counterfeit electronics to the military.
- Ft Lauderdale man received 2 ½ years in prison and was fined $54,000 for supplying counterfeit parts, labels and certificates to the Air Force and NASA.
- 1,505 "plain encased seals" for tail rotor gear boxes of UH-60 helicopters were found to be made of substandard nitrile rubber by a company in Taiwan for about $1 each.
- July 2009 a St. Petersburg, FL company that provides millions of dollars in safety devices to DoD contractors was under investigation for supplying counterfeit parts.
- Fudge Titanium could threaten the next Mars Rover. Additionally, the suspect titanium was also traced to Air Force F-15 and F-22 fighter jets and C-17 Cargo planes.

OSHKOSH DEFENSE

Sources of Counterfeit Electronic Parts

Counterfeit parts can come from many different sources.

This flow illustrates how counterfeit parts can be sourced and eventually sold:

While this slide shows a flow for an electronic component, bear in mind that anything can be counterfeited. Counterfeiting is a complex criminal enterprise.

* *China photos courtesy of Tom Sharpe & SMT Corporation*

** *Photo courtesy of Basal Action Network*

OSHKOSH DEFENSE

Impact of Counterfeit Parts

Counterfeit parts can cause:

- Personal injury
- Mission failure
- Reduced reliability and product recall
- Potential loss of contracts
- Shutdown of manufacturing lines
- Negative cost and schedule impact
- Penalties for companies and individuals
- Damage to our corporate image

Our defense systems must be of a quality sufficient to protect our soldiers, our friends, our cities and ourselves without failure on a moments notice, anytime, anywhere.
Don't allow the counterfeit part you let get into the system be the one to cause mission failure.

OSHKOSH DEFENSE

Oshkosh Defense – Risk Assessment

Oshkosh Defense primarily integrates assembled and tested electrical and electronic assemblies that we source exclusively from our approved suppliers.

The risk for the introduction of counterfeit electrical and electronic items lies with our suppliers and their component supply chain.

Through this training, Oshkosh Employees and suppliers will be:

- Made aware of general strategies to avoid, detect, & mitigate
- Trained on the Counterfeit Parts Avoidance and Detection system at Oshkosh Defense and their responsibilities in that system

Avoidance:

Most cost effective step in the process

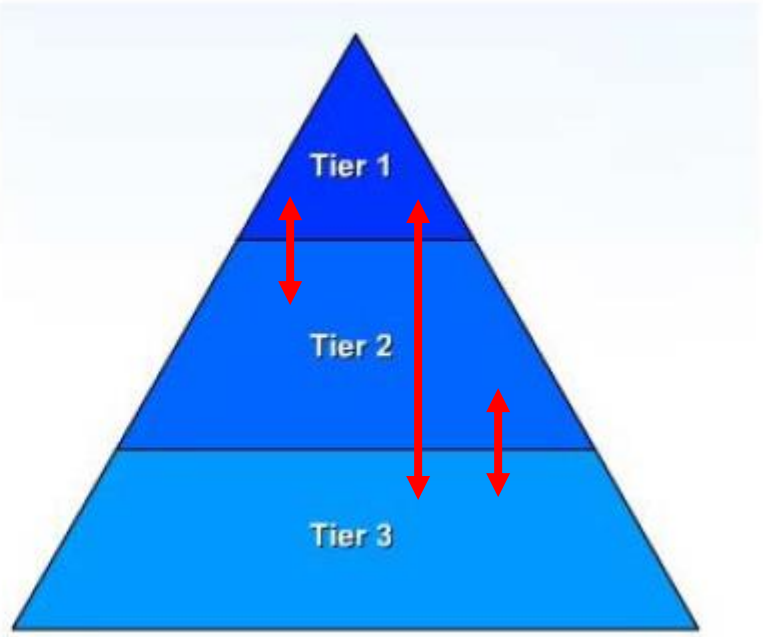
OSHKOSH DEFENSE

How do counterfeit electronic items infiltrate?

The number of suppliers is limited only by the number of companies that can provide the supplies.

However, they are classified in three different tiers:

- Tier 1 - Original Manufacturer or Authorized Manufacturer
- Tier 2 - Authorized Distributor
- Tier 3 - Broker, Independent Distributor, Gray Market



Part surpluses and shortages provide opportunity

- "Buyers" buy excess inventory from original manufacturers, authorized manufacturers, authorized buyers, brokers, and other independent distributors.
- The buyers may sell the excess inventory to other customers or they may sell it back to the same original manufacturers they buy from when the manufacturers have a shortage of items on hand.
- Often those customers sell back what they don't need to the "buyers" who in turn sell them again to other customers.
- Item traceability, authenticity, and accountability become an issue when they change hands so many times.

Tier 3 risks

Independent Distributors are in the business of buying large quantities of overstocked items with the intent to sell and redistribute.

- Stocking Distributors typically have inventories on hand purchased from OEMs and other sources
- Broker Distributors are independent distributors working “just in time” to link supply and demand

Independent Distributors will have less quality control and often operate in what is considered a “Gray Market”

- There are no contract agreements with OEMs
- Gray markets are sometimes used to find the “best deal”
- The parts they purchase may not always be from the OEM’s overstock
- There is not as much control over these items and the chain of custody cannot always be verified to ensure authenticity.
- Whoever is offering the lowest price may be the counterfeiter or the counterfeiter’s distribution chain.

It is recommended that military buyers **avoid** Tier 3 suppliers as normal course of business.

OSHKOSH DEFENSE

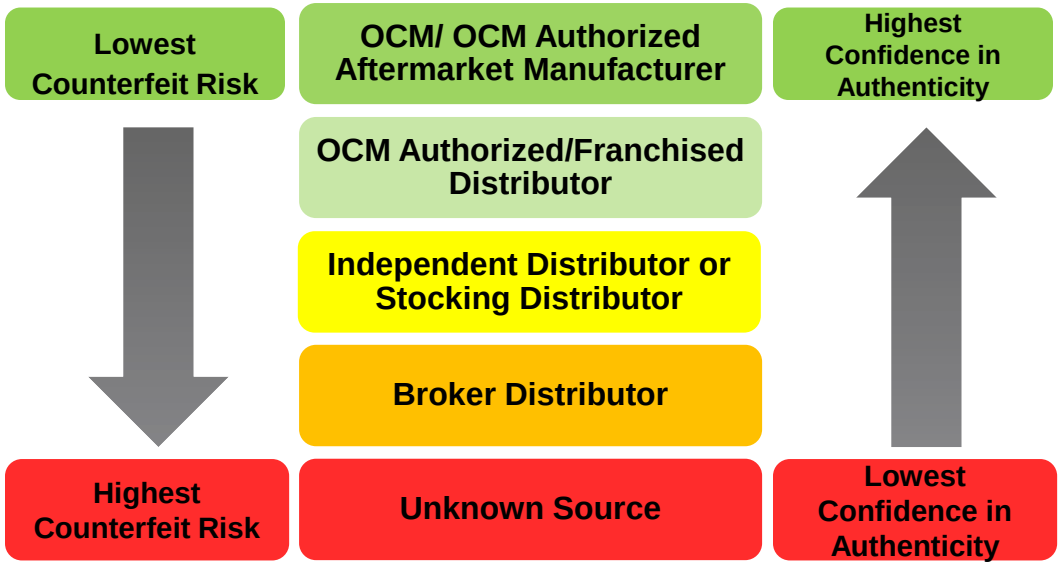
Avoidance Strategies

Government and Industry investigations have shown that the **risks of receiving counterfeit parts varies based on the supplier entity** providing the parts. The risk ladder shown here is a useful reference for understanding the counterfeit risk hierarchy from a procurement or sourcing point of view.

Procuring directly from the Original Component or Equipment manufacturer (OCM/OEM) results in lowest risk of counterfeit.

OCM Authorized Distributors are the new lowest risk. OCM Authorized distributors have documented agreements with a manufacturer to sell their items.

- Authorized distributor status should be verified with the manufacturer.



Counterfeit Avoidance Requirements are contained in Oshkosh Purchase Order Terms and Conditions as well as Quality Requirements. Refer to your specific PO for review of your requirements.

OSHKOSH DEFENSE

Avoidance Strategies

Key Counterfeit Avoidance Strategies include the following:

- **Procurement Process**
  Require the exclusive utilization of OCM's/OEM's or their authorized distributors

- **Chain of Custody**
  Require a documented, unbroken chain of custody from the original source of manufacture for all components provided to Oshkosh, either directly or indirectly as parts included in assemblies delivered to Oshkosh.
  - Anti-counterfeit parts system requirements typically require that suppliers provide OCM/OEM traceability documentation when requested, which would include:
    - OCM/Authorized supplier certificates of conformance
    - OCM/Authorized supplier shipping and receiving documents
    - OCM/Authorized supplier packing slips
- **Supply Chain Management**
  - Flow down counterfeit avoidance strategies, including the use of OCM/OEM authorized sources throughout supply chain.
  - Formally assess sources of supply for compliance.
- **Obsolescence Management and Parts Management Processes**
  - Anticipate obsolescence issues in time to initiate actions such as redesign or lifetime buys.
- **Counterfeit Awareness Training**
  - Provide training in house, and also to suppliers.

OSHKOSH DEFENSE

Oshkosh Defense – Avoidance Strategy

Supply Chain:

Oshkosh Defense requires our suppliers of electrical and electronic assemblies and components to do the following:

- Conduct a risk assessment and have their own avoidance and detection system based on their risk.
- Flow down the DFARS to their supply chain.
- Only purchase electrical and electronic components from Tier 1 and Tier 2 sources.
- Conduct an assessment of their suppliers, and periodically audit and evaluate the avoidance and detection systems in their supply chain.
- Require a documented chain of custody and traceability information for electrical and electronic components in accordance with the DFARS, maintain that information, and make it available to Oshkosh upon request.
- If a part must be sourced from a Tier 3 source, it must be considered suspect until proven authentic through appropriate inspection and/or testing.

OSHKOSH DEFENSE

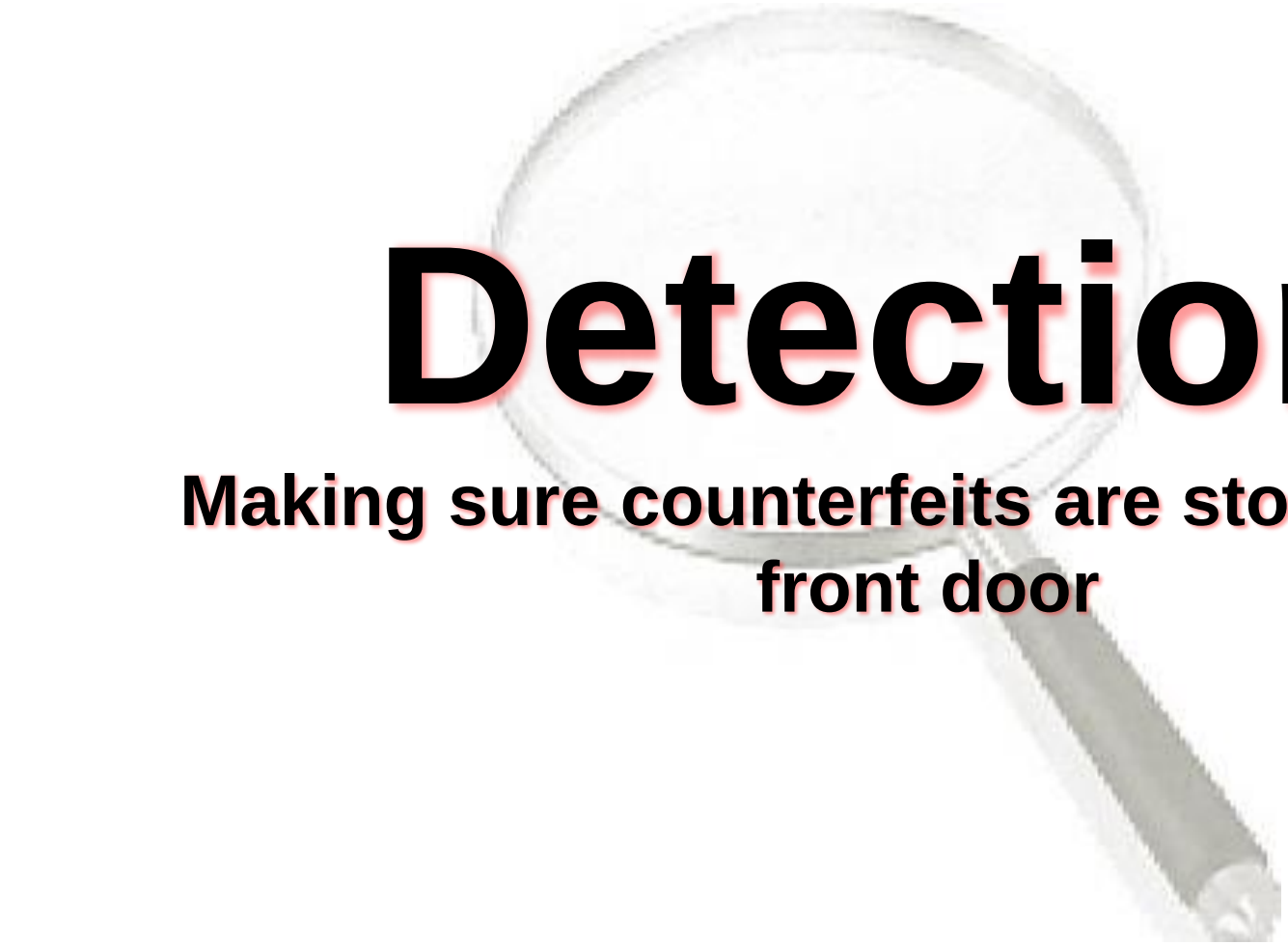
Oshkosh Defense – Avoidance Strategy

Internal:

To enhance the supplier strategy, Supplier Quality will do the following:

- Conduct an assessment of new electrical/electronic items suppliers, including and audit and evaluation of their avoidance and detection system, prior to becoming approved suppliers.
- Periodically assess risk and schedule surveillance audits for electrical/electronic suppliers.
- Conduct an evaluation of the avoidance and detection system any time an electrical/electronic supplier is being audited.

	Question		Objective Evidence
1	Is there a documented purchasing process that ensures all EEE components are purchased in the following order of precedence: a. Only from OEM/OCM, b. Sources with written authority of the OEM/OCM or c. Suppliers that obtain parts exclusively from the OEM/OCM		Procedure is authorized and in place. - 3 Documented evidence of use via PO review. - 5
2	How is the flow down of the appropriate engineering, manufacturing and DFARs requirements to your suppliers of EEE material used in assemblies delivered to Oshkosh communicated?		Evidence of communication via procedure or PO requirement or attachment. - 5
3	How are sources/contractors and subcontractors assessed to determine the risk of receiving, probability of detecting, and the impact if a counterfeit part is installed in the electronic device and its intended function in the end		Documented results of the assessment. - 3 Evidence that the assessment technique used is appropriate. - 3



Detection:

Making sure counterfeits are stopped at the front door

OSHKOSH DEFENSE

Identifying the Types of Items

Counterfeit items can be hard to spot. In many cases, they look like the real thing and may even work like the real thing, or at least during initial inspections, although that may not last.

There are a limited number of ways to misrepresent an item:

- Knock-offs: look just like the real thing only with lower grade material
- Refurbished parts: previously used parts salvaged from scrapped material polished and cleaned.
- Re-marked: incorrect die, different labels or inferior material.
    - Sanded
    - Micro-blasted component surface
- Mislabeled: falsifying documents or labeling as something it's not.

OSHKOSH DEFENSE

Visual Inspection Strategies

Those handling the shipping and receiving of packages are the organization's first line of defense against receiving counterfeit items.

Some of the key things that can be done at the receiving area include:

- Before the package is opened, look at the shipping label. Is it over-taped; does it look like something is underneath the label? Are any of the words misspelled or are the logos not exactly right? Is there smearing of the print?
- How's the actual package look? Is it ripped or torn? Is there excess tape on it; does it look like it was dropped or damaged?
- Who's the package being shipped to? Do they know it's coming? Can they tell you the size and expected weight?
- With the increasing sophistication of counterfeiters, these types of anomalies are less likely to occur and advanced inspection or testing is necessary to confirm counterfeit materiel.

OSHKOSH DEFENSE

Certification and Traceability Strategies

- Ensure the item is from the seller and manufacturer listed in the purchase order.
- Ensure the serial number, part number, lot codes, and data codes listed on the shipping label are included with or on the actual item and do not appear to have been altered or tampered with.

- Certificate of Conformance (C of C)
  - **Is** a document a manufacturer or supplier uses to certify that the part meets all of the MIL-PRF 19500 and all other requirements spelled out in the contract.
  - **Is not** traceability information

- Traceability information
  - Part traceability consists of the names and locations of everyone within the supply chain that have had contact with the part.
  - If parts do not have traceability, the risk is higher that the item may be counterfeited.

OSHKOSH DEFENSE

Testing Strategies

The more critical or sensitive the item the more testing and evaluation should be done:

There are two types of testing:

Non-invasive or Non-destructive

- Visual inspection
- Touch test
- Microscope
- Test for Blacktopping
- X-ray

Invasive or Destructive

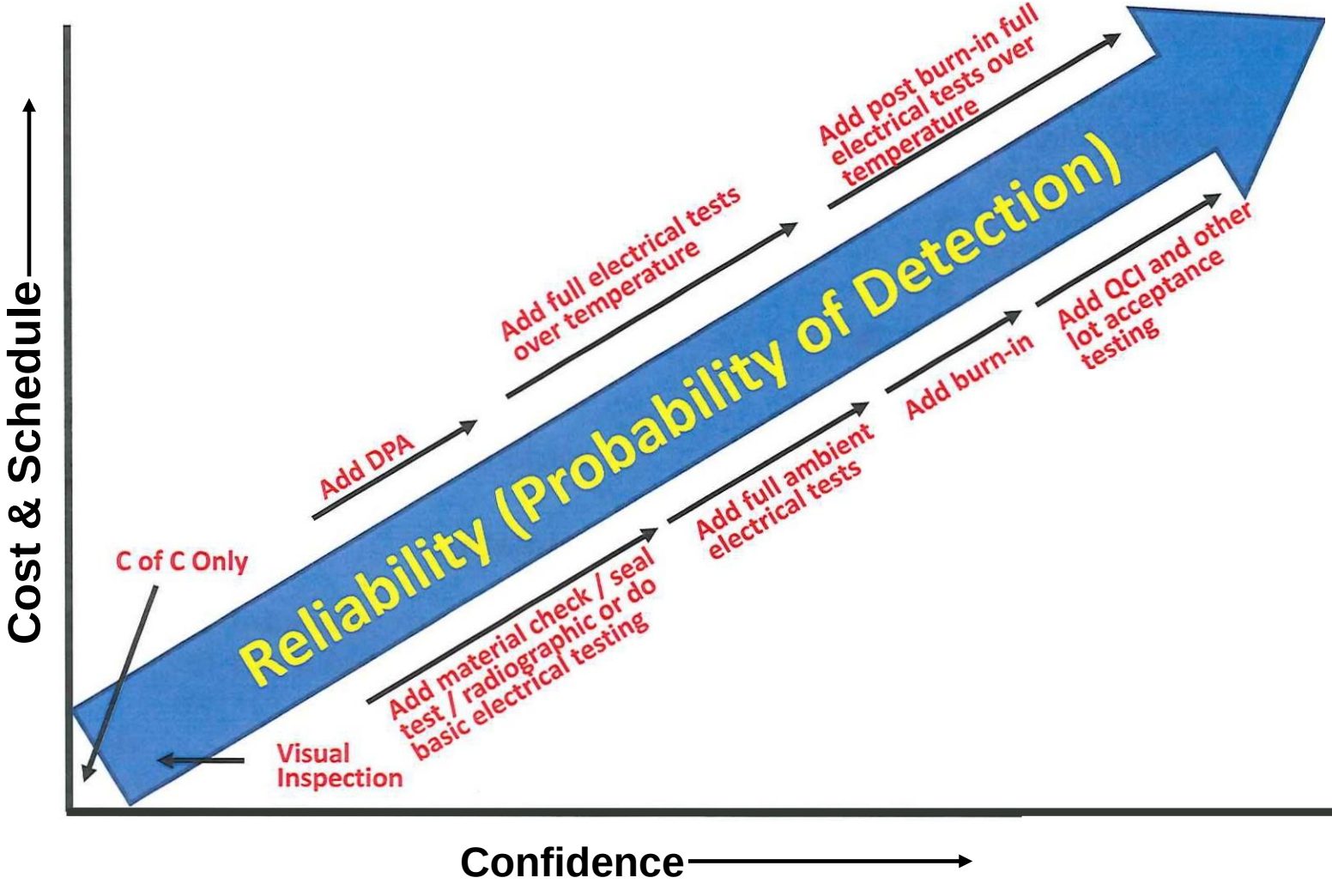
- Items to be destructively tested are typically sent out to labs or other experts to perform the tests.

SAE AS6171 should be used as a reference as it provides standardized testing and detection requirements

OSHKOSH DEFENSE

Probability of Detection

This chart shows that more time, effort, and expenditure on validating parts increases the Level of confidence that the part is authentic.



DETECTION: Suspect “Warning Flags”

Listed below area few examples of some counterfeit “warning flags” that can indicate to your sourcing, receiving, inspection, and test groups that there could be a counterfeit issue with a part or material.

The bottom line: the more flags you see, the more suspicion you should have that a part or material may not be authentic. If things don’t look right – Investigate!

Review the warning flags shown here:

- Item coming from source other than the OCM or authorized sources from suspect locations (e.g., China)
- Price too low/significantly different from history
- Scarce items are suddenly available
- Chain of ownership unverifiable
- No certificate of conformance
- Obsolete item
- Unknown supplier
- Non-homogeneous log
- Prohibited materials present
- Item marking issues:
  - Does not match similar items
  - Alterations/resurfacing
  - Incomplete
  - Wrong size/location/methods
  - Quality difference
  - Lot number/date code issue
- Package/Construction Issues:
  - Size/shape/color/finish/ materials
  - Evidence of rework/repair/ refinishing/resurfacing
  - Poor quality

Additional inspection recommendations that can identify red flags can be found In SAE standards AS5553 or AS6174

OSHKOSH DEFENSE

Oshkosh Defense – Detection Strategy

Supply Chain:

- Document a process for inspection, and when appropriate testing, of electrical and electronic materials prior to acceptance.
- Requires a process for detection prior to acceptance at their supply chain of electrical and electronic components.
- Requires a special process for inspection/testing and handling of material purchased from the Tier 3 sources, and only purchase from a Tier 3 source if there is a business need that warrants the additional risk.
- Requires an appropriate, risk based, testing plan for the end item prior to delivery to Oshkosh.
- Required to maintain complete records of traceability that can be provided to Oshkosh Defense within two business days.
- Provide internal and sub-tier training on detection strategies.

OSHKOSH DEFENSE

Oshkosh Defense – Detection Strategy

Internal:

Supplier Quality

- Responsible for communicating any special inspections or detection requirements for receiving inspection through the inspection notes in JDE. (QCP-0267)

Receiving Inspection

- Review inspection notes in JDE and perform any counterfeit detection specific product inspections or documentation reviews when required. (QCP-0045)

Everyone

- **Do not** open or attempt to internally inspect delivered components
- **Do** be aware of “red flags” and discuss any concerns with the supplier quality manager

Mitigation:

Minimizing damage to our programs and reputation

OSHKOSH DEFENSE

Mitigation Strategies: When solid traceability to the OCM cannot be established.

- Ensure processes are in place to quarantine parts that require testing and verification until they are verified as authentic – treat them as suspect until evidence proves otherwise.
- Mitigation Strategies and Authenticity testing should be developed using a risk-based approach.

- Cross checking Independent Suppliers and part numbers against the GIDEP and/or ERAI can be beneficial in the evaluation of risk that given part or supplier may be introducing a high risk for counterfeit.

TEST IF YOU CANNOT TRACE!

OSHKOSH DEFENSE

Counterfeit Item Mitigation Strategies

If you suspect that a counterfeit item may have infiltrated your supply chain, the following items must be addressed immediately as initial steps in an effort to minimize or bound the impact:

Quarantine affected parts:

- Locate any parts in stock and on assemblies, ensure they are quarantined and clearly marked as nonconforming.
- Identify any suspect items that may have left your facility.
- Notify your Oshkosh procurement representative

Gather all traceability or chain of custody information or authenticity testing records associated with the suspect part:

- This may include:
  - Purchase order
  - Certificates of Conformance
  - Test Data
  - Inspection or DPA reports
  - Other information relevant to detection
- Review information to assist with bounding the issue.

Verify the item is or is not counterfeit:

- Conduct additional testing in an effort to confirm if the item is counterfeit.
- Engage the manufacturer of the part for assistance to the extent possible

Remediation/Corrective Action:

- If required, a plan for Rework/Replacement/Repair of fielded product will be determined in conjunction with the Oshkosh program team, Oshkosh legal, and Customer input.

OSHKOSH DEFENSE

Disposition – Protecting supply chain and ourselves

Disposition

Disposition – Protecting supply chain and ourselves

Counterfeiting invariably involves fraud (often from an upstream supplier that can be several tiers removed), therefore coordination with appropriate officials must take place prior to making any disposition of parts.

If the suspect items are contained within your facility, best practices dictate:

- Maintaining counterfeit parts or materials in quarantine, clearly identified as non-conforming/counterfeit product, pending a review by your organization's management and legal representation.
- Counterfeit parts should not be returned to the supplier in such a way that they could be reintroduced into the supply chain to be sold again to another victim.
- Legal authorities may be contacted to initiate an investigation into the counterfeiting activity. If an investigation is initiate, parts may be required as evidence.

In cases where product may have been delivered to Oshkosh and returned for rework or replacement, suspect components must not be disposed of until such time as it is determined that legal authorities will not require the parts for an investigation.

Do not throw parts away until it is clear they aren't needed for investigation.

OSHKOSH DEFENSE

Oshkosh Defense – Mitigation & Disposition

Supply Chain:

- Must document a method to quarantine suspect material; supply chain must:
  - Prevent shipment of assemblies that may be suspect to customers
  - Identify, segregate and control suspect material
  - Prevent return of suspect parts/components to suppliers
  - Ensure control is maintained until authenticity is confirmed

Oshkosh Defense – Mitigation & Disposition

Internal:

- Any suspect counterfeit material is to be market “Suspect Counterfeit” and a Nonconforming Material Ticket will be entered with “Suspect Counterfeit” in the defect description.
- When reviewing material for disposition, any Material with “Counterfeit” or “Suspect counterfeit” in the defect description MUST be dispositioned to MRB.
- Material will be controlled by the MRB as non-conforming, suspect counterfeit material and will not be sent to the customer.
    - The MRB will work with the supplier of the items to determine the investigation plan for suspect material.
    - Additionally, these assemblies will not be returned to the supplier until MRB has reviewed and approved the control measures the supplier will take to prevent the re-use or distribution of the counterfeit or suspect counterfeit EEE components until proper disposition can be determined.
    - MRB will also not “return to stock” any material until it has determined it to be authentic.

OSHKOSH DEFENSE

Communication:

Communication: Timely & Effective Reporting

Oshkosh requires suppliers to provide notification if it is suspected that a counterfeit item has been delivered to us. This notification must be directed to your Oshkosh Procurement Representative.

Ensure that communication and reporting of counterfeit issues is timely and effective. Structures that may require communication include:

- Internal organizations:
  - Program
  - Legal
  - Business Operations
- Customers
- Criminal investigators
- Government reporting (e.g., GIDEP)*
- Industry programs (e.g., ERA)

*Oshkosh strongly encourages all eligible suppliers to join GIDEP for reporting and monitoring of counterfeit and other nonconformance alerts. Visit www.GIDEP.org for information on joining GIDEP.

Reference AS5553 Appendix G for additional information and guidelines for reporting.

OSHKOSH DEFENSE

DOD and Oshkosh Combating Counterfeits: Potential consequences and Liabilities

- Section 818 of the 2012 Defense Authorization Act mandates requirements concerning the detection and mitigation of counterfeit parts. The DOD is required by law to:
  - Make costs of counterfeit rework and corrective actions unallowable
  - Require that counterfeit risk be managed throughout the supply chain
  - Implement criminal penalties and possible debarment for intentional failure to exercise adequate counterfeit prevention methods.

Counterfeit Risk Must Be Managed Throughout the Supply Chain.

OSHKOSH DEFENSE

Conclusion

- The counterfeiting of electronic parts and materials is a serious threat and can compromise the integrity of the important products we provide
- The use of Original Component or Equipment manufactures and their authorized sources results in the least risk for counterfeit items infiltrating our products.
- If needed, parts or materials cannot be acquired from low risk sources in order to fulfill your Oshkosh purchase order, you must notify your procurement representative, and parts must be authenticated in accordance with the terms and conditions of your contract.
- If you suspect counterfeit items may have been supplied to Oshkosh, you must notify your Oshkosh procurement representative immediately.
- Counterfeit risk must be controlled throughout the entire supply chain.
- Thank you for your continued efforts to ensure counterfeit components do not infiltrate our supply chains.

OSHKOSH DEFENSE

APPENDIX

Reference Info for Counterfeit Parts

- *Department of Commerce*
  - *Defense Industrial Base Assessment Counterfeit*
    http://www.bis.doc.govlindex.php!forms-documents/doc view/37-defense-industrial base-assessment-of-counterfeit-electronics-2010
- *IDEA-1004-C ((Electronic Components Inspection Manual"*
  - *Independent Distributors of Electronics Association*
    http://www.idofea.org
- *DOE G 414.1-3 "Suspect/Counterfeit Items Guide"*
  http://www.directives.doe.govlpdfsldoeldoetextlnewordl4141g4141-3.pdf
- *Suspect I Counterfeit Items Awareness Training*
  http:1lwww.hss. energy gov/CSAICSP!sci
- *Coalition Against Counterfeiting and Piracy (CACP) type toolkit*
  http://www.theglobalipcenter.com!pages/coalition-against-counterfeiting-and-piracy
- *AS5553 - Counterfeit Electronic Parts*
  http://www.sae.orgltechnical/standards/AS5553
- *AS6081 - Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition -Distributors Counterfeit Electronic Parts; Avoidance Protocol, Distributors*
  http://standards.sae.org/as6081/

OSHKOSH DEFENSE

GIDEP

- Participation in the Government Industry Data Exchange Program (GIDEP) is an important risk prevention step
- Suppliers with counterfeit risks, suspect or confirmed counterfeits, should enter that part incident into GIDEP
- Purpose is to share risks with DOD and industry to ensure appropriate risk mitigation measures are being taken
- For additional guidance, go to the GIDEP members website (http://www.gidep.org). Non-participants may contact the GIDEP Help Desk @ (951) 898-3207 for guidance

DOD Provides Tools to Reduce Industry Risks/Costs

OSHKOSH DEFENSE

INNOVATION DRIVES FORWARD




Thank You

OSHKOSH DEFENSE