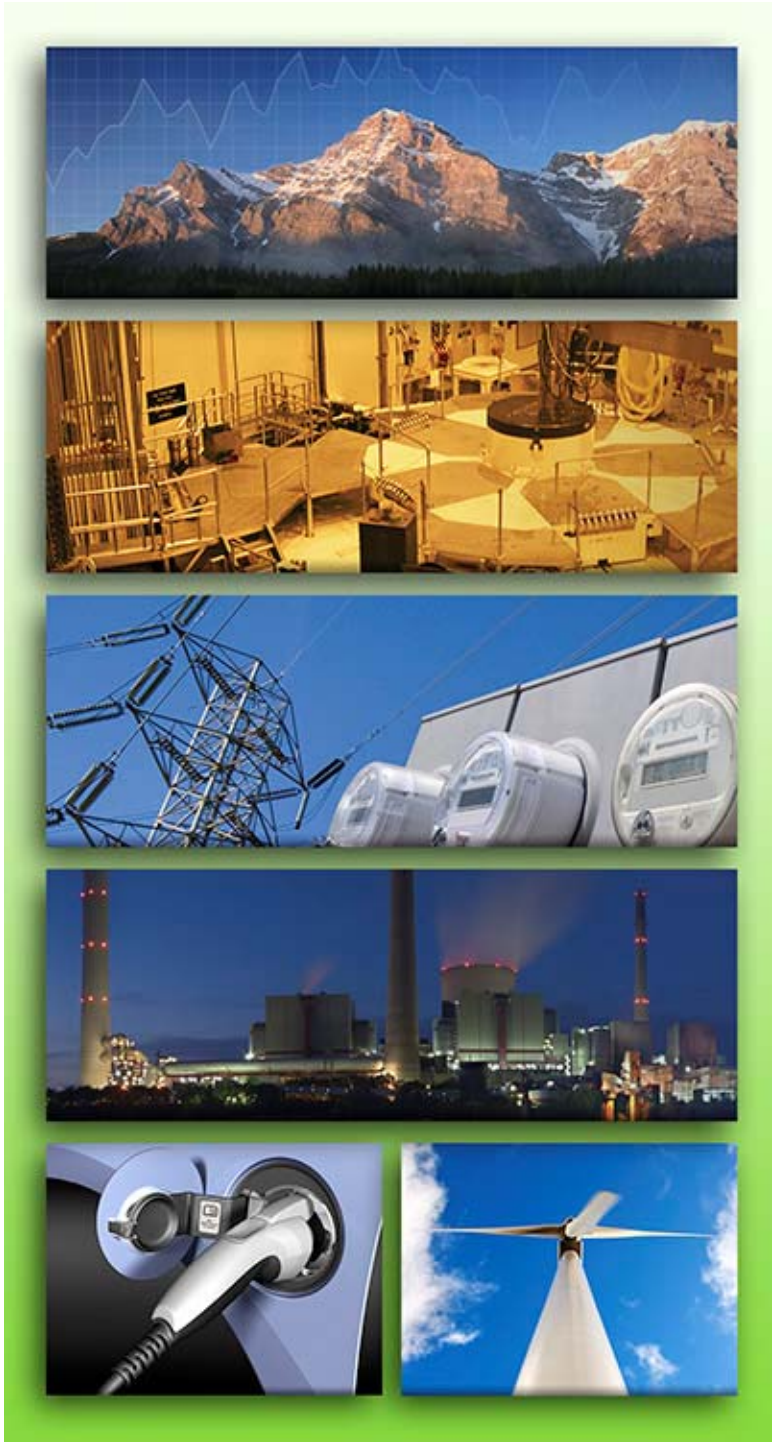


EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Counterfeit and Fraudulent Items – Mitigating the Risk

NRC Workshop on Vendor Oversight for New Reactor Construction

June 17, 2010
New Orleans Marriot

Marc Tannenbaum, EPRI Project Manager

What are we concerned about?

Counterfeit and Fraudulent Items

- Counterfeit
  - Intentionally manufactured or altered to imitate a legitimate product without the legal right to do so
  - A counterfeit item is one that has been fabricated in imitation of something else with purpose to defraud by passing the false copy for genuine or original or is an items copied without the legal right or authority to do so

- Fraudulent
  - Items that are intentionally misrepresented with intent to deceive. Fraudulent items include item provided with incorrect identification or falsified or inadequate certification.

What are we concerned about?

- Suspect items are items that are suspected of being counterfeit or fraudulent
  - It may not always be cost effective to verify if a suspect item is indeed counterfeit, fraudulent or substandard
    - Legally, it may not be appropriate to call an item counterfeit or fraudulent unless it is verified as such
  - Simply obtaining an authentic item or one that complies with the specification may be the prudent course of action
    - Conclusive investigation can be very expen$ive

Why should we Worry about Counterfeits Today?

More than $272.7 million worth of counterfeit goods seized in 2008 in the U.S.

- 14,000 seizures in 2008
- 38% Increase in value over 2007
- Major league baseball caps
- Integrated circuits for fighter jets
- Commercial airliner parts

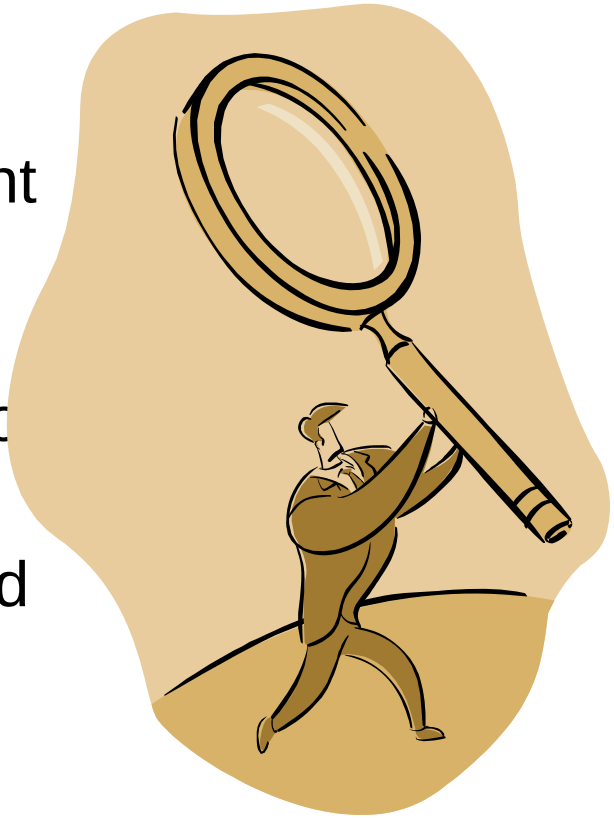
It is estimated that counterfeiting costs the U.S. 750,000 jobs annually

Recent Shots on Goal in the Nuclear Industry

- Fasteners
- Valves
- Electronic components
- Circuit Breakers

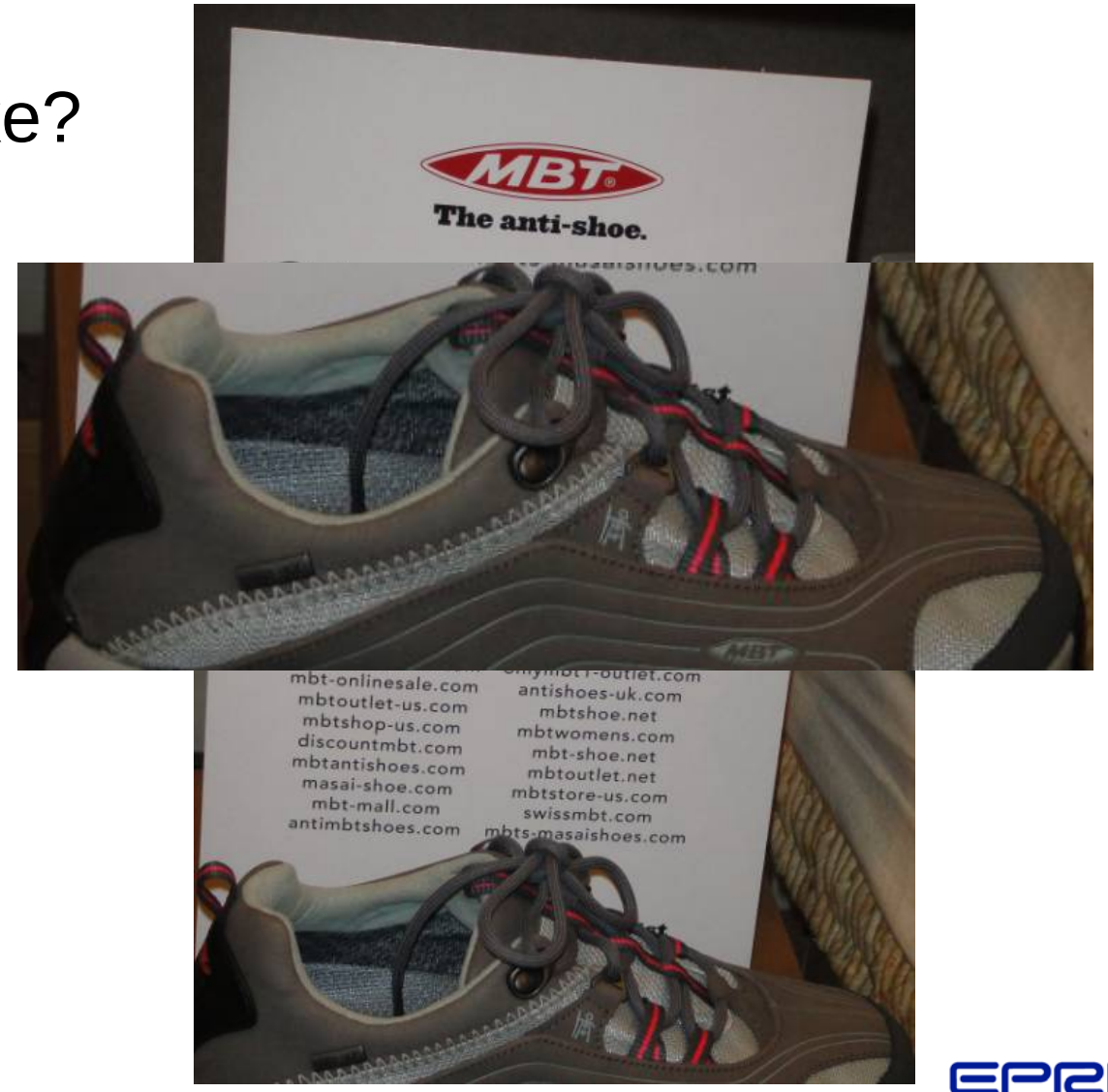
Is it difficult to spot a counterfeit?

- You need to know when to look closely
  - Knowledge of the supplier can be limited . . . is the supplier . . .
    - The original equipment/component manufacturer (OEM/OCM)?
    - The Authorized by original equipment manufacturer (OEM) to sell or distribute
    - Aware of counterfeiting issues and potential impact on their products
    - Located in a region with established risk
  - You need to know what to look for
    - Data on other incidents



Let’s take a look at some examples . .

Real or Fake?

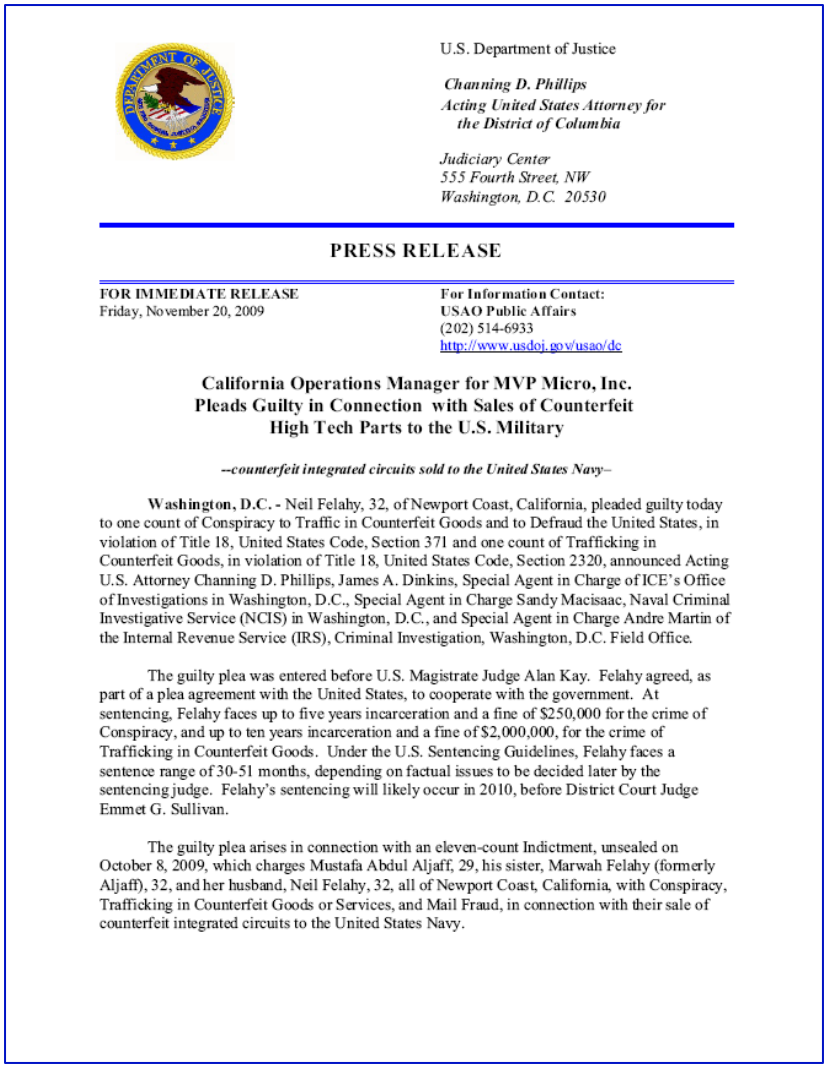


EPRI ELECTRIC POWER RESEARCH INSTITUTE

August 2009 – Fasteners with Unsubstantiated CMTRs

Integrated Circuits

- March-June 2009 Integrated Circuits sold to the US Navy as
  - MVP Micro
  - BeBe Star
  - Consulting, Inc.
  - Red Hat Distributors
  - Red Hot Distributors
  - RH Distributors
  - Force One Electronics
  - Labra Electronics
  - Becker Components
- Conviction - November 2009



U.S. Department of Justice

Channing D. Phillips
Acting United States Attorney for
the District of Columbia

Judiciary Center
555 Fourth Street, NW
Washington, D.C. 20530

PRESS RELEASE

FOR IMMEDIATE RELEASE
Friday, November 20, 2009

For Information Contact:
USAO Public Affairs
(202) 514-6933
http://www.usdoj.gov/usao/dc

California Operations Manager for MVP Micro, Inc. Pleads Guilty in Connection with Sales of Counterfeit High Tech Parts to the U.S. Military

--counterfeit integrated circuits sold to the United States Navy--

Washington, D.C. - Neil Felahy, 32, of Newport Coast, California, pleaded guilty today to one count of Conspiracy to Traffic in Counterfeit Goods and to Defraud the United States, in violation of Title 18, United States Code, Section 371 and one count of Trafficking in Counterfeit Goods, in violation of Title 18, United States Code, Section 2320, announced Acting U.S. Attorney Channing D. Phillips, James A. Dinkins, Special Agent in Charge of ICE's Office of Investigations in Washington, D.C., Special Agent in Charge Sandy Macisaac, Naval Criminal Investigative Service (NCIS) in Washington, D.C., and Special Agent in Charge Andre Martin of the Internal Revenue Service (IRS), Criminal Investigation, Washington, D.C. Field Office.

The guilty plea was entered before U.S. Magistrate Judge Alan Kay. Felahy agreed, as part of a plea agreement with the United States, to cooperate with the government. At sentencing, Felahy faces up to five years incarceration and a fine of $250,000 for the crime of Conspiracy, and up to ten years incarceration and a fine of $2,000,000, for the crime of Trafficking in Counterfeit Goods. Under the U.S. Sentencing Guidelines, Felahy faces a sentence range of 30-51 months, depending on factual issues to be decided later by the sentencing judge. Felahy's sentencing will likely occur in 2010, before District Court Judge Emmet G. Sullivan.

The guilty plea arises in connection with an eleven-count Indictment, unsealed on October 8, 2009, which charges Mustafa Abdul Aljaff, 29, his sister, Marwah Felahy (formerly Aljaff), 32, and her husband, Neil Felahy, 32, all of Newport Coast, California, with Conspiracy, Trafficking in Counterfeit Goods or Services, and Mail Fraud, in connection with their sale of counterfeit integrated circuits to the United States Navy.

Steel Shapes and Products

- February 2009 – Radioactive Steel Shapes and Products
  - Authorities in Germany find highly radioactive products at a port including:
    - Bars
    - Valves
    - Elevator Buttons
  - Likely the result of Cobalt 60 from “scrap metal” being introduced to blast furnaces during fabrication
    - Cobalt 60 is used in medical and food irradiation applications

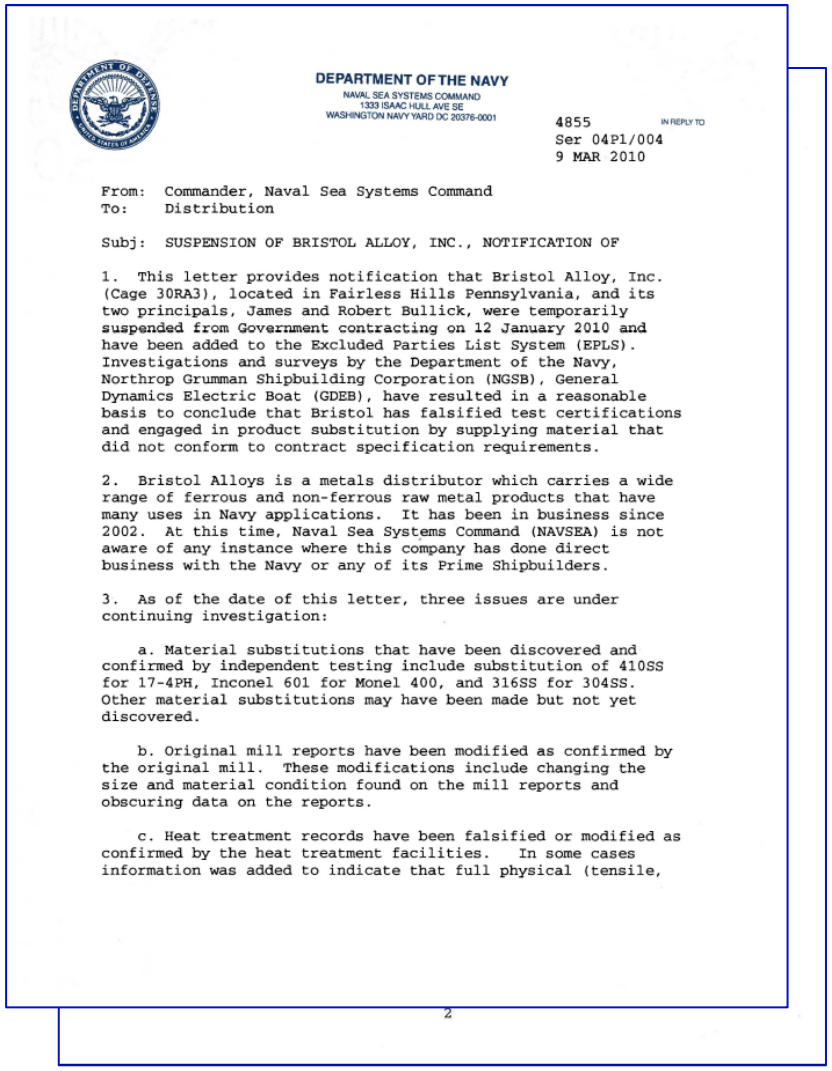
Sources: www.spiegel.de/international/world/0,1518,607840,00.html
http://www.thehindu.com/2009/03/02/stories/2009030255471100.htm

Bearings

- April 2009 – SKF Bearings
- Counterfeit SKF bearings seized in Czech Republic
  - Over 30 tons of product
  - Non-authorized dealer
  - Other bearing manufacturer's items also seized

Source: http://investors.skf.com/files/press/skf/200906112159-2.pdf

Ferrous and Non Ferrous Raw Materials



DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVE SE
WASHINGTON NAVY YARD DC 20376-0001

4855 IN REPLY TO
Ser 04P1/004
9 MAR 2010

From: Commander, Naval Sea Systems Command
To: Distribution

Subj: SUSPENSION OF BRISTOL ALLOY, INC., NOTIFICATION OF

1. This letter provides notification that Bristol Alloy, Inc. (Cage 30RA3), located in Fairless Hills Pennsylvania, and its two principals, James and Robert Bullick, were temporarily suspended from Government contracting on 12 January 2010 and have been added to the Excluded Parties List System (EPLS). Investigations and surveys by the Department of the Navy, Northrop Grumman Shipbuilding Corporation (NGSB), General Dynamics Electric Boat (GDEB), have resulted in a reasonable basis to conclude that Bristol has falsified test certifications and engaged in product substitution by supplying material that did not conform to contract specification requirements.

2. Bristol Alloys is a metals distributor which carries a wide range of ferrous and non-ferrous raw metal products that have many uses in Navy applications. It has been in business since 2002. At this time, Naval Sea Systems Command (NAVSEA) is not aware of any instance where this company has done direct business with the Navy or any of its Prime Shipbuilders.

3. As of the date of this letter, three issues are under continuing investigation:

a. Material substitutions that have been discovered and confirmed by independent testing include substitution of 410SS for 17-4PH, Inconel 601 for Monel 400, and 316SS for 304SS. Other material substitutions may have been made but not yet discovered.

b. Original mill reports have been modified as confirmed by the original mill. These modifications include changing the size and material condition found on the mill reports and obscuring data on the reports.

c. Heat treatment records have been falsified or modified as confirmed by the heat treatment facilities. In some cases information was added to indicate that full physical (tensile,

2

- March 2010
- Bristol Alloy, Inc.
  - "Modified" CMTRs
  - 316ss for 304ss
  - 410ss in lieu of 17-4PH
  - Inconel 601 for Monel 400
  - Falsified heat treat data
  - Falsified physical & chemical testing
  - Obscured data on original mill reports

Why has there been relatively little impact in the commercial nuclear generation industry?

- Our operating environment and culture
  - Robust QA programs – Existing precautions
  - Robust supplier controls and receiving inspections
  - Safety culture and safety-conscious work environments
  - Configuration management practices for quality and non-quality items

- The vintage of our equipment has insulated our operating fleet
  - Not enough profit potential (customer demand) to make it worth counterfeiters' time
  - Counterfeiters go after recognized, high-demand items

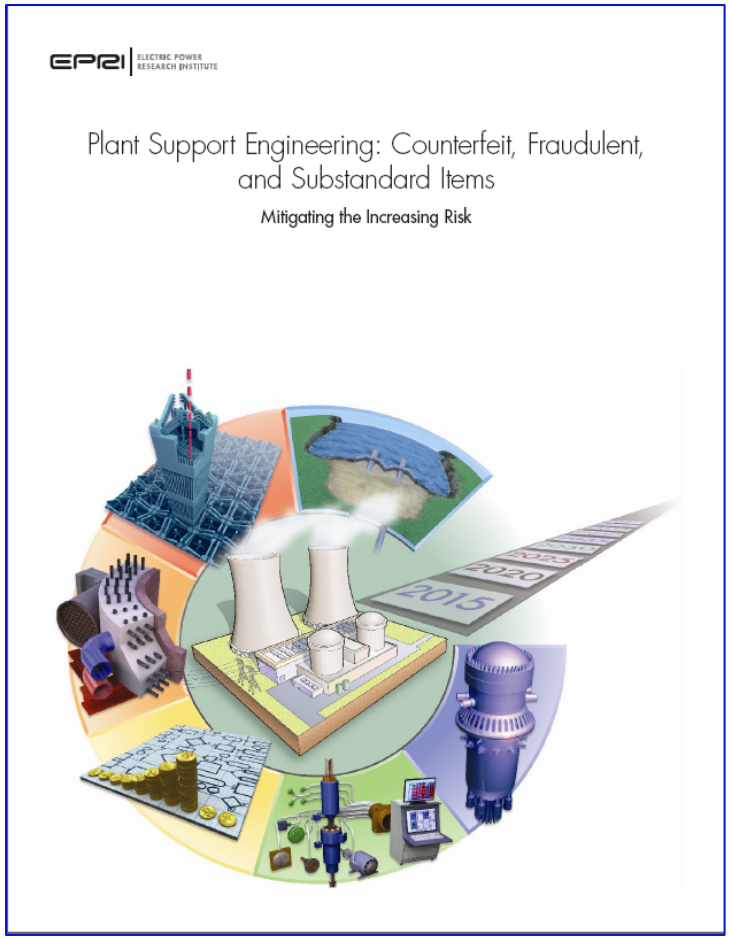
What are we doing about it?

Historical Initiatives

- Concern in the 1980's was addressed in:
  - U.S. NRC Generic Letter 89-02
    - *Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products*
  - U.S. NRC SECY 89-010
    - Advance Notice of Proposed Rulemaking, "*Acceptance of Products Purchased for use in Nuclear Power Plant Structures, Systems, and Components*
  - U.S. NRC Information Notice 89-70
    - *Possible Indications of Misrepresented Vendor Products*
  - EPRI NP-6629
    - Appendix C, *Identifying Substandard/Fraudulent Items*

Counterfeit, Substandard and Fraudulent Items 1019163

- Completed in October 2009
  - Close coordination with NRC, NUPIC, DOE
  - Rollout January 12 & 13 in Charlotte
- Following-up with development of a CFSI Database
- Working closely with NRC, DOE, INPO



Counterfeit, Substandard and Fraudulent Items 1019163

- Rollout was coordinated with NRC, INPO, and included hands-on training

Counterfeit, Fraudulent, and Substandard Items: Mitigating the Increasing Risk

- Key Points
  - Establish a Scope of Concern for your organization
  - Continue to apply existing guidance
  - Educate buyers, procurement engineering, receiving personnel, maintenance and craft
  - Educate suppliers and enhance communication
    - New questions for suppliers
  - Identify at-risk procurements
  - Develop a CFSI Response plan

  - The industry must address this issue as a community moving forward

Conclusions on CFSI's

- Serious risk exists, and it is increasing
- We need to share information in the future
- Develop a response plan
  - What do you do when you find a potential CFSI?
  - To whom do you report it?
- We can take actions now to reduce our risk
  - Training & awareness
  - Enhanced communication between suppliers and customers
  - Enhanced supplier qualification
  - Identify scope of concern
  - Enhanced inspection

Blueprint for the future

- EPRI is developing an industry database in cooperation with INPO
  - Capture known incidents from the nuclear industry
    - Plants
    - Suppliers
  - Capture known incidents from other industries
    - Construction and Engineering Firms
    - Department of Energy
    - Government Industry Data Exchange Program
  - Automated screening and feedback
    - Equipment Level (PKMJ / POMS)
    - Stock Code Level (Scientech / RAPID)
  - “Google” search capabilities

What Can You do Mitigate Risk?

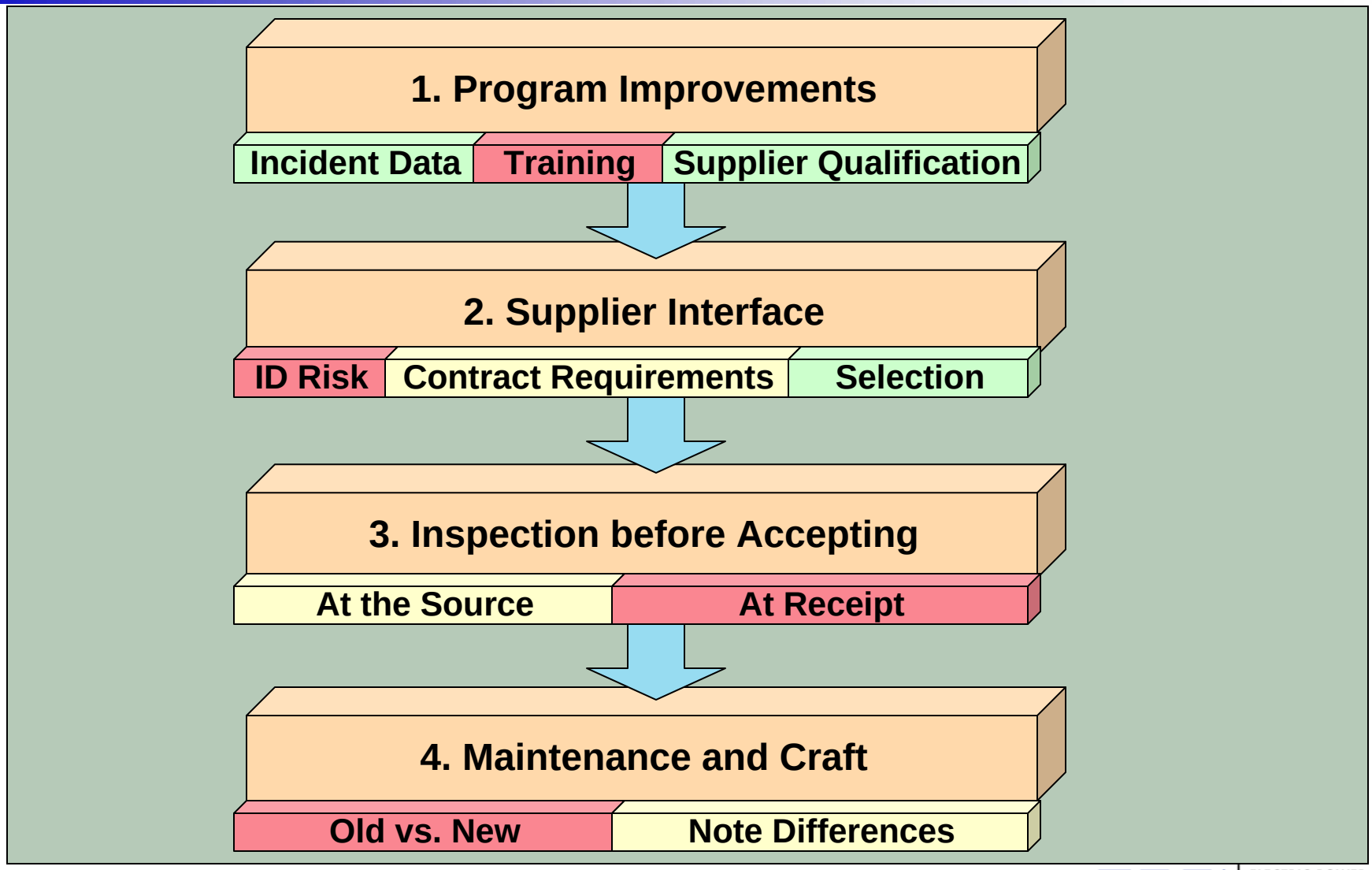
Figure VII-28: Top Ten Reasons For Counterfeits Entering the Supply Chain	
Less Stringent Inventory Management by Parts Brokers	179
Greater Reliance on Gray Market Parts by Brokers	168
Greater Reliance on Gray Market Parts by Independent Distributors	152
Insufficient Chain of Accountability	141
Less Stringent Inventory Management by Independent Distributors	139
Insufficient Buying Procedures	124
Inadequate Purchase Planning by OEMs	117
Purchase of Excess Inventory on Open Market	113
Greater Reliance on Gray Market by Contract Manufacturers	107
Inadequate Production by OCM	105
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, May 2009.	

Source: U.S. Department of Commerce Bureau of Industry and Security Office of Technology Evaluation Defense Industrial Base Assessment: Counterfeit Electronics, January 2010

What You Can do to Mitigate Risk

- Enhancements Recommended by the 1980s Nuclear Industry Initiatives
  - Increased engineering involvement in the procurement process, including assessments (audits and surveys) of suppliers
  - Increased awareness of counterfeiting and fraud, and implementing guidance in NRC IN 89-70 and EPRI NP-6629, Appendix C
  - Sharing of objective information regarding procurement in industry forums
  - Procure item from the original equipment manufacturer or authorized distributor whenever possible
    - When not possible, establish product performance by traceability to the OEM or testing and inspection
  - Establish acceptance criteria at the front end of the procurement process Establish acceptance criteria at the front end of the procurement process

What You Can do to Mitigate Risk



What Can be done in your organization to Mitigate Risk?

- Establish a Scope of Concern
- Implement barriers through enhanced processes and procedures
  - Existing Guidance
  - Supplier Selection
  - Procurement Document Requirements and descriptions
  - Bid Evaluation
  - Identify and address at-risk procurements
  - Inspection
  - Disposal of rejected items and scrap
- Training and Awareness
- Locate sources of information on known counterfeits in your product types or industry and make it readily available to the right people in your organization
- Develop a CFSI Response Plan

What should be included in the Scope of Concern?

Integrated Circuits

Bearings

Piping

Fasteners

Circuit Breakers

MCCBs

Capacitors

Worm Gears

Pumps

Tubing

Flanges

Machined Parts

Valves

Tools

Pipe Fittings

Anti Rotation Keys

1E Components

Sealants

Safety Equipment

Structural Steel

Relays

Fire Protection Equipment

Scope of Concern

Do we only need to worry about counterfeit items in critical equipment applications?

Counterfeiting and fraud can impact everything we purchase

- **Serious consequences can result if we use counterfeit items that are not even plant equipment or parts . . .**
  - Consider the following examples of counterfeit items identified in DOE facilities:
    - Rigging Hardware
    - Ammunition
  - What could happen if these items are counterfeit?
  - Could impact on the plant be significant?

Scope Considerations

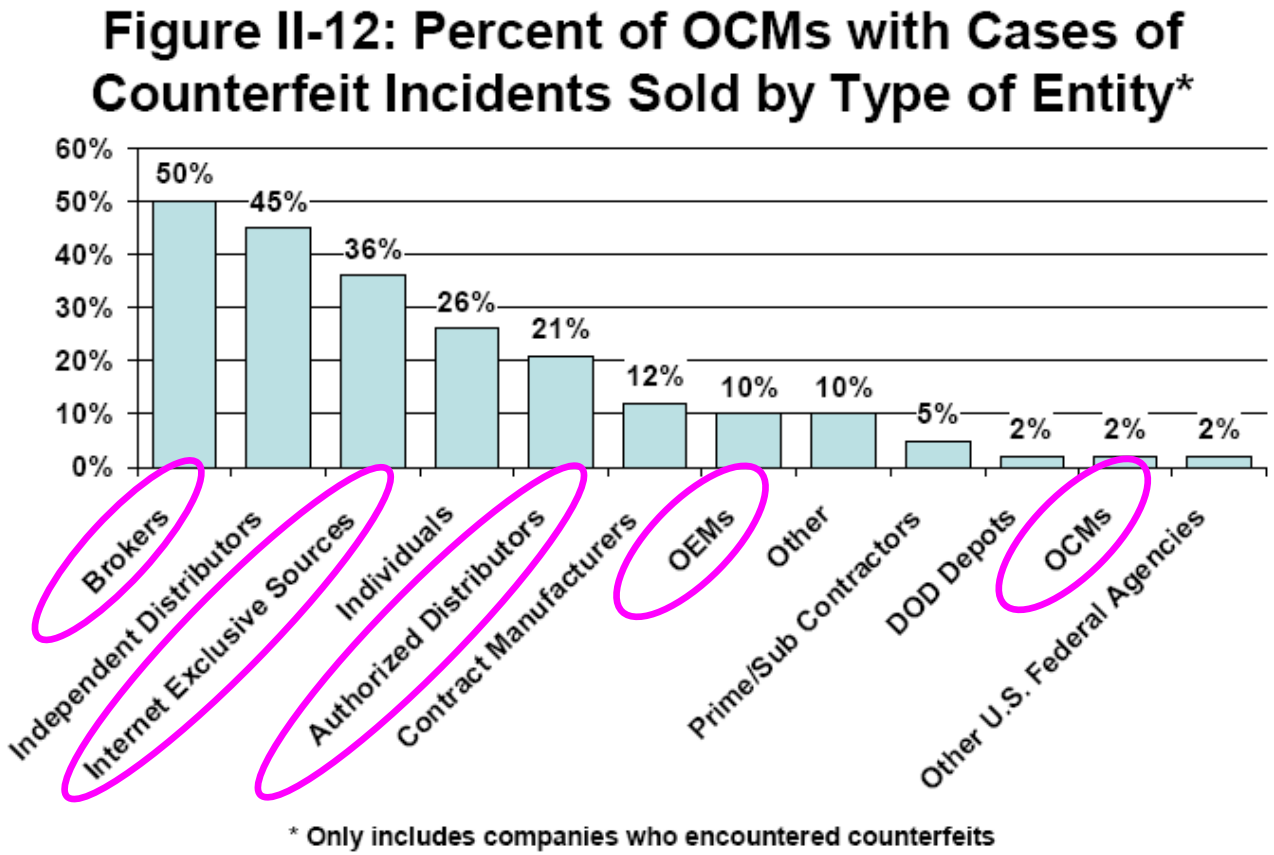
- Operational Equipment
  - Electronics
  - Spare parts
  - Spare components
  - Consumables (lubricants, gaskets, sealants, etc.)

- Maintenance Support
  - Personnel Safety Equipment
  - Lifting and Rigging Equipment
  - Tools

- Security
  - Weapons and Ammunition

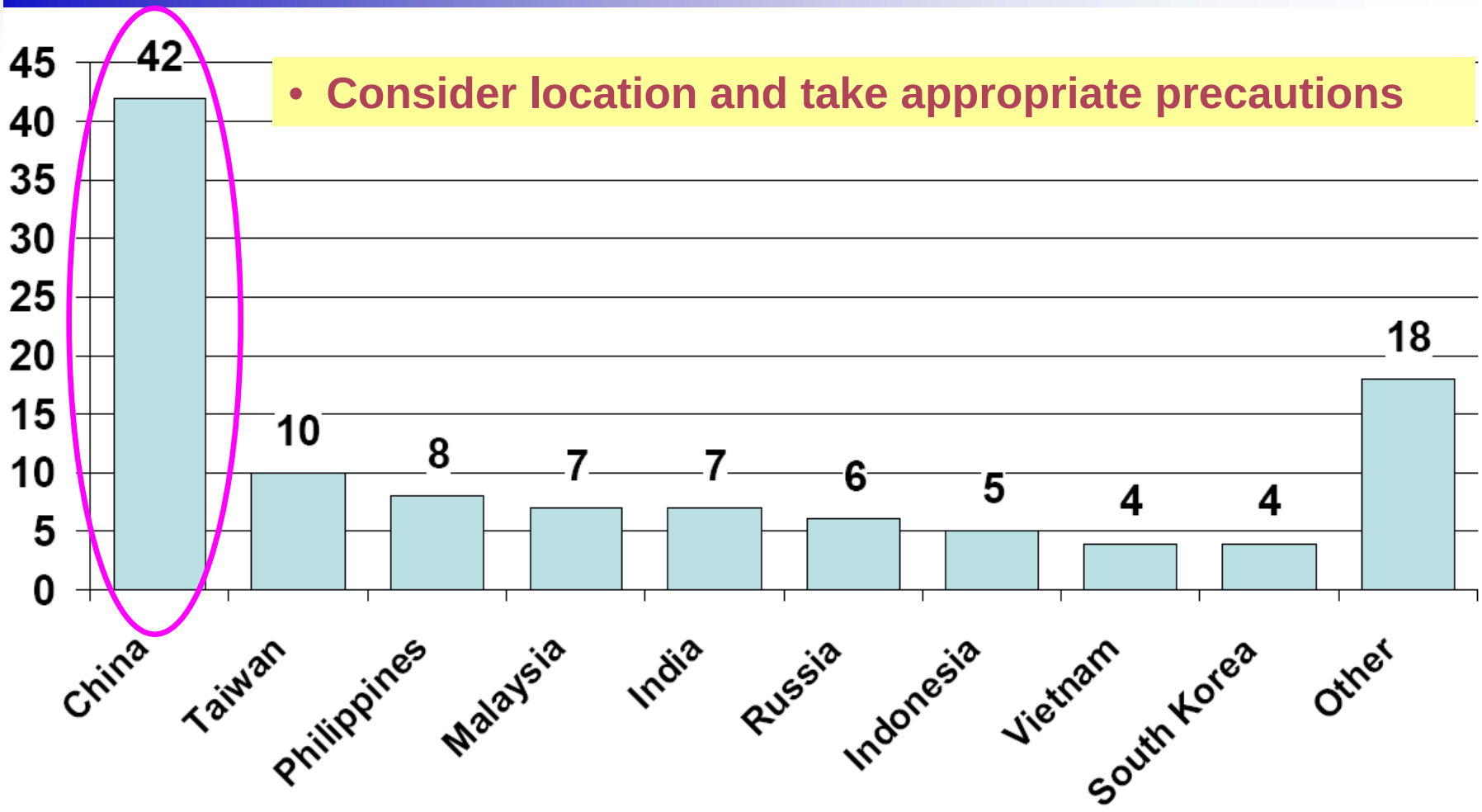
Supplier Selection Considerations

- **Establish preferred categories of suppliers**



Source: U.S. Department of Commerce Bureau of Industry and Security Office of Technology Evaluation Defense Industrial Base Assessment: Counterfeit Electronics, January 2010

Supplier Selection Considerations



- Consider location and take appropriate precautions

Suspected Sources of Counterfeit Electronics in 2008 by Country of Origin

Source: U.S. Department of Commerce Bureau of Industry and Security Office of Technology Evaluation Defense Industrial Base Assessment: Counterfeit Electronics, January 2010

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Supplier Selection Consideration

- Audit original equipment and component manufacturers (OEM/OCMs to ensure items they supply are made “in-house”
- Determine if suppliers have anti-counterfeiting measures and training in place
- Determine if suppliers have appropriate return policies
  - Inspection of returned items
  - Returning a greater quantity than purchased is prohibited

Procurement Document Requirements and Description Considerations

- Contractual requirements pertaining to disposal of rejected and surplus items
- Incorporate terms associated with provision of counterfeit or fraudulent items
- Clear communication of actions that will be taken if counterfeit or fraudulent items are provided
- Request certification
- Use escrow payments when appropriate

- Clear, detailed descriptions

Use Standard Contract Language addressing Counterfeit and Fraudulent Items

- **Delivery of Suspect/Counterfeit Items**
- Vendor is hereby notified that the delivery of suspect/counterfeit items is of special concern to (Buyer's Name). If any parts covered by this Order are described using a manufacturer part number or using a product description and/or specified using an industry standard, Seller shall be responsible to assure that the replacement parts supplied by Seller meet all requirements of the latest version of the applicable manufacturer data sheet, description, and/or industry standard. If the Seller is not the manufacturer of the goods, the Seller shall make all reasonable efforts to assure that the replacement parts supplied under this Order are made by the Original Equipment Manufacturer (OEM) and meet the applicable manufacturer data sheet or industry standard. Should Seller desire to supply a replacement part that may not meet the requirements of this paragraph, Seller shall notify Purchaser of any exceptions and receive Purchaser's written approval prior to shipment of the replacement parts to Purchaser. If suspect/counterfeit parts are furnished under this order or are found in any of the goods delivered hereunder, such items will be dispositioned by (Buyer's Name) and / or the Original Equipment Manufacturer, and may be returned to the vendor. The Vendor shall promptly replace such suspect/counterfeit parts with parts acceptable to (Buyer's Name) and the Vendor shall be liable for all costs, including but not limited to (Buyer's Name)'s internal and external costs, relating to the removal and replacement of said parts.

Bid Evaluation Considerations

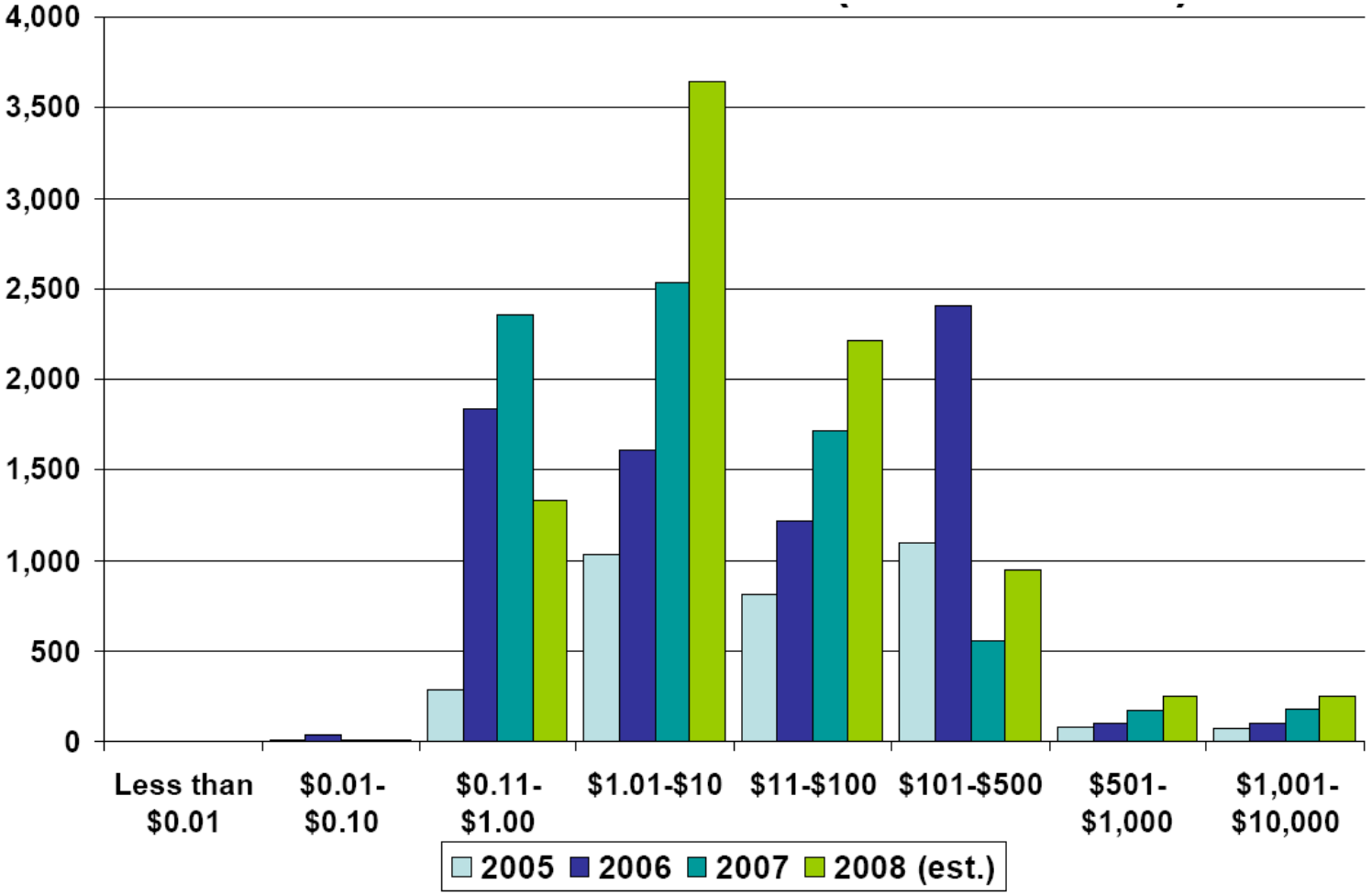
- Change policies that require selection of the lowest-cost bid
- Incorporate evaluation criteria that addresses:
  - Type of supplier (i.e. internet, broker, authorized distributor original manufacturer, etc.)
  - Level of experience with the supplier
  - Historical performance of the supplier

Identification of At-Risk Procurements

- Procurement involves
  - A non-authorized or internet-based supplier, distributor, broker
  - A new supplier
  - Expedited schedule
  - A supplier that does not take precautions against counterfeit and fraudulent items
  - A supplier located in a high-risk region
  - A supplier offering a significantly discounted price
  - A supplier that can't offer a traceable source, or refuses to provide/be accountable for certification

- Items are
  - High volume/low cost
  - In a known high-risk category
  - New items or equivalent items

Know the "$weet-$pots"



Resale Value of Counterfeited Items – Electronic Components

Source: U.S. Department of Commerce Bureau of Industry and Security Office of Technology Evaluation Defense Industrial Base Assessment: Counterfeit Electronics, January 2010

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Enhanced Inspection Considerations

- Perform enhanced testing and examination (including destructive) on “at-risk” procurements

- Request inspection and testing criteria from the original equipment component or equipment manufacturer (OCM/OEM)

- Use photographs of authentic items to aid authentication when performing receipt inspection
  - Verify manufacturer markings are correct
  - Verify other markings such as UL, FM, NEMA are correct

Enhanced Inspection

- Consult available industry data on known counterfeits when performing receipt inspection

- Be aware of manufacturing location
  - Beware of items marked with a country of origin that does not match where the item is manufactured

- For electronics, consider implementing guidance in:
  - SAE AS5553 (4/2009)
  - IDEA-STD-1010-A (10/2006)

Disposal of Rejected and Surplus Items

- Proper destruction and disposal of all unsalable items, surplus and scrap
  - Prevent dumpster diving
  - Curtail sale of surplus

Training

- Educate personnel on counterfeiting and fraud prevention and detection
  - Executive Management
  - Buyers
  - Inspectors
  - Maintenance and Craft
  - Suppliers
- Establish regularly scheduled refresher and update training sessions

Some Existing Sources of Incident Data

- Electronics
  - www.erai.com
- General
  - http://www.nema.org/gov/anti-counterfeiting/
  - http://www.ul.com/global/eng/pages/offerings/services/programs/anticounterfeitingoperations/
  - www.nuclearcounterfeit.com
- Government Contractors
  - www.gidep.org

EPRI does not endorse sources of information. Websites are included for information purposes only and list is not all inclusive

Response Plan Considerations

- Proceduralize the process for handling a counterfeit item

1. Quarantine the suspect CFSI(s)
2. Gather information about the items
3. Add incident to your corrective action program/system
   - Consider reporting to industry databases
4. Contact the OEM/OES
   - They stand the most to loose, should know of any other related incidents, will have Information about any ongoing investigations, and can refer you if they are not interested
5. Carefully decide if your supplier should be notified
   - Will you be tipping-off counterfeiters so the evidence can be hidden?
6. Carefully decide if and when suspect items should be returned
   - Gather information about the items and decide if it should be kept for “evidence”
7. Notify the NRC if:
   - Item was installed in safety-related equipment or is intended for safety-related use
8. Notify appropriate agency
   - As advised by manufacturer, Immigrations and Customs Enforcement, Federal Bureau of Investigation, etc.

Develop a tool to ensure pertinent information is collected

CFSI Incident Report

Incidents reported may not yet be confirmed cases of counterfeit, fraudulent, or substandard items (CFSI). Reporting suspect items is encouraged as a preventative measure. Additional notification will be provided for incidents confirmed to be false by the original equipment manufacturer

Issue Date: 09/01/09

Report Number:CFSI-01

Part 1: Item Information

ITEM TYPE (NOUN, ADJECTIVE, ADJECTIVE FORMAT): Optocoupler, phototransistor	ADDITIONAL DESCRIPTION:
CFSI ITEM SUPPLIER (PROVIDED CFSI) Unnamed internet electronics supplier	CFSI ITEM SUPPLIER (PROVIDED CFSI) PART/MODEL NO:
ORIGINAL EQUIPMENT MANUFACTURER (AUTHENTIC) Fairchild / QT Opto	OEM (AUTHENTIC) PART/MODEL NO. H24A1
ORIGINAL EQUIPMENT SUPPLIER (AUTHENTIC)	OES (AUTHENTIC) PART/MODEL NO.
ASSEMBLY LEVEL Part	DISCIPLINE Microelectronic/IC
LOT, BATCH, OR SERIAL NUMBER INFO (COUNTERFEIT):	DATE/DATE CODE (COUNTERFEIT):
WHEN IDENTIFIED During Receiving	PROMPTED DISCOVERY Suspect Packaging/Configuration
COMMENTS:	

Part 2: Reporting Information

IS CFSI SUPPLIER APPROVED DISTRIBUTOR/AGENT? ☐ Yes ☒ No

WAS CFSI SUPPLIER NOTIFIED? ☐ Yes ☒ No

The original equipment manufacturer or other reliable source (not the CFSI supplier themselves) should be contacted to determine if the supplier who provided the CFSI is an approved distributor/agent. If CFSI supplier is not an approved distributor/agent, it is recommended that they not be notified prior to contacting the OEM and reporting the incident to proper authorities. If possible, suspect items should not be returned.

WAS OEM NOTIFIED?: ☒ Yes ☐ No

OEM should always be notified first so they may determine status of the CFSI supplier, inform authorities conducting ongoing investigations and assist in confirming or refuting authenticity of the item(s)

WAS NRC NOTIFIED? ☐ Yes ☒ No

NRC should be notified if the CFSI was:
(1) Was purchased for use in a safety-related application and was identified as a CFSI before successful receipt (was not accepted into inventory)
(2) Was purchased for use in a safety-related or nonsafety related application and was identified as a CFSI after successful receipt (was accepted into inventory or was installed)

Page 1 of 3

CFSI Incident Report

art 3: Status

AS ITEM CONFIRMED TO BE A CFSI? ☒ Yes ☐ No ☐ Under Investigation

OMMENTS:
EM requested approved distributor be contacted. Approved distributor Digikey was very operative in helping confirm the devices received were not genuine items

art 4: Contact Information

RGANIZATION THAT IDENTIFIED CFSI: midyne Group	CONTACT NAME: Scott Borland
ACILITY: ew Market	PHONE NUMBER: 800.
RGANIZATION TYPES uclear Supplier	EMAIL:

art 5: Incident Description and Guidance

lease include photographs of the authentic and counterfeit items as well as any information that might be seful for others in determining if they are in possession of similar CFSIs

OMMENTS:

n August of 2009, a manufacturer that provides instruments to nuclear power plants questioned he authenticity of several Fairchild H24A1 phototransistor optocouplers during a routine spection. The optocouplers are used in timers that are supplied to several of its nuclear ustomers. No optocouplers were included in equipment provided to nuclear customers

pon further investigation, the OEM and an authorized distributor claim the optocouplers are not egitimate Fairchild parts. The optocouplers were procured from a company in the US.

he manufacturer who identified the parts did not alert the seller, but did notify the appropriate uthorities. Figure 5-1 below illustrates the differences in packaging and size that caused the anufacturer to verify authenticity of the parts. The smaller device is packaged incorrectly, and he date code indicates the suspect device was manufactured after the genuine H24A1 device was iscontinued by the OEM.

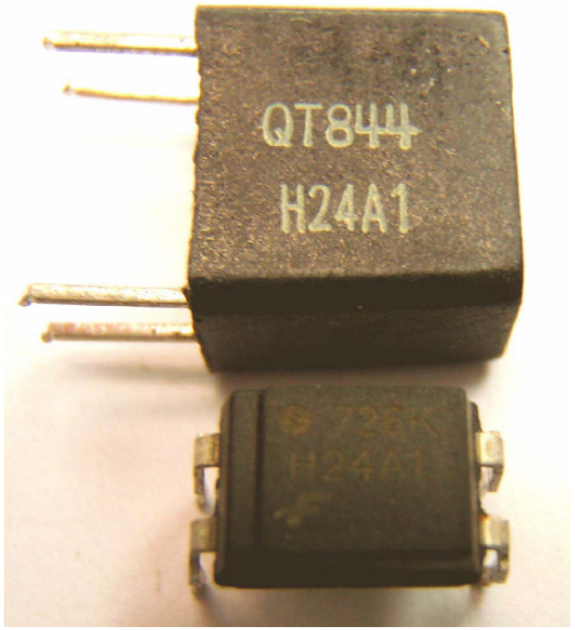
he Supplier was contacted by our purchasing department after the parts were confirmed as ounterfeit, as well as I notified the appropriate authorities. The supplier was not contacted during he investigation. Note that none of the parts were returned to the supplier.

HOTO OF AUTHENTIC ITEM	PHOTO OF CFSI See next page

Page 2 of 3

CFSI Incident Report

Authentic (top), Counterfeit (Bottom)



Page 3 of 3

Actions taken to Prevent Counterfeits

Figure VII-29: Internal Actions Taken to Prevent Infiltration of Counterfeits

Action	OCMs	Distributors	Circuit Board Assemblers	Prime/Sub Contractors	DOD
Performing screening and testing on inventory	27%	8%	41%	37%	21%
Training staff on the negative economic and safety impacts of counterfeit products	31%	65%	28%	36%	15%
No internal actions taken	35%	19%	34%	32%	72%
Revising procurement procedures to more carefully screen/audit/evaluate authorized returns from customers	35%	76%	25%	23%	11%
Revising company procedures for disposal of "seconds," defective parts, and production overruns	34%	44%	22%	17%	11%
Other	8%	12%	9%	17%	0%
Revising procurement procedures to reduce purchases from independent distributors and brokers	-	-	13%	4%	11%
Embedding new security measures in existing product lines	12%	4%	3%	2%	2%
Adding security markings to existing inventory	12%	0%	0%	2%	8%

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

Future Actions you can take to Mitigate Risk

- Use of “positive identification” techniques
  - Overt and covert
    - Radio Frequency ID
    - Holographs
    - Manufactured-in features

- Cause evaluation/investigation considerations
  - How far do we go to determine authenticity when a suspect item is found?
  - Forensic features and labs?

Future Actions to Mitigate Risk

- Effective collection and sharing of data on suspect items you find
- Contribute to industry databases


EPRI
ELECTRIC POWER
RESEARCH INSTITUTE
Questions?
Together...Shaping the Future of Electricity