Counterfeit Parts in Critical Infrastructure, Past, Present, and Future

Daniel Pasquale, Senior Systems Engineer

U.S. NRC Office of Investigations

Conducts investigations of allegations of wrongdoing
Maintains current awareness of inquiries and inspections by other NRC offices
Makes appropriate referrals to the Department of Justice
Liaise with other agencies and organizations to ensure the timely exchange of information of mutual interest


CFSI Past:

Notable counterfeit, fraudulent, suspect items (CFSI) events from the commercial nuclear industry

Pentas Controls (2010)
Vision Tech (2010)
MVP Micro Inc. (2010)
Laddish Valves (2007)
Square D Circuit Breakers (2007)
Hunt Valves (2006)
Crane Valves (1991)
Fasteners (1988)
Generic Communications (CFSI):

Recurring themes:

- Fraudulent test documents and certifications (substandard or improper materials, poor quality and/or workmanship)
- Misrepresenting refurbished equipment as original (new vs. used, vs. never used, vs. refurbished)
- Substitution of non-standard parts
- No clear traceability to the source


19 (agency) actions to assess and enhance CFSI processes!

- Tech staff committed to screen CFSI information into the NRC’s Operating Experience program and initiate a CFSI Technical Review Group (TRG) to assess, trend and process accordingly
- OI committed to promoting information sharing through interagency outreach efforts with appropriate Federal agencies
Post 9/11 Shift in Threat Resolution:

**Resources**

- **Pre-9/11**
  - Identification
  - Response
  - Elimination

- **Post-9/11**

CFSI Present:

IPR Center welcomes the Nuclear Regulatory Commission as its 21st partner agency (2012)

- Liaises with other law enforcement agencies to:
  - Ensure the timely exchange of information of mutual interest
  - Participate in PROACTIVE investigative efforts
  - Rapidly de-conflict information and evidence

CFSI Present:

**Reputable Organizations**

- Kobe Steel (2017)
- Creusot Forge (2015)
- KHNP (2012)

**Nefarious Organizations**

- Social activists
- Organized Crime (money laundering/human trafficking)
- Terrorist cells
- Cyber Supply Chain Risk
Cybersecurity Supply Chain Risk?

"...it is clear that an attack vector does exist from the supplier development environment." - EPRI 1026562, (2012)

"the supply chain represents a significant risk to industrial control systems (ICS)." - U.S. Industrial Control Systems Cybersecurity Annual Assessment Report

"Threats to the supply chain are constantly growing in sophistication, number, and diversity. Intentional threats include counterfeit products and malicious software." - NISTIR 7622, (2012)

"...the challenge to supply chain management in a cyber-contested environment is significant." - Defense Science Board (DSB) Task Force Report, (2013)

Emerging themes:

Favorable market conditions:
- obsolescence • Aging operating units
- advancing technology • Digital I&C
- global supply chain • 58 nuclear plants under construction worldwide
- diminishing suppliers (10 CFR 50, Appendix B) • More CGDs
- new norms • High in-service failures

Favorable criminal environment:
- lack of reporting
- little fear of prosecution
- low fines and sentences upon conviction
- unprecedented anonymity
- may involve alternate illicit activities

Favorable profit margins:
- high profit potential
- low capital and labor costs
- access to sub-suppliers
- easily distributed via the internet
- no research & development costs
- no advertising costs
- minimal legal expenses

Favorable market conditions:
- high profit potential
- low capital and labor costs
- access to sub-suppliers
- easily distributed via the internet
- no research & development costs
- no advertising costs
- minimal legal expenses

CFSI Future:

Critical Infrastructure Security and Resilience

"... advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure."
Specific NRC Responsibilities under PPD 21

“The NRC is to collaborate, to the extent possible, with DHS, DOJ, the Department of Energy, the Environmental Protection Agency, and other Federal departments and agencies, as appropriate, on strengthening critical infrastructure security and resilience.”

Benefits of Membership:
- Avoids duplicative efforts
  - do more with less
- Promotes CFSI information sharing and de-confliction
- Centralized reporting for non-Part 21 CFSI
  - supports +CGDs
- Assists in protecting IP Rights of key suppliers
- Significantly reduces supply chain risk
  - Supply chain visibility
- Expedites CFSI Alerts/Advisories
  - emerging trends
- Centralized reporting for non-Part 21 CFSI
- Supports +CGDs
- Assists in protecting IP Rights of key suppliers
- Harder for the dishonest to re-invent themselves

CFSI Future:
Operation Chain Reaction’s (OCR) Energy Infrastructure Initiative (EI)

Benefits of Membership:
- Significantly reduces supply chain risk
- Supply chain visibility
- Promotes CFSI information sharing and de-confliction
- Expedites CFSI Alerts/Advisories
- Contains the spill
- Accesses more Operating Experience (OpEx)
- Emerging trends
- Avoids duplicative efforts
- Do more with less
- Centralized reporting for non-Part 21 CFSI
- Supports +CGDs
- Assists in protecting IP Rights of key suppliers
- Harder for the dishonest to re-invent themselves

In Summary:

“...there is an identified and ongoing need for enhanced cooperation and education amongst all stakeholders and intermediaries to ensure that the fight against such criminality and its effects becomes more cohesive and well informed.”


In all aspects of IPR crime enforcement, there is an identified and ongoing need for enhanced cooperation and education amongst all stakeholders and intermediaries to ensure that the fight against such criminality and its effects becomes more cohesive and well informed.”

Key Takeaways

- OI supports the staff’s and law enforcement’s recommendations for a more PROACTIVE and COLLABORATIVE approach to CFSI
- EI Phase I - IPR Center 2012 (>5 yrs. of maturity)
- EI Phase II - Supplier participation 03/2018
- EI Phase III - The “data-net” (2019)