Counterfeits in GOV and Critical Infrastructure Supply Chain

National Intellectual Property Rights Coordination Center

Outline

- The Counterfeiting Problems
  - How CFSI became a concern 2007-2011
  - Gov Supply Chain Issues
- Birth of Operation Chain Reaction (OCR)
- Product Focus & Threats
- OCR Strategy
- Detection in Acquisition Process
- Collaboration
  - Current & OCR TF
  - Future Nuclear partner Collaboration
- How LE has responded to combat CFSI issues
  - Case examples

National Intellectual Property Rights Coordination Center

The Counterfeiting Problem

"…Robert P. Ernst, who heads research into counterfeit parts for the Naval Air Systems Command's Aging Aircraft Program…estimates that as many as **15% of all the spare and replacement microchips the Pentagon buys are counterfeit.** As a result, he says, 'we are having field failures regularly within our weapon systems-and in almost every weapon system.' He declines to provide details."

http://images.businessweek.com/ss/08/10/1002_counterfeit_narrated/index.htm

National Intellectual Property Rights Coordination Center

Gov Supply Chain Issues

- Aging technologies and systems
  - Obsolete sustainment parts
  - OEM doesn't manufacture part anymore
- Government Cost savings
  - Websites / brokers that offer parts (not vetted – acquisition training)
  - Companies compete for government contracts as the sub tier suppliers – not the Prime
- Operating/production costs
  - Too high to create new equipment at the speed technology advances
  - Most new projects take 10 yrs to develop / and test operationally
- DOD and USGOV working on methods for early detection processes to ID CFSI

National Intellectual Property Rights Coordination Center

Operation Chain Reaction

- FIRST - Operation Chain Reaction (OCR) targets counterfeit items entering the supply chain of the Department of Defense (DoD), other U.S. government agencies and critical infrastructure
- Sixteen (16) Federal Agencies participate in OCR

National Intellectual Property Rights Coordination Center

Operation Chain Reaction

- Task force partners - initiated numerous cases
  - Involving - Counterfeit (CF) brands - commercial, industrial, and military grade
  - Top commodities are semiconductors, networking equipment, and weapon sights
- From FY2014 to FY2017:
  - **Approximately $19 million (MSRP) seizures** - CF goods and proceeds
  - **33 arrests**
  - **47 indictments**
  - **34 convictions**

National Intellectual Property Rights Coordination Center

Product Focus – Integrated Circuit

Integrated circuit (aka IC, semiconductor, microcircuit, microchip, silicon chip, or chip) is a **miniaturized electronic circuit that has been manufactured in the surface of a thin substrate of semiconductor material.**

EASY to counterfeit

7

National Intellectual Property Rights Coordination Center

CFSI - Where Integrated Circuits End Up

1. IC applications -

- Consumer electronics
- Automotive
- Medical
- Aircraft
- Spacecraft
- Military
- SCADA – (ex) Nuclear Plants

2. Counterfeit ICs can result in -

- Product malfunction or product failure, loss of property
- Serious bodily injury, including electrical shock, electrocution, and/or death
- Cyber Threat concern

Everything that has an on and off switch……has an IC in it.

8

USA – largest exporter of e-waste

China – largest importer of e-waste and largest exporter of counterfeit electronics

9

National Intellectual Property Rights Coordination Center

OCR Special Project

234 Chinese/Hong Kong companies involved in counterfeit integrated circuit trafficking

462 U.S. importers from identified CN/HK companies

- 70 open investigations identified (ITAR, improper license, CPI groups)

171 DoD prime contractors identified domestically

10

National Intellectual Property Rights Coordination Center

OCR Strategy

The Benefits of Collaboration

1. **Pursue Criminal Investigations**
   - **Develop referral packages (leads and conduct requested trade data analysis)**
     - Analyze seizure and import patterns from CBP trade data
   - **Deconflict leads with our partners**
     - Coordinate with **manufacturers** to verify authenticity
2. **Raise Quality Assurance**
   - **Demonstrate National Security implications of current methodology of procuring microelectronics within DoD and USGOV**
     - Coordinate with USGOV leadership
     - **Prevent them entering the supply chain**

11

National Intellectual Property Rights Coordination Center

Detecting Possible Fraud in the Acquisition Process

Examples:

- Counterfeit parts
- Product Substitution
- Cost Mischarging
- Progress payment fraud

Fraud Indicators:

- Serial numbers missing
- Inspection reports that appear altered by whiteouts
- Requests for payment that are inconsistent with earlier cost history
- History of frequent invoice/voucher errors, poor documentation, & claiming unallowable costs
- Little or no physical progress on the contract even though significant costs have been billed

National Intellectual Property Rights Coordination Center

Process for Information Sharing of CFSI

- Nuclear Plant identifies a part that is counterfeit, fraudulent, and/or suspect item (CFSI)
- Plant sends part and company information to IPR Center OCR Program Manager
  - OperationChainReaction@ice.dhs.gov
- OCR team conducts research to identify preliminary information on the company
- OCR team deconflicts with task force partners and potentially disseminates information as an investigative lead
- OCR team may also share information back with industry

13

National Intellectual Property Rights Coordination Center

- **September 2016** – Michael Westcott, owner of Lightning Technology Inc., convicted of manufacturing and selling $4 million in counterfeit Cisco transceivers from 2006 to 2015
- Cisco transceivers, including several of the long range models counterfeited by Lightning, are used by the **U.S. Navy** in critical communication systems in **nuclear submarines, aircraft carriers, ship self-defense systems,** and **ballistic missile defense systems**
- **November 2017** – Westcott sentenced to 37 months in prison and agreed to pay $325,000 in damages to Cisco

14

National Intellectual Property Rights Coordination Center

- **March-April 2016** – Jiang Guanghou YAN, owner of *HK Potential*, and two other Chinese nationals were convicted of **conspiracy to traffic in counterfeit goods**
- The counterfeit ICs were knowingly sold to individuals purporting to be U.S. Navy contractors to be used in **nuclear submarines**
- **July-December 2016** – All 3 defendants were sentenced to between 12 to 15 months imprisonment

15

National Intellectual Property Rights Coordination Center

Chatsworth Rubber and Gasket Case

- Product Substitution
- The owner of a business supplied substandard O-Rings to NASA that were used on various aircraft
- Individual was sentenced to 30 months in prison, 3 years of supervised release and restitution of $216,848

National Intellectual Property Rights Coordination Center

Resiliency Strategy

- Infrastructure resilience, as defined by the U.S. Department of Homeland Security in 2010 is "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event."
- Infrastructure resilience effectiveness leads to
  - Ability to reduce the magnitude and/or duration of disruptive events by:
    - **Anticipate** - Communicating to leadership the support the plants need for sustainment
    - **Adapt** - Avoiding counterfeits entering the supply chain
    - **Recover** - Avoiding operational costs of counterfeit parts upon inspection (aging systems)
    - **Recover** - Avoiding regulation costs of parts found after installation

17

National Intellectual Property Rights Coordination Center

William G. Ross
HSI Deputy Director
National IPR Center
William.G.Ross@ice.dhs.gov

18