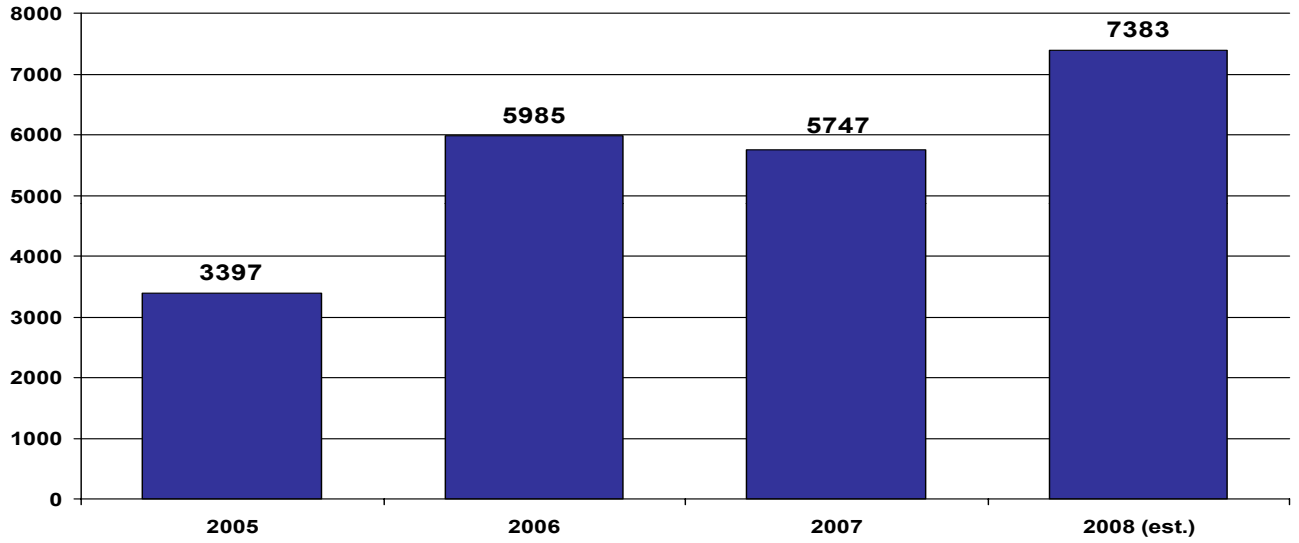
REVISITING COUNTERFEIT, FRAUDULENT, SUSPECT ITEMS (CFSI) - AN NRC AGENCY WIDE ASSESSMENT- JUNE 30, 2011

DAN PASQUALE, NRO/DCIP/CQVB

(301) 415-2498

Daniel.Pasquale@nrc.gov

Total Counterfeit Incidents:
OCMs, Distributors, Board Assemblers 2005 - 2008



NOTE: ***For NRC regulated activities, there have been no recent reports of CFSI being installed in safety related applications.***

CURRENT FACTORS

1. Material shortages
   a. obsolescence
   b. new orders (multiple and simultaneous)
2. Diminishing Appendix B suppliers
   a. reliance on Commercial Grade Dedication
   b. increased use of unauthorized distributors
3. Spike in CFSI incidents
   a. recent “near-misses” in commercial nuclear plants
   b. counterfeit electronics in the U.S. Department of Defense
   c. 2010 Joint Strategic Plan on Intellectual Property Enforcement
4. The advent of cyber security
   a. Critical Digital Assets (firmware/software)
5. Global supply chain
   a. disengaged suppliers
   b. focused factories & lean manufacturing
6. Advancing technology
   a. analog – digital transition
   b. innovations in micro-circuitry
   c. proficiency in counterfeiting techniques

OFFICE OF THE INSPECTOR GENERAL (OIG)
U.S. Nuclear Regulatory Commission
Audit of NRC's Vendor Inspection Program
OIG-10-A-20 September 28, 2010

OIG recommends that the Executive Director for Operations:

10. Develop and implement a formal <u>agency-wide</u> strategy and plan in order to monitor and evaluate CFSI.

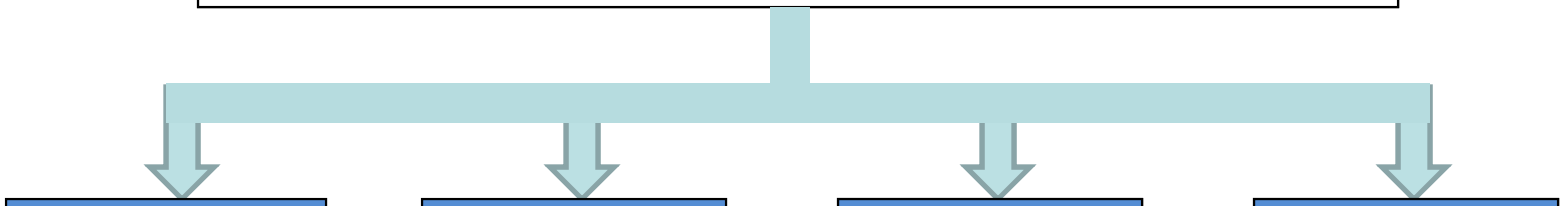
>>> SECY Paper completed by OCT. 24, 2011 <<<

DEVELOPMENT OF AN AGENCYWIDE CFSI RESPONSE STRATEGY

CFSI TASK LEAD:
Dan Pasquale
(301) 415-2498

MISSION STATEMENT

"To coordinate the diverse staff resources within the agency to improve the agency's abilities to respond to challenges associated with counterfeit, fraudulent, and suspect items. This effort shall include agency-wide assessments of the following key areas: 1.) supply chain oversight, 2.) communications (both internal and external), 3.) Agency response protocols, and 4.) Cyber security supply chain oversight "



WORKING GROUP ON SUPPLY CHAIN OVERSIGHT	WORKING GROUP ON CFSI COMMUNICATIONS	WORKING GROUP ON CFSI RESPONSE PROTOCOLS	WORKING GROUP ON CYBER SECURITY SUPPLY CHAIN OVERSIGHT
WG Leader: ***Eugene Huang*** *Includes conventional supply chain processes*	*WG Leader:* ***Garrett Newman*** *Includes how CFSI information should be shared*	*WG Leader:* ***Doug Bollock*** *Includes how the various organizations need to interact*	*WG Leader:* ***Jeff Jacobson*** *(Stacy Smith)* *Relationships between security & sabotage including cybersecurity*

PROGRAM DEVELOPMENT STEPS (to date):

Each of the working groups evaluated:

- Regulatory Requirements
- Existing Guidance
- Industry Practices
- Best practices from other industries

Gaps were compiled and assessed for significance

Potential recommendations were developed

CATEGORIES of ASSESSMENT RESULTS

I. Methods being employed in the nuclear industry to **detect** Counterfeit, Fraudulent, and Suspect items (CFSI), including detection at the sub-vendor level and during commercial grade dedication activities

II. Reporting requirements/practices/thresholds for CFSI, including how CFSI information is shared internal/external to the nuclear industry and reported to the NRC (including all NRC regulated activities)

III. Response protocols once CFSI is detected/reported, including at licensees, suppliers, and within the NRC (including legal/judicial actions)

IV. Regulatory Guide 5.71 expectations regarding quality controls imposed on suppliers of **critical digital assets**, including controls for testing, design, manufacture, storage, purchasing of components, etc.

IMPLEMENTATION CONSIDERATIONS

1. No Action
2. Rely on Industry Actions and Initiatives
3. Enhance NRC Business Practices
    - New/revised internal NRC policies, practices, procedures
    - NRC coordination with Federal agencies and international governments
4. NRC Regulatory Activities
    - Regulatory guidance and communications
    - Inspections, audits and licensing reviews
    - New/revised regulations
    - Legislation recommendations

SUPPLY CHAIN

- Guidance for authentication and testing of CFSI components
- Guidance regarding fraudulent documentation
- Contractual requirements for suppliers regarding CFSI
- Guidance for non-reactors regarding CFSI

COMMUNICATION

- Existing reporting requirements have high thresholds and are event-driven
- Existing Part 21 and Appendix B language does not explicitly address CFSI
- Sharing of CFSI information
- NRC Communications Processes

RESPONSE PROTOCOL

- Guidance to address identified CFSI when NRC becomes aware
- Quarantine requirements for CFSI material
- NRC guidance for CFSI inspections
- NRC jurisdiction for foreign suppliers

CYBER SECURITY SUPPLY CHAIN

- Guidance for implementation of supplier controls (Regulatory Guide 5.71)
- NRC inspection authority for non-safety related critical digital assets (Regulatory Guide 5.71)
- NRC inspection guidance on cyber security controls passed down by licensees (Regulatory Guide 5.71)
- ,Guidance for QA treatment of critical digital assets (Regulatory Guide 5.71)

Questions

- Dan Pasquale, NRO/DCIP/CQVB

  (301) 415-2498

  Daniel.Pasquale@nrc.gov

- Richard Rasmussen, NRO/DCIP/CQVB

  (301) 415-1340

  Richard.Rasmussen@nrc.gov