



**COUNTERFEIT,
FRAUDULENT,
SUSPECT ITEMS (CFSI)**

- Post SECY-11-0154 -

February 16, 2012

Public Meeting

Daniel Pasquale

Sr. Operations Engineer
Quality and Vendor Branch
Office of New Reactors

Daniel.Pasquale@nrc.gov



POLICY ISSUE
(INFORMATION)

ML112200150

October 28, 2011

SECY-11-0154

FOR: The Commissioners

FROM: R. W. Borchardt
Executive Director for Operations

SUBJECT: AN AGENCYWIDE APPROACH TO COUNTERFEIT, FRAUDULENT,
AND SUSPECT ITEMS

PURPOSE:

This paper informs the Commission of the staff's plans to identify and implement proactive strategies to detect and prevent the intrusion of counterfeit, fraudulent, and suspect items (CFSI) into equipment, components, systems, and structures regulated by the U.S. Nuclear Regulatory Commission (NRC).

SUMMARY:

This paper provides the Commission with the staff's agencywide strategy and plan to monitor and evaluate CFSI potentially impacting NRC-regulated activities. The paper also documents the staff's assessment of the current regulations, guidance, and licensee procurement processes associated with preventing the intrusion of CFSI into NRC regulated activities.

The staff assembled an internal task force comprised of representatives from the various offices potentially affected by the CFSI issue. As part of this effort four working groups were formed to assess activities and potential vulnerabilities in its specific area including reviewing best practices from several external sources, from the commercial nuclear industry, other heavy industry business sectors, and Federal agencies and law enforcement organizations. The staff also interacted with representatives from the Nuclear Procurement Issues Committee (NUPIC) and the Electric Power Research Institute (EPRI) in developing this paper.



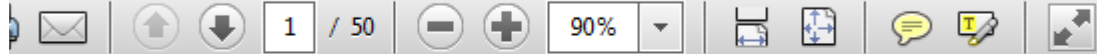
The Commissioners

- 2 -

The staff's assessment focused on the major elements of the commercial nuclear procurement process, including current NRC regulations and guidance, current licensee procedures, and supplier practices, inter-organizational communication, and NRC internal activities. The assessment also evaluated the status of cyber security as it relates to supply chain oversight of critical digital assets (CDAs).

Collectively, the working groups identified 24 issues where additional attention could potentially provide for a more robust CFSI program. The agency presented these issues to stakeholders via a Category 3 public meeting to solicit additional insights into the extent of the issues and solicit ideas on how to respond to the issues. The meeting was attended by the stakeholders and the members of the NRC working groups. The comments from the public meeting were considered by the working groups and factored into the final recommendations presented in the paper. As a result, 19 planned actions were identified to address the 24 issues. These actions were categorized into the following five categories: (1) industry process enhancement and best practices, (2) regulatory guidance, (3) communication, (4) training, and (5) industry oversight for detecting and preventing CFSI.





Staff Review of Counterfeit, Fraudulent, and Suspect Items (CFSI)

**Daniel Pasquale
Douglas Bollock
Garrett Newman
Eugene Huang
Jeffrey Jacobson
Stacy Smith
NRO/DCIP/CQVB**

Office of New Reactors
CFSI Working Groups—
Supply Chain Oversight, Response Protocols, Communication, Cyber Security Supply Chain
Oversight
November 18, 2011

ML112130293

PLANNED ACTIONS



1	<i>Conduct periodic public meetings</i>		NRC/Industry
2	<i>Issue Generic Communication: Potential CFSI training</i>		NRC/Industry
3	<i>Issue Generic Communication: Proactive Strategies</i>		NRC/Industry
4	<i>Revise 10CFR21 to include evaluation for potential reporting of CONFIRMED CFSI.</i>	2013	NRC
5	<i>Issue Generic Communications for specific instances or trends Industry/Gov/Int'l input</i>	<i>As Needed</i>	NRC/Industry
6	<i>Add CFSI to NRC Allegations Training</i>	2013	NRC
7	<i>Expand NRC OpE/ConE program for CFSI</i>	2013	NRC
8	<i>Evaluate the need for a pilot program to inspect licensee procurement/Part 21 programs.</i>	2013	NRC
9	<i>Evaluate the need for additional CFSI guidance in NRC inspection procedures</i>	2013	NRC
10	<i>Develop CFSI training for NRC inspectors</i>	2013	NRC

PLANNED ACTIONS



11	<i>New Inspection Procedure for suppliers of safety related CDAs</i>	2013	CYBER
12	<i>Evaluate the need for additional controls for non-safety related CDAs - pending program implementation & NRC governance.</i>	2013	CYBER
13	<i>Licensee inspection and NRC oversight of 73.54 suppliers</i>	2013	CYBER
14	<i>Evaluate the results of licensee inspection and NRC oversight of the 73.54 suppliers and expand the sample population as needed</i>	2013	CYBER
15	<i>Promote information sharing and outreach efforts with U.S. Government agencies & International regulators</i>	2013	NRC
16	<i>Continue developing NSIR's Temporary Instruction to inspect licensee's implementation of 73.54</i>	2013	CYBER
17	<i>Evaluate the need to expand the CFSI program to the FSME /medical community</i>	2013	NRC
18	<i>Evaluate the need to expand the CFSI program to the NMSS community</i>	2013	NRC
19	<i>Perform and agency-wide CFSI program effectiveness review</i>	2014	NRC

CFSI SECY Recap

The 19 Planned Actions



Expected Outcome: (Feb. 16, 2012)	Develop and convey to stakeholders the NRC's expectations for completing the 19 Planned Actions.
Content:	<ol style="list-style-type: none"> 1. Strategy for conducting & holding public meetings 2. Issue Generic Communication: Proactive Strategies 3. Issue INFORMATION NOTICE: CFSI Training
Facilitator:	NRC
Deliverables:	<ol style="list-style-type: none"> 1. Establish cooperative working groups and POCs for key topics 2. Identify specific deliverables for next meeting
Due dates:	Next public meeting (approximately 6 weeks)
Topics for further discussions:	<ol style="list-style-type: none"> 1. Sharing CFSI Information 2. Reporting CFSI (10CFR2, Allegations Process, FBI) 3. The role of the supply chain in Cyber Security Plans

1. CONDUCT PERIODIC PUBLIC MEETINGS



a)	<i>Develop a method for sharing CFSI Information, including issues identified during receipt inspection and during commercial grade dedication</i>	How	Who
b)	<i>Develop an industry accepted practice for using the corrective action program and nonconformance programs for entering CFSI related to safety related components</i>	How	Who
c)	<i>Develop an industry accepted practice for using the corrective action program to enter non-safety related CFSI into the corrective action program</i>	How	Who
d)	<i>Develop industry accepted procurement practices that align with ASME NQA-1 CFSI initiatives</i>	How	Who
e)	<i>Establish an industry CFSI database (INPO and EPRI databases in development)</i>	How	Who

Topics for Future CFSI Public Meetings



Expected Outcome:	Develop a schedule of future CFSI public meetings to address areas requiring additional discussion
Content:	Assign a POC and needed content as additional issues are identified.
Facilitator:	NRC via the public meeting process
Deliverables:	Establish a list of proposed topics with corresponding POCs, content and proposed deliverables & due dates
Due dates:	Next public meeting (approximately 6 weeks)
Topics for further discussions:	As needed

2. ISSUE GENERIC COMMUNICATION for CFSI TRAINING



a)	<i>Communicate with the industry about potential CFSI training or applicable information sources.</i>	Initial	NRC/Industry
----	---	---------	--------------

Potential CFSI Training & Knowledge Sources



Expected Outcome:	INFORMATION NOTICE documenting known sources of available CFSI education and skill training relevant to the commercial nuclear industry.
Presently identified training areas (including non-nuclear)	<ul style="list-style-type: none"> • Industry Overview of CFSI (EPRI) • Using the Allegations Process (NRC) • Addressing CFSI in DOE facilities (DOE) • IAEA Training (International) • Counterfeit Electronics (CALCE, NASA) • Federal Law Enforcement Training (FLETC) •etc
Ownership:	NRC/Industry
Deliverables:	Title of the course along with a brief description and accurate contact information of the instructor/organization.
Due dates:	Next public meeting (approximately 6 weeks)
Additional knowledge sources needed	Suggest areas for additional training

3. ISSUE GENERIC COMMUNICATION PROACTIVE STRATEGIES



a)	<i>Provide industry best practices for quarantining CFSI items and removing them from the supply chain without returning them to the supplier</i>	How	NRC & Industry
b)	<i>Provide industry best practices for identifying and informing the industry of CFSI trends</i>	How	NRC & Industry
c)	<i>Provide industry best practices for enhanced commercial-grade dedication, and receipt inspection practices</i>	How	NRC & Industry
d)	<i>Provide industry best practices for product authentication to provide additional assurance in preventing CFSI</i>	How	NRC & Industry
e)	<i>Provide industry best practices for using batch sampling with authentication testing</i>	How	NRC & Industry
f)	<i>Provide industry best practices for the use of standardized anti-CFSI language in procurement documents</i>	How	NRC & Industry

Content for the Generic Communication of Proactive Strategies



Expected Outcome:	To capture industry's strategy for implementing the proactive process elements identified in the SECY (and supporting Working Group's report)
Content:	Identify proactive strategies that will be incorporated and those requiring additional discussion
Ownership:	Industry/NRC
Deliverables:	Proposal of industry's strategy for implementation
Due dates:	Next public meeting (approximately 6 weeks)
Topics for further discussions:	<ol style="list-style-type: none"> 1. Sharing CFSI information 2. Disposal of CFSI