PUBLIC SUBMISSION

As of: October 30, 2014
Received: October 29, 2014
Status: Pending_Post
Tracking No. 1jy-8f75-d6dc
Comments Due: November 03, 2014
Submission Type: Web

Docket: NRC-2014-0212
Oversight of Counterfeit, Fraudulent, and Suspect Items in The Nuclear Industry

Comment On: NRC-2014-0212-0001
Oversight of Counterfeit, Fraudulent, and Suspect Items in the Nuclear Industry; Draft Regulatory Issue Summary

Document: NRC-2014-0212-DRAFT-0007
Comment on FR Doc # 2014-23509

6

10/2/2014
79FR 59521

Submitter Information

Name: Roger Johnston
Address:
5 Navajo Court
Oswego, IL, 60543
Email: rbsekurity@gmail.com

General Comment

The summary on page 3 of the attributes of a positive security culture is good, but I would add: (1) engaging in imaginative and proactive analysis of problems and CFSI threats and vulnerabilities, (2) rewarding innovative and proactive efforts to improve safety and the identification of CFSI, and (3) providing and promoting anonymous tip and whistle blower reporting mechanisms,

Quality control/assurance is emphasized throughout the document as the way to tackle CFSI, but this hasn't worked well in other industries in the past and it won't work well in the nuclear arena. Detecting CFSI should be a separate program with independent people who are more proactive and less passive to the problem than QC/QA/Procurement people, and who conduct proactive threat and vulnerability analyses, or coordinate with others who do this. (They would also have fewer conflicts of interest because the discovery of CFSI is usually taken to be a failure of the QC/QA/Procurement departments.) Also, formalistic, objective evidence of the failure of a product to perform to spec--which this document emphasizes--is a poor way to head off problems with CFSI (or with deliberate sabotage of hardware or software, for that matter).

The idea on page 7 that departure from a technical requirement is the best or only way to detect CFSI is incorrect. CFSI products can fail in ways never foreseen in formal technical requirements and procurement documents. It is simply not possible to specify all the things that could go wrong with a given non-trivial product, or all the ways a fake product could be configured by a malicious adversary to fail.

SUNSI Review Complete
Template = ADM-013

E-RIDS = ADM-03
Add = T. Mensah (tmm)
J. Gaslevic (JCG2)

Also on page 7, the situation seems to be that if I didn't know something was CFSI, I'm off the hook. This would seem to be a strong incentive for see-no-evil, hear-no-evil, speak-no-evil. The encouragement on page 7 to voluntarily report CFSI issues thus seems a little naive. This is one way an anonymous tip line could help.

There seems to be little emphasis on doing effective threat and vulnerability on CFSI issues. It is also disappointing that there seems to be little emphasis on hands-on training for detecting CFSI, and for learning how to exploit anti-counterfeiting tags, track & trace, serialization, and random virtual numeric tokens.

A minor point, but what is the difference on page 2, 2nd line between "enforcement" and "enforcement action"? Does this imply "enforcement" involves no action?