# POLICY ISSUE
(INFORMATION)

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.

CONTACT: Daniel J. Pasquale, NRO/DCIP
301-415-2498

The staff's assessment focused on the major elements of the commercial nuclear procurement process, including current NRC regulations and guidance, current licensee procedures, supplier and subtier 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 to 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 this paper. As a result, 19 planned actions were identified to address the 24 issues. These planned actions were categorized into the following five categories: (1) industry process enhancements and best practices, (2) regulatory guidance, (3) communication, (4) training, and (5) industry oversight for detecting and preventing CFSI.

BACKGROUND:

The integrity of the supply chain is a fundamental element of an effective quality assurance program for NRC licensee facilities and the suppliers of basic components to these facilities. For example, six of the 18 criteria presented in Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities," are directly related to assuring that adequate procurement controls at these facilities have been appropriately established and effectively implemented. Although Appendix B to 10 CFR Part 50 applies to reactor facilities, some non-reactor facilities and some materials users have complimentary or comparable quality standards.

During the late 1980s and early 1990s, the NRC and the commercial nuclear power industry performed a major reassessment of the supply chain in response to numerous attempts to introduce counterfeit or fraudulent materials and components into NRC-licensed facilities. NRC personnel assisted investigators and law enforcement officials in investigations to identify and prosecute the sources of these materials.

The NRC issued generic communications to inform licensees and suppliers about threats, methods to identify the CFSI, and steps to mitigate risk to the nuclear supply chain. These guidance documents have remained effective for more than two decades, with little to no significant counterfeit activity evidenced in the commercial nuclear industry since their inception.

However, other industries have seen an increase in CFSI activity in recent years. In 2010, the U.S. Department of Commerce (DOC) published the results of a study of the electronics supply chain supporting the U.S. Department of Defense (DOD). The results of the study indicated that the electronics industry may be experiencing a far greater challenge today than the nuclear industry experienced in the 1990s. The report was based on an extensive survey of original equipment manufacturers, original component manufacturers, electronics distributers, brokers, and suppliers to DOD. The survey asked more than 80 procurement and quality-related questions for the purpose of assessing the depth and breadth that counterfeiting has permeated DOD's electronic supply chain. The survey showed the significant trend of a 120 percent rise in

electronic counterfeiting since 2005. Similar trends have been noted in other heavily industrialized business sectors, including the petroleum, automotive, transportation, and commercial airline industries, as evidenced by the numerous publications being issued from industry trade groups representing the interests of these industries.

Current Factors Influencing the Introduction of CFSI

Historically, obsolete parts have created opportunity for a potential for CFSI. The buyers of rare or hard-to-find items have been known to pay large sums of money or assume unconventional levels of risk to prevent a process disruption at a plant or of a critical mission. The DOC study shifted that paradigm by reporting that obsolescence was a factor in less than half of the reported counterfeit instances. The majority of recently documented cases were related to new items, commonly referred to as "in-process" items. Additionally, counterfeiters have significantly upgraded their capabilities and skills to manufacture CFSI that are increasingly more difficult to detect.

A concern that factored into the NRC's decision to evaluate the extent of CFSI was the industry's transition from analog to digital instrumentation and controls technology. Along with the shift to more advanced technologies come the risks and vulnerabilities other industrialized business sectors are experiencing.

Based on interactions with NUPIC and EPRI, the staff determined that the following factors were key contributors to the current rise in counterfeit electronic activity:

- part standardization, making a product's design vulnerable
- long, complex supply chains and a shift to a more globalized supplier base
- the advent of the Internet and increased use of alternate sourcing techniques
- internal quality assurance programs not focused on CFSI
- a sense of complacency based on the belief that someone else along the supply chain had been checking for CFSI
- use of commercially manufactured parts or components in applications requiring high degrees of quality assurance

Office of the Inspector General (OIG) Audit OIG-10-A-20

The NRC's OIG performed an audit of the agency's Vendor Inspection Program. OIG's audit report (OIG-10-A-20, "Audit of NRC's Vendor Inspection Program," dated September 28, 2010) included the recommendation (Recommendation 10) that the Executive Director for Operations develop and implement a formal agencywide strategy and plan to monitor and evaluate CFSI (Agencywide Documents Access and Management System (ADAMS) Accession Number ML102710583).

The OIG audit assessed the current agency policies and procedures for ensuring that the commercial use of nuclear power is adequately protected against another resurgence of CFSI.

OIG determined that the NRC's overall approach to CFSI is primarily reactive and that the agency could strengthen its approach by implementing more proactive elements to augment its existing processes. The report also acknowledged that both the Federal Government and the private sector have begun to recognize the increasing trends of CFSI in nuclear and other industries and, to this end, have highlighted shortcomings in the agencies' current processes. OIG concluded that "a lack of a formal strategy hampers NRC's ability to identify resource needs and allocations to address CFSI and impairs agency knowledge management efforts to address it."

DISCUSSION:

In response to OIG's recommendation, the staff committed to develop and implement a formal agencywide strategy and plan to monitor and evaluate CFSI. An internal task force was created, that consisted of representatives from the various offices potentially affected by the CFSI issue, and guided by a CFSI Steering Committee made up of senior management personnel from the Office of New Reactors (NRO), the Office of Nuclear Reactor Regulation (NRR), the Office of Nuclear Material Safety and Safeguards (NMSS), the Office of Nuclear Security and Incident Response (NSIR), the Office of Federal and State Materials and Environmental Management Programs (FSME), the Office of Investigations (OI), the Office of Enforcement (OE), and the Office of the General Counsel (OGC). NRO served as the lead office for this task force.

The Steering Committee approved a charter and, based on that charter, created four working groups:

- supply chain oversight
- communication
- response protocols
- cyber security supply chain oversight

Each working group is led by a representative from NRO's Quality and Vendor Branch and supported by representatives from those NRC offices directly affected by the activities addressed by each working group. A CFSI knowledge management community of practice web site was created to be the central communication tool for storing and sharing the CFSI support information among the participants. A survey was used to obtain each representative's perspective on CFSI. The survey provided an agencywide view of the governing regulatory basis, specific information sources, communication needs, reporting requirements, and potential impacts from intrusion of CFSI into each of the regulated activities.

Each of the working groups assessed activities and potential vulnerabilities in its specific areas using the following process:

(1) Identify current regulatory practices and guidance.

(2) Gather and assess information relating to current counterfeiting activity, security risks and events, and current practices in both regulated and non-NRC-regulated activities.

(3) Evaluate the differences and potential vulnerabilities between items (1) and (2) above.

(4) Provide planned actions to address any identified differences or potential vulnerabilities as a result of the above evaluation.

Working group evaluations included reviewing best practices from several external sources, including (1) the commercial nuclear industry, (2) other heavy industry business sectors, and (3) Federal agencies and law enforcement organizations. The insights from these evaluations helped to identify potential issues and frame the scope of actions that would be appropriate for the NRC and the nuclear industry to address and resolve.

The agency presented the 24 issues identified by the working groups to stakeholders in a Category 3 public meeting to solicit additional insights into the extent of the issues and to 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 agencywide strategy and plan presented in this paper.

WORKING GROUP SUMMARY:

The following is a summary of the four individual working groups' activities:

(1) Working Group on Supply Chain Oversight

This working group focused on regulations, guidance, and industry practices related to keeping CFSI out of the nuclear supply chains of NRC-regulated activities. The working group focused on methods being employed in the nuclear industry to detect CFSI, including detection at the subvendor level and during commercial-grade dedication activities. The group also discussed the anticounterfeiting techniques that have been proven to be effective in detecting and preventing CFSI intrusion into the supply chains. The groups discussed the contribution that appropriate testing would have in detecting a fraudulently identified product and for ensuring that the item would perform its intended safety function. Additional discussions focused on the inspection of documentation during the procurement process and weaknesses in the commercial-grade dedication process that could create opportunities to introduce CFSI into the nuclear supply chain.

(2) Working Group on Communication

This working group focused on regulations, guidance, and industry practices related to communicating about CFSI. The working group discussed methods being employed in the nuclear industry and related industries to communicate about CFSI internally and externally. Topic discussion included the NRC internal operating and construction experience programs, use of the international operating experience database, EPRI's and the Institute of Nuclear Power Operation's development of a CFSI database for industry, and external Federal agency communication tools and guidance such as the Government-Industry Data Exchange Program.

(3) Working Group on Response Protocols

This working group focused on regulations, guidance, and industry practices for assessing NRC actions that could or should be taken following notification of a CFSI incident related to an NRC-regulated activity. Topic discussions included the sequence of actions that are necessary to effectively engage the full capabilities afforded the agency in investigating, communicating, and prosecuting CFSI at NRC-regulated activities. Other topics included the external Federal agencies and local authorities that would need to be engaged, internal organizations that would serve as points of contact for the various response activities, and jurisdictional limitations when foreign suppliers are used and what the response protocols should be in those instances.

(4) Working Group on Cyber Security Supply Chain Oversight

This working group focused on regulations, guidance, and industry practices for supplier oversight of cyber security-related items or components. The working group discussed the roles of the various offices related to cyber security. Specifically, NSIR oversees cyber security policy, guidance, oversight and event response, and licensing activities, for NRC licensees and applicants. When the source of cyber threats can be attributed to elements in the supply chain (e.g., sources of supply, manufacturing vulnerabilities, and distribution channels), a collaborative effort is necessary to address cyber threats. Representatives from NRO and NSIR offices participated in discussion topics facilitated through the Working Group on Cyber Security Supply Chain Oversight to formulate a unified strategy for responding to cyber security threats emanating from the supply chain.

IMPLEMENTATION:

As a result of activities of the working groups, the staff identified 24 issues, which are listed in more detail in the working groups' final report, "Staff Review of Counterfeit, Fraudulent, and Suspect Items (CFSI)" (ADAMS Accession Number ML112130293). The planned actions to address these issues fit into five categories and are summarized below. The working groups' final report contains a more detailed description of the agencywide strategy and plan, implementation goals, and impacted offices.

Endorsement of Industry Process Enhancements and Best Practices:

- The staff will establish periodic meetings with stakeholders, including industry representatives, for the purpose of communicating each party's progress and direction, sharing best practices, and understanding and assisting with any identified barriers to success.

- The staff will issue generic communications to share industry efforts to address CFSI.

Developing or Clarifying Regulatory Guidance:

- The staff will coordinate with the effort to clarify 10 CFR Part 21, "Reporting of Defects and Noncompliance," to specifically define CFSI in guidance as a deviation that requires

evaluation under 10 CFR Part 21 and a condition adverse to quality under Criterion XVI, "Corrective Action," of Appendix B to 10 CFR Part 50.

- The staff will continue with cyber security program development activities, to include verification and assessment of appropriate system and service acquisition security controls as required by the cyber security plan. The NRC has approved implementation schedules for each site as required by the cyber security rule, 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks."

- The staff will continue with development of guidance for vendor inspection of safety-related CDAs. The licensees have committed to implement system and service acquisition security controls in their cyber security plans. The NRC will inspect the implementation of these controls in accordance with 10 CFR 73.54(f).

Communication:

- The staff will continue to issue generic communications or otherwise notify the industry of cyber or other clandestine threats to CDA supply chains that the NRC identifies through the operating and construction experience programs or through research conducted by the staff.

- The staff will incorporate CFSI information from appropriate sources (domestic and international) and related industry organizations that could apply to U.S. commercial nuclear facilities into the current NRC operating experience and construction experience programs.

- The staff will continue to promote information sharing through interagency outreach efforts with appropriate Federal agencies (e.g., U.S. Government Inter-Agency Anti-Counterfeiting Working Group, DOD, Department of Energy, Department of Homeland Security, National Aeronautics and Space Administration, Department of Justice, etc.). Affected directives and implementing procedures will be revised as necessary.

Training:

- The staff will continue to communicate with stakeholders via the NRC's existing generic communications program about any potential CFSI training or applicable informational sources that could increase awareness of CFSI.

- The staff will emphasize through the NRC's allegations training module that the allegation process should be used when a licensee, a supplier, or an NRC staff member identifies CFSI.

- The staff will develop training for NRC inspectors to assist them in assessing the effectiveness of programs and processes of licensees and suppliers of basic components to identify and prevent CFSI.

Inspecting for Effective Industry Oversight for Detecting and Preventing CFSI:

- The staff will evaluate the need to develop and implement a pilot program to inspect a limited number of licensees to assess the effectiveness of their 10 CFR Part 21, procurement, and commercial-grade dedication programs and the need for ongoing inspections under the Reactor Oversight Process.

- The staff will evaluate the need to provide additional guidance in NRC inspection procedures to assess the effectiveness of the programs and processes of licensees and suppliers of basic components to identify and prevent CFSI.

- The staff will develop new inspection guidance focused on suppliers of safety-related CDAs contained in the cyber security plan.

- The staff will conduct NRC vendor inspections at suppliers of safety-related CDAs, in accordance with 10 CFR Part 21 and evaluate the results of these inspections to determine the need to expand the inspection sample to suppliers and subsuppliers of nonsafety-related CDAs.

- The staff will continue to inspect and verify licensees' implementation of their cyber security programs including commitments for supplier oversight. The staff has issued Regulatory Guide 5.71 as an acceptable approach for licensees to meet the cyber security rule requirements.

- The staff will continue to implement the existing program for inspecting sources and materials to meet the governing regulatory requirements. The staff will continue to periodically inspect licensees and work with the Agreement States and the Food and Drug Administration. The NRC will perform an agencywide reassessment in the future to determine if any additional effort is needed in this area.

- The staff will continue to implement the existing NRC fuel cycle facility oversight programs and spent fuel storage and radioactive material transportation activities, which include quality assurance controls such as management measures that can contribute to the identification and prevention of CFSI. The staff will monitor the results from the CFSI task force's efforts and will integrate any best practices and lessons learned into the program as necessary.

- The staff will perform an agencywide reassessment in FY 2014 to determine the effectiveness of the implemented measures and pilot programs and to determine the need to implement additional CFSI countermeasures. Included in this assessment will be a review of CFSI operating experience and a collaboration of the working groups to assess if any changes need to be implemented.

RESOURCES:

The staff plans to expend the following resources to implement the actions outlined in the plan. NRO is the most impacted and has budgeted resources that can be reallocated. Other offices will need to reallocate or use the add/shed process in order to fund the proposed actions.

| | **FY12** | **FY13** | **FY14** |
|---|---|---|---|
| | **FTE** | **FTE** | **FTE** |
| FSME | 0.1 | 0.0 | 0.0 |
| HR | 0.1 | 0.1 | 0.1 |
| IP | 0.1 | 0.0 | 0.0 |
| NMSS | 0.2 | 0.1 | 0.1 |
| NSIR | 0.5 | 0.5 | 0.5 |
| NRO | 0.9 | 0.6 | 0.6 |
| NRR | 0.2 | 0.2 | 0.2 |
| OGC | 0.2 | 0.2 | 0.2 |
| OE | 0.1 | 0.1 | 0.1 |
| OI | 0.2 | 0.1 | 0.1 |
| **TOTAL** | **2.3** | **1.6** | **1.6** |

COORDINATION:

This action has been coordinated with the Office of the General Counsel (OGC). OGC has reviewed this package and has no legal objection.

The Chief Financial Officer reviewed this package and determined that it has no financial impact.

***/RA by Michael F. Weber for/***

R. W. Borchardt
Executive Director
for Operations