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

Contents

1.0 SUMMARY

The U.S. Nuclear Regulatory Commission (NRC) established the counterfeit, fraudulent, and suspect items (CFSI) working groups to focus on the development and implementation of a formal agencywide strategy and plan to monitor and evaluate CSFI. This action was, in part, conducted in response to Recommendation 10 of the Office of the Inspectors General's (OIG's) report OIG-10-A-20, "Audit of NRC's Vendor Inspection Program," dated September 28, 2010. The Office of New Reactors (NRO) led the efforts and coordinated with other NRC offices to develop a formal agencywide strategy to monitor and evaluate CFSI.

On December 8, 2010, NRO organized an agencywide kickoff meeting for the CFSI community. One of the objectives of this meeting was to form working groups that applied to each office. During this meeting, each organization was asked to respond to a 16-question CFSI community survey to provide a starting point for the working groups. A steering committee was instituted with representatives from the various NRC offices that would be affected by CFSI. The CFSI Steering Committee comprised senior management personnel from 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 Enforcement (OE), the Office of Investigations (OI), and the Office of General Counsel (OGC).

The CFSI Steering Committee approved the following program charter to focus the resources of the newly formed task force:

> 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 agencywide 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.

Four working groups were created consistent with the approved CFSI program charter:

- Working Group on Supply Chain Oversight
- Working Group on Communication
- Working Group on Response Protocols
- Working Group on Cyber Security Supply Chain Oversight

Each working group was 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. Each working group followed a similar methodology in coming up with issues or potential issues related to the potential to let CFSI into entities regulated by the NRC.

First, each working group identified current NRC regulations, NRC and industry guidance, and industry practices. These findings comprise the current regulatory basis and status quo of the industry.

Next, the working groups gathered and assessed information relating to current counterfeiting activity, security risks and events, current practices in non-NRC-regulated activities, and proposed activities in NRC-regulated activities. The working groups assessed operating experience internal to the commercial nuclear industry, such as that collected by the Nuclear Energy Institute (NEI) and the Electric Power Research Institute (EPRI), and external experience, such as that collected by the U.S. Department of Energy (DOE), U.S. Department of Defense (DoD), the National Aeronautics and Space Administration (NASA), and the Aircraft Industry Association (AIA). Various government agencies, industry organizations, and commercial entities have published a number of recent works to try to educate their stakeholders and the supply community on how to respond to the issue of CFSI. Although a great number of these are still focused on receipt activities performed at the receiving dock, many are more proactive in nature. These proactive measures are evident in such changes as the adoption of standard anticounterfeiting procurement clauses, mandating strict due diligence in selecting appropriate suppliers and distributors, and requiring the prevention of identified CFSI from being reintroduced into the supply chain.

Following these research efforts, the working groups brainstormed to develop vulnerabilities, issues, or potential issues that exist in the current NRC regulations and practices that could allow the introduction of CFSI. It soon became apparent that each working group was identifying similar issues, so the group leaders decided to consolidate further discussions. This allowed them to capture the input from the individual working groups and consolidate it into unified responses for each identified issue.

After agreeing on the issues, the working groups began discussing ways to resolve these issues, using best practices and applicable operating experience. The groups assessed the issues for their relative safety benefit, further assessed them along with potential solutions, and came up with final recommendations. The issue statements, a description of each issue, the associated issue's assessments, and recommendations follow later in this report, organized by the four key areas they represent.

2.0 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. 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.

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 responded, in cooperation with internal investigators and law enforcement officials, by participating in investigations to identify and prosecute the sources of these materials.

The NRC issued generic communications to inform licensees and suppliers of 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 a study of the electronics supply chain supporting DoD. The report 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 387 original equipment manufacturers (OEMs), original component manufacturers, electronics distributers, brokers, and suppliers to DoD. The survey was extensive, asking 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. This trend appears to repeat itself in other heavily industrialized business sectors as well, including the petroleum, automotive, transportation, and commercial airline industries.

Current Factors Influencing the Introduction of CFSI

Historically, obsolete parts have served as the targets 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. However, the DOC study shifted that paradigm by reporting that obsolescence was only 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. 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 the Nuclear Procurement Issues Committee (NUPIC) and EPRI, the staff determined that the following factors were influencing CFSI:

- 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 in CFSI
- a sense of complacency based on the belief that someone else along the supply chain had been checking for CFSI
- using commercially manufactured parts or components in applications requiring high degrees of quality assurance

3.0 CURRENT REGULATORY BASIS

The current NRC regulations contain provisions which can be interpreted and applied to address CFSI. Nonetheless, the agency had not specifically written the regulations to address CFSI, giving rise to a potential for issues to exist. Regulatory requirements related to CFSI include the following:

- requirements for a quality assurance program under various regulatory requirements, including 10 CFR Part 50 Appendix B
- reporting requirements, such as those in 10 CFR 50.72, "Immediate Notification Requirements for Operating Nuclear Power Reactors"; 10 CFR 50.73, "Licensee Event Report System"; and 10 CFR Part 21, "Reporting of Defects and Noncompliance"
- requirements on deliberate misconduct, such as those in 10 CFR 50.5 and 10 CFR 110.7b, "Deliberate Misconduct", and 10 CFR 50.9, "Completeness and accuracy of information"
- 10 CFR 50.65, "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants" (maintenance rule)
- 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks" (cyber security rule)

In Appendix B to 10 CFR Part 50, the NRC establishes requirements for quality assurance and quality control for safety-related structures, systems, or components (SSC), which are necessary to provide adequate assurance that a SSC will perform satisfactorily in service. The requirements apply to all activities affecting the safety related functions of those SSCs, including designing, purchasing, fabricating, handling, shipping, storing, cleaning, erecting, installing, inspecting, testing, operating, maintaining, repairing, refueling, and modifying.

In 10 CFR Part 21, the NRC establishes requirements for reporting to the agency defects that are identified in "basic components." In commercial nuclear power plants licensed or certified under 10 CFR Part 50 or 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," a basic component is an SSC that ensures integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe-shutdown condition, or the capability to prevent or mitigate the consequences of accidents. For other facilities and other activities licensed under 10 CFR Parts 30, 40, 50 (other than nuclear power plants), 60, 61, 63, 70, 71, or 72, a basic component is an SSC that affects a safety function and in which a defect or failure to comply with any applicable regulation in the regulation, order, or license issued by the Commission could create a substantial safety hazard. The concept of a basic component includes safety-related design, analysis, inspection, testing, fabrication, replacement of parts, or consulting services that are associated with the component hardware, design certification, design approval, or information in support of an early site permit application (under 10 CFR Part 52), whether these services are performed by the component supplier or others. The regulations of 10 CFR 21 require that the Commission be notified of defects and failures to comply associated with basic components used in NRC-licensed or certified facilities.

In 10 CFR 50.65, the NRC includes requirements for safety-related and selected nonsafety-related SSCs. The rule requires the licensee to demonstrate through monitoring, that it is effectively controlling the performance or condition of an SSC, such that the SSC remains capable of performing its intended function, or that there is a basis for determining that the SSC is capable of meeting its intended function.

In 10 CFR 73.54, the NRC introduced the cyber security threat element to a broad range of components, including those that are safety-related or security-related. The regulations also include selected support equipment and structures. The regulation provides the legal basis for accepting supplier controls for these components, collectively referred to as Critical Digital Assets (CDA), to prevent the introduction of products that could contain a cyber threat.

In 10 CFR 70.62, the NRC establishes safety program requirements for uranium enrichment and fuel fabrication facilities. The safety program is comprised of process safety information, integrated safety analysis and management measures. Management measures are defined in 10CFR70.4 as functions performed by the licensee, generally on a continuing basis, that are applied to items relied on for safety (IROFS), to ensure the items are available and reliable to perform their functions when needed. Management measures include configuration management, maintenance, training and qualifications, procedures, audits and assessments, incident investigations, records management, and other quality assurance elements.

4.0 EXTERNALLY PROPOSED LEGISLATION AND INDUSTRY INITIATIVES

The threat from CFSI is by no means exclusive to threats against commercial nuclear power plants. Documented examples of counterfeit material, parts, and related documentation are now plentiful in the heavy industry market sectors and involve common commodities, from structural steel to electronic microchips. DoD experiences a high prevalence of CFSI; a recent DOC study of DoD procurement practices indicated that 39 percent of all electronic distributors to DoD encountered some form of CFSI. In response, the U.S. Government initiated a review of the current Federal Acquisition Regulations (FAR) to identify and amend areas of the regulations that create vulnerabilities for CFSI. This inter-agency effort was named The U.S. Government's Anti-Counterfeiting Working Group. Although the product of this group's efforts are not directly applicable to NRC licensees, the staff is following this activity to determine if the actions taken provide a basis and a need for revisions to NRC requirements.

NEI and EPRI are updating guidance for industry relating to the procurement and receipt of items, as well as other guidance related to counterfeit and fraudulent items. They are also currently updating their training programs with newer inspection practices and better tools. EPRI is currently testing a suspected counterfeit and fraudulent item incident database that can be used for online reporting and searching of related information. This database will be able to share pertinent data with the NRC, DOE, engineering and procurement firms, manufacturers, and suppliers. NEI is also developing a standard procurement clause that can be used in purchasing documents that will aid the screening and reporting of CFSI.

5.0 SUPPLY CHAIN OVERSIGHT WORKING GROUP

This working group examined current NRC regulations, guidance, and procedures governing the oversight of licensee's and suppliers of basic components used to keep CFSI out of the nuclear supply chain of NRC-regulated activities. The working group also reviewed current industry practices along with external government regulations and policies to gain insight into how other agencies and industries are dealing with CFSI. The working group then examined the insights gained from external agencies and industry to identify possible areas within the NRC that may benefit from an improvement or change.

The working group reviewed the following discussion topic areas during roundtable discussions:

- control of CFSI inventory
- applicability to fuel facilities and fuel production
- counterfeit circuit breakers
- counterfeit materials, fasteners, and piping/fitting
- fraudulent documentation
- storage casks
- counterfeit electronics
- repair and service contractors
- commercial-grade dedication
- reverse engineering

The discussion topic areas served as a starting point to help narrow the focus areas to examine the effective methods available for detecting and preventing the entry of CFSI into the supply chain. The roundtable discussions with the Supply Chain Oversight Working Group resulted in the identification of eight issues. Below is a summary of each issue, a brief summary of the current regulatory structure, the issue analysis, and detailed recommendations.

5.1 Issue 1: Authentication and Testing

The NRC currently has no regulatory guidance or requirements for the authentication and testing of components necessary to identify a counterfeit or fraudulently identified item.

Description

Electronic microchips contain electrical, electronic, and electromechanical devices (EEE), ranging from discreet items to integrated circuits mounted on printed circuit boards. A typical microchip consists of three distinct parts:

(1) Package. A black package that protects the internal circuitry and the silicon "die" and gives a surface for etched tracking codes. The tracking code is a combination of part number, date, and serial numbers.

(2) Terminal frame. The terminal frame is also known as the pin frame or the "spider."

(3) Die. The silicon die houses the integrated circuitry or microchip.

Outside of the commercial nuclear field, reported incidents indicate that counterfeiters have learned how to open a package, in a process known as “de-capping,” and replace the original integrated circuitry dies with dies of lesser quality or older, or with well-worn dies of questionable origin. Dust manufactured from ground-up packaging can be mixed with epoxy paint to “blacktop” a reworked component. Then, counterfeiters can re-etch the package with fraudulent markings. The reworked component is difficult, if not impossible, to detect by visual inspection or by scratching the resurfaced blacktop. Even with a scanning electron microscope, detection is difficult. One way to combat these incidents is to ensure that items and components are procured from the OEM, which is a practice often used among nuclear licensees. Performing full functional testing of electronic devices to ensure they will perform their intended safety functions is an acceptable alternative to using an authentic part, only if the tests envelope all of the parameters needed by the item to perform its safety function. This level of assurance is rarely achieved by “burn-in” testing alone. Burn-in testing alone, even at extended times & temperatures is effective for detecting manufacturing defects (e.g. infant mortality) but cannot be relied upon to determine if the item had been mishandled, poorly assembled, or will perform as specified under accident conditions. The NRC currently has no regulatory guidance or requirements for the authentication and testing of components necessary to either identify a counterfeit or fraudulently identified item or to require procurement from the OEM or an OEM-authorized distributor.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—There does not appear to be an adverse trend in industry operating experience that could cause a threat to nuclear safety-related applications. Furthermore, the NRC requires nuclear power plant licensees to have a QA program under Appendix B to 10 CFR Part 50. Generic Letter 89-02, “Actions To Improve the Detection of Counterfeit and Fraudulently Marketed Products,” dated March 21, 1989, also describes a sampling plan and engineering verification of critical characteristics in regards to a commercial-grade dedication program. The work group determined the guidance stated in Generic Letter 89-02 to be adequate. However, based on DoD experience, the risk is still present because items or components could possibly pass receipt inspection and fail later in service. However, because these components are not manufactured in a controlled environment, their failures would not be consistent enough to increase common-cause failure rates. Therefore, the safety benefit of addressing this issue was determined to be low to medium.

- Costs—In order to address this issue, the NRC could conduct rulemaking to require licensees and suppliers of basic components to either (1) procure directly from the Original Equipment Manufacturer (OEM) or an authorized distributor, or (2) use specific testing methods upon receipt inspection to verify the integrity of selected components. Alternatively, the NRC could issue a generic communication to clarify practices and recommendations that are already available to the industry. Rulemaking would have a high internal cost and would have a moderate-to-high cost to regulated entities. Associated costs for issuing a generic communication would be minimal because external organizations would simply update their receipt inspection process and both pretesting and post testing installation as they deem appropriate.

Recommendations

The NRC should include this issue in a generic communication that also addresses other issues identified by the CFSI working groups. The emphasis in such a communication would be to promote authentication guidance and testing along with batch sampling to increase assurance in preventing CFSI. Recommendation 3 captures this action.

Also, the NRC should increase industry awareness of inspection techniques for complex components and work with the collective efforts of the U.S. Government's Anti-Counterfeiting Working Group. The NRC should periodically document developments and efforts for future implementation. Section 10.0, Recommendation 2 captures this action.

5.2 Issue 2: Identify Fraudulent Documentation

The NRC has no guidance that specifically addresses the need for licensees or suppliers to implement programs to identify fraudulent documentation.

Description

Currently, licensees and suppliers review documentation in terms of procurement of inventory during their receipt inspection process. Experience shows that documentation plays a key role in the ability of a counterfeit or fraudulent item to successfully pass through receipt inspection and potentially be installed into a safety-related application. However, if a document's data conflict with the markings on the item, or if the document has any anomalies, the receiving personnel could be alerted that the item is possibly a CFSI. Commercial-grade dedication programs and the applicable areas under Appendix B to 10 CFR Part 50 are used to ensure that the items received meet the critical characteristics, however, the NRC has no specific guidance for identifying and evaluating fraudulent documentation. Licensees and suppliers can incorporate additional industry guidance if they so choose to enhance their programs. Often, clues discovered in the documentation packages accompanying the product provide valuable insight into the existence of wrongdoing.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—The NRC requires nuclear power plant licensees to have a QA program under Appendix B to 10 CFR Part 50. Generic Letter 89-02 also describes a sampling plan and engineering verification of critical characteristics in regards to a commercial-grade dedication program. Due to the control the NRC already requires in Appendix B as further explained in generic letters, the safety benefit of addressing this issue was determined to be low.

- Costs—In order to address this issue, the NRC could conduct rulemaking to require licensees and suppliers to implement programs to identify fraudulent documentation, or the NRC could issue a generic communication to clarify practices and recommendations that are already available to the industry. Rulemaking would have a high internal cost and would have a moderate to high cost to regulated entities. The costs associated with issuing a generic communication would be minimal because external organizations would update their receipt inspection process as they deem appropriate.

Recommendations

The NRC should include this issue in a generic communication that will also address other issues, with the emphasis on promoting proactive industry practices for receipt inspection. Section 10.0, Recommendation 3 captures this action.

5.3 Issue 3: Passed-Down Contractual Requirements

Current NRC requirements do not mandate that licensees pass down contractual requirements for supplier CFSI programs to identify and eliminate fraudulent goods obtained from subsuppliers.

Description

Currently, licensees and vendors use their receipt inspection process to ensure that the items they are procuring meet their purchase orders. To create another layer of protection, EPRI is currently working on guidance that the licensees and vendors can use to include specific wording in the contractual requirements that are passed down to the suppliers. The goal is to identify and eliminate fraudulent goods obtained from subsuppliers. The NRC currently does not require licensees and vendors to pass down contractual requirements for supplier CFSI programs to identify and eliminate fraudulent goods obtained from subsuppliers.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—Appendix B to 10 CFR Part 50, Criterion XV addresses nonconformances. Licensees and vendors are required to use their nonconformance process if they identify a discrepancy during receipt inspection. In addition, EPRI is currently developing specific wording for licensees and vendors to include in their contractual agreements that will aid in identifying and eliminating fraudulent goods. Due to the requirements in Appendix B and the nonconformance processes that licensees and vendors are required to follow, the safety benefit of addressing this issue was determined to be low.

- Costs—To address this issue, the NRC could conduct rulemaking to require licensees to explicitly require CFSI activities in their procurement documents, or the NRC could issue a generic communication to clarify practices and recommendations that are already available to the industry. Rulemaking would have a high internal cost. The associated costs of issuing a generic communication would be minimal because external organizations would simply update their procurement and receipt inspection processes as they deem appropriate.

Recommendations

The NRC should include this issue in a generic communication that addresses other issues, with emphasis on endorsing or conditionally endorsing the guidance that EPRI is currently developing. The EPRI guidance provides specific wording that licensees and vendors should use in their contractual requirements. Section 10.0, Recommendations 2 and 3 capture this action.

5.4 Issue 4: Regulatory Treatment of Nonsafety Systems

The NRC currently has no regulatory guidance for implementing measures to prevent CFSI associated with the regulatory treatment of nonsafety systems (RTNSS).

Description

In the early 1990s, the NRC developed an approach to address the proposed increased use of passive safety features in advanced reactor designs. Unlike the operating reactors of that era, the passive advanced light-water reactor designs, such as the AP600 and the AP1000 designs, proposed extensive use of safety systems that rely on the driving forces of buoyancy, gravity, and stored energy sources. In addition to the active systems used during normal plant operations, the passive advanced light-water reactor designs proposed nonsafety-grade active systems to provide defense-in-depth capabilities for reactor coolant makeup and decay heat removal. These systems would be the first line of defense to reduce challenges to the passive systems in the event of transients or plant upsets. The licensing-related analyses proposed by the industry for the passive designs rely solely on the passive safety systems to demonstrate compliance with the acceptance criteria of various design-basis transients and accidents. To incorporate the defense-in-depth measures into the licensing process, while recognizing the role of the passive safety features in responding to design-basis events, the staff and industry developed the RTNSS process.

Currently, the NRC has no specific guidance on the prevention of CFSI for any SSCs that fall under the RTNSS label.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—RTNSS applies to nonsafety-grade systems that add defense in depth to passive safety-related systems. Therefore, the safety benefit of addressing this issue was determined to be low.

- Costs—The NRC could conduct rulemaking to create regulations to require a program that would prevent CFSI in regards to RTNSS, or the NRC could continue to promote training and awareness in CFSI procurement activities and evaluation of CFSI once identified. The associated costs for the latter solution would be minimal because the NRC would be using its current process to share information from the industry and other government sources of information.

Recommendations

The NRC should address the issue by using the agency's continual effort to interact with the industry to identify methods of training and awareness, as well as how to evaluate CFSI once identified. The agency should periodically review operating experience to evaluate for any trends and reassess as necessary. Section 10.0, Recommendation 2 captures this action.

5.5 Issue 5: Procurement of Nonsafety-Related Critical Infrastructure Equipment

The NRC does not have regulatory requirements associated with preventing CFSI in the procurement of nonsafety-related critical infrastructure equipment.

Description

Appendix B to 10 CFR Part 50 has procurement requirements but only applies to safety-related applications. 10 CFR 73.54 applies to all CDAs and in addition, Appendix B to 10 CFR Part 50 also applies to safety-related CDAs. However, there currently is no regulatory equivalence of Appendix B to 10 CFR Part 50 for nonsafety-related CDAs.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—Licensees must follow the regulations in Appendix B to 10 CFR Part 50 in regards to safety-related applications. Because this issue covers nonsafety-related critical infrastructure equipment, the safety benefit of addressing this issue was determined to be low.

- Costs—The NRC plans to continue to monitor applicable operating experience as well as to interact with members of the industry about industry guidance and recommendations. The costs associated with this plan was determined to be minimal.

Recommendations

The NRC should address the issue by establishing periodic meetings to interact with NEI and other industry representatives as the industry formalizes voluntary initiatives. Section 10.0, Recommendation 1 captures this action.

5.6 Issue 6: Procurement of NRC-Regulated, Nonreactor Items (NMSS)

The NRC has no regulations or guidance documents that define explicit controls for the prevention of CFSI in the procurement of NRC-regulated, nonreactor items (e.g., items relied on for safety (IROFS), items important to safety).

Description

When applied to facilities and activities other than nuclear power plants, a basic component is an SSC, or part thereof, that affects their safety function that is directly procured by the licensee of a facility or activity subject to the regulations in 10 CFR Part 21, and in which a defect or failure to comply with any applicable regulation, order, or license issued by the Commission could create a substantial safety hazard. The concept of a basic component encompasses safety-related design, analysis, inspection, testing, fabrication, replacement of parts, or consulting services that are associated with the component hardware.

For the procurement of non-reactor items for use in NRC-regulated facilities, 10 CFR Part 21 applies to basic components as defined in the regulations or in an NRC-approved exemption[1]. However, the NRC currently has no regulations or guidance documents that define explicit controls for the prevention of CFSI in the procurement of NRC-regulated, nonreactor items in fuel cycle facilities and spent fuel storage and radioactive material transportation activities.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—An adverse trend in industry operating experience, that could cause a threat to nuclear safety related applications, does not appear to be present. Non-reactor licensees and certificate holders are inspected periodically and are required to (1) implement the procurement requirements specified in 10 CFR Part 21 for the purchase of basic components and (2) have QA controls in place, which can contribute to the identification and prevention of CFSI. Such QA controls may include a system of management measures, a QA program that complies with ASME NQA-1 or Appendix B to 10 CFR Part 50, or other QA requirements defined in the CFR or license commitments (See Issue 7 for further details). These QA controls include requirements for procurement documents, control of purchased items and services, and for performing inspections and addressing nonconforming items. Given the effectiveness of the QA controls and the regular inspections of these activities, the safety significance of this issue was determined to be low.

- Costs—There are no additional costs associated with this issue. The NRC periodically inspects these facilities and reassesses actions necessary based on applicable operating experience.

Recommendations

The NRC should continue with its existing oversight programs for fuel cycle facilities and spent fuel storage and radioactive material transportation activities. The NRC will inspect these facilities and activities periodically and include the issue in a generic communication that also addresses other issues identified in the CFSI working groups and monitor CFSI activities such as periodic meetings, to integrate as necessary. Section 10.0, Recommendation 18 captures this action.

5.7 Issue 7: CFSI at NMSS-Regulated Facilities and Activities

The NRC has no regulatory requirements specifically targeted at preventing, detecting, or communicating incidences of CFSI at fuel cycle facilities and in spent fuel storage and radioactive material transportation activities.

---

[1]Many fuel cycle facilities licensed under 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," have requested, and been granted, exemptions to the definitions of 10 CFR Part 21 in order to more clearly delineate the applicability of 10 CFR Part 21 to enrichment and fuel fabrication facilities and to incorporate terminology used in Part 70 (i.e. IROFS).

Description

The regulations in 10 CFR Part 70 control uranium enrichment, plutonium processing, and fuel Fabrication. They require that applicants and licensees develop and maintain a safety program that includes management measures. Management measures are functions performed by the licensee to ensure that IROFS are available and reliable to perform their functions when needed. Management measures are submitted as part of the license application for NRC review and approval and include such topics as configuration management, maintenance, training, qualifications, procedures, audits and assessments, incident investigations, records management, and other quality assurance elements. In addition to implementing management measures, plutonium processing and plutonium fuel fabrication facilities are required to have a QA program that meets the requirements of Appendix B to 10 CFR Part 50.

The regulations in 10 CFR Part 71 control the packaging and transportation of radioactive material. Subpart H of Part 71 provides QA requirements that must be applied to the design, purchase, fabrication, handling, shipping, storing, cleaning, assembly, inspection, testing, operation, maintenance, repair, and modification of components of packaging that are important to safety. The regulations in 10 CFR Part 72 control the storage of spent nuclear fuel and radioactive waste. Subpart G of Part 72 specifies requirements for the establishment, maintenance, and execution of QA programs used for the design, purchase, fabrication, handling, shipping, storing, cleaning, assembly, inspection, testing, operation, maintenance, repair, modification of SSCs, and decommissioning that are important to safety.

The regulations in 10 CFR Part 76 control the certification of gaseous diffusion plants. In accordance with § 76.93, gaseous diffusion plant certificate holders must establish, maintain, and execute a QA program that satisfies the requirements of ASME NQA-1-1989, "Quality Assurance Program Requirements for Nuclear Facilities."

The regulations in 10 CFR Part 40 control the issuance of licenses to receive title to, receive, possess, use, transfer, or deliver source and byproduct materials. License applicants are required to provide a description of QA procedures that will be used in facility surveillance programs and to limit potential radiation doses resulting from depleted uranium. Currently, 10 CFR Part 40 is undergoing rulemaking that will add further QA requirements similar to those contained in 10 CFR Part 70.

Currently, the NRC has no regulatory requirements specifically targeted at preventing, detecting, or communicating incidences of CFSI at fuel cycle facilities and in spent fuel storage and radioactive material transportation activities. However, the implementation of the QA controls described above, in addition to continuous NRC oversight of these programs, provides an array of quality assurance elements that can contribute to the identification and prevention of CFSI.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—An adverse trend in industry operating experience that could cause a threat to nuclear safety related applications does not appear to be present. Fuel cycle facilities and spent fuel storage and radioactive material transportation activities are inspected periodically and are required to have a system of QA controls that can contribute to the identification and prevention of CFSI. Therefore, the safety significance of this issue was determined to be low.

- Costs— There are no additional costs associated with this issue. The NRC will continue to periodically inspect these facilities and activities and reassess actions necessary based on applicable operating experience.

Recommendations

The NRC should continue with its existing enrichment and fuel fabrication facility programs and spent fuel storage and radioactive material transportation activities, which include QA controls that can contribute to the identification and prevention of CSFI. NRC will continue to inspect these facilities periodically and include the issue in a generic communication that also addresses other issues identified in the CFSI working groups and monitor CFSI activities such as periodic meetings, to integrate as necessary. Section 10.0, Recommendation 18 captures this action.

5.8 Issue 8: Procurement of CFSI in Medical and Industrial Items

The NRC has no regulations or guidance documents that define explicit controls for the prevention of CFSI in the procurement of NRC-regulated medical and industrial items associated with materials licenses.

Description

The NRC and Agreement States inspect byproduct materials, manufacturing, and distribution licensees for compliance with regulations, licensing conditions, and commitments. The NRC has a memorandum of understanding (MOU) with the U.S. Food and Drug Administration (FDA) because both the NRC and FDA have regulatory responsibilities for medical devices, drugs, and biological products using byproduct, source, or special nuclear material. Through the MOU, both agencies have agreed to promptly inform each other whenever they receive a report or otherwise become aware of a potential public health problem, such as a malfunction, failure, or medical event involving products of mutual regulatory concern. No NRC regulations or guidance documents exist to define explicit controls for the prevention of CFSI in the procurement of NRC-regulated medical and industrial items.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—No operating experience or events have been identified. The NRC and FDA conduct periodic inspections in their applicable regulated fields and communicate with each other if an issue occurs that is related to the other's regulated field. Therefore, the safety benefit of addressing this issue was determined to be low.

- Costs—There are no additional costs associated with addressing this issue. The NRC will continue to inspect licensees and work with Agreement States and FDA to protect public health and safety.

Recommendations

The NRC should continue to periodically inspect licensees and work with the Agreement States and FDA. Perform an agencywide reassessment in the future to determine if any additional effort is needed. Section 10.0, Recommendation 17 captures this action.

6.0 COMMUNICATION WORKING GROUP

This working group focused on regulations, guidance, and industry practices related to communicating about CFSI. Effective sharing of CFSI information has been proven to be a significant proactive tool in preventing the infiltration of CFSI into an industry's supply chain. The majority of OEMs and original component manufacturers draw from many of the same resources to design, manufacture, and assemble their final products, particularly in electronic component assembly. Sharing accurate CFSI information quickly and with the appropriate recipients can significantly help to accomplish the following:

- minimize the quantities of fraudulent items associated with a specific incident
- prevent future purchases
- preserve investigatory information
- provide the appropriate authorities with adequate time to take appropriate actions

Sharing CFSI information also provides useful information for proactive CFSI prevention, such as the following:

- incorporating anti-CFSI countermeasures into future product designs

- developing realistic training modules tailored to specific job descriptions that could contribute to preventing the spread of CFSI

- assisting in performing effective receipt inspections for CFSI by providing a central repository to find information and images relating to specific items or components

6.1 Issue 9: Reporting Thresholds

Current reporting requirements only mandate the reporting of defects and failures to comply that could lead to a substantial safety hazard and significant events driven by equipment failures. Basic components that are determined to be CFSI but do not constitute a substantial safety hazard or cause a reportable event would not have to be reported.

Description

Currently, 10 CFR Part 21 is the main reporting mechanism for CFSI. The regulation in 10 CFR Part 21 requires the evaluation and reporting of supplied basic components that contain a defect or that fail to comply with the Atomic Energy Act of 1954, as amended, or any applicable rule, regulation, order, or license of the Commission or standard design approval under 10 CFR Part 52, relating to a substantial safety hazard. As the regulation applies to CFSI, the staff concluded that counterfeit and fraudulent items constitute deviations in basic components and in certain facilities could create a substantial safety hazard. Therefore, counterfeit or fraudulent items should be evaluated and reported consistent with the guidance afforded for a defect in accordance with 10 CFR Part 21.

The NRC defines “substantial safety hazard” in 10 CFR Part 21 as follows:

> a loss of safety function to the extent that there is a major reduction in the degree of protection provided to public health and safety for any facility or activity licensed or otherwise approved or regulated by the NRC, other than for export, under parts 30, 40, 50, 52, 60, 61, 63, 70, 71, or 72 of [Title 10 of the *Code of Federal Regulations*].

During construction under 10 CFR Part 50 or 10 CFR Part 52, evaluation and reporting of defects is satisfied under 10 CFR 50.55(e). During operation under 10 CFR Part 50 and 10 CFR Part 52, evaluation and reporting of defects is satisfied under 10 CFR Part 21, 10 CFR 50.72, and 10 CFR 50.73. Safeguard events related to defects may be evaluated and reported under 10 CFR 73.71, “Reporting of Safeguards Events,” rather than 10 CFR Part 21. These reporting requirements have a similarly high significance threshold to 10 CFR Part 21. Non-reactor facilities perform the evaluation and reporting of defects and failures to comply in accordance with 10 CFR Part 21 during construction and operations. In all cases, vendors of basic components are subject to the reporting requirements of 10 CFR Part 21.

Therefore, under the current regulatory guidance, CFSI identified, evaluated, and determined not to be reportable by a vendor or licensee are not required to be communicated to the NRC or other affected parties. As a result, the potential exists that other affected entities could be affected by the same source of CFSI without knowing.

The work group acknowledges that the threshold established by the above regulations, in addition to robust quality assurance programs, is adequate to protect the public health and safety and the environment. However, safety could be enhanced by promoting more proactive communication of CFSI.

During the CFSI public meeting held on June 30, 2011, NEI informed the NRC staff that the Institute of Nuclear Power Operations (INPO) requires the reporting of all CFSI and has a process for disseminating that information. EPRI also informed the NRC staff that it is developing a CFSI database. The EPRI database is populated voluntarily by EPRI members, and information is shared with members. EPRI indicated that it would be willing to work with the NRC to continue to develop the database and promote its use. EPRI also stated that it was open to sharing certain nonsensitive information with entities other than power reactors if information flowed in both directions.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—The safety benefit of addressing this issue was determined to be high because of the generic impacts of failure to communicate about CFSI. However, the work group recognizes that a robust quality assurance program is the key to preventing CFSI and that industry efforts are in progress to address this issue.

- Costs—In order to address this issue, the NRC could conduct rulemaking to expand the scope of 10 CFR Part 21 or create a new CFSI reporting rule. The latter may require a change to the NRC's statutory authority. These activities have a high internal cost and would have a moderate-to-high cost to regulated entities. The NRC could work to endorse the industry's voluntary initiatives and issue generic communication. The costs associated with these activities would be low to moderate internally and externally.

Recommendations

The work group recommends that the NRC establish periodic meetings with the industry to formalize the ongoing voluntary initiatives such as use of the corrective action program for CFSI and information-sharing efforts such as the EPRI CFSI database. The staff will monitor implementation and may reevaluate the need for rulemaking in the future. Recommendation 1 captures these actions.

The task group also recommends clarifying the definition of "deviation" to include CFSI in the ongoing 10 CFR Part 21 rulemaking and guidance effort. Section 10.0, Recommendation 4 captures this action.

6.2 Issue 10: Regulatory Definitions

There is no specific documented NRC position on whether CFSI constitutes as a deviation, failure to comply, or a condition adverse to quality as defined in existing rules and guidance. As a result:

- "evaluation" under 10 CFR Part 21 may not be conducted for basic components
- corrective action may not be taken and repetition may not be precluded for issues that do not rise to the level of a significant condition adverse to quality

Description

In 10 CFR Part 21, the NRC defines a deviation to be, in part, a "departure from the technical requirements included in a procurement document." Criterion XVI, "Corrective Action," of Appendix B to 10 CFR Part 50 provides "deficiencies, deviations, defective material and equipment" as examples of conditions adverse to quality. The staff maintains that CFSI meets the definition of deviation. As a deviation, the NRC expects the licensees to evaluate the item and, if necessary, report a substantial safety hazard or failure to comply. Under the regulations (i.e. Part 21, Part 50.5) the NRC has taken enforcement action against entities that supplied counterfeit or fraudulent items that met the safety threshold for reportability.

During the CFSI public meeting held on June 30, 2011, NEI presented their view that CFSI would constitute a deviation under 10 CFR Part 21, a nonconformance under Criterion XV, "Nonconforming Materials, Parts, or Components," of Appendix B to 10 CFR Part 50, and a condition adverse to quality under Criterion XVI of Appendix B to 10 CFR Part 50.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—The safety benefit of addressing this issue was determined to be low because the industry stated that CFSI fall into its 10 CFR Part 21 and corrective action programs as deviations and conditions adverse to quality. However, the NRC staff has never documented its position on the subject.

- Costs—The internal costs of issuing guidance to address this issue are low. The external implementation costs are also low because the industry should not have to change its current process.

Recommendations

The NRC should address this issue by including it in the generic communication as well as by incorporating it into guidance for the ongoing 10 CFR Part 21 rulemaking effort. Section 10.0, Recommendations 3 and 4 capture these actions.

6.3 Issue 11: 10 CFR Part 21 Reporting Responsibility

The current interpretation of 10 CFR Part 21 only applies to basic components (including items that have completed the commercial-grade dedication process) after product acceptance. CFSI identified during receipt inspection and commercial-grade dedication activities may not be evaluated for reportability under 10 CFR Part 21.

Description

The current interpretation of 10 CFR Part 21, specifically the terms “supplied” and “delivery,” creates a transfer of 10 CFR Part 21 evaluation and responsibility between a vendor and customer (the licensee or another vendor). It is common practice that transfer occurs after product acceptance of a basic component. The work group recognizes that the supplying entity may not evaluate CFSI rejected during receipt inspection, especially if the entity is the source of the CFSI.

Additionally, CFSI identified in commercial-grade items that have not completed the dedication process are still considered to be commercial products and are not required to be evaluated or reported under 10 CFR Part 21 even though the dedication process is considered to be a safety-related activity. Commercial-grade items have the highest risk for CFSI.

During the CFSI public meeting held on June 30, 2011, the industry, represented by NEI, stated that, although 10 CFR Part 21 may not be used before product acceptance, the corrective action programs could be used. NEI also informed the NRC staff that INPO requires the report of all CFSI. EPRI stated that its information-sharing initiatives are not limited to the limitations identified by this issue; however, it should be noted that these initiatives are entirely voluntary at this time.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—The safety benefit of addressing this issue was determined to be medium because the items in question have been prevented from being put into use. In the case of rejected basic components containing CFSI, the vendor is responsible for evaluation and reporting of defects in accordance with 10 CFR Part 21. In the case of commercial items, these items must go through a commercial-grade dedication process conducted under an Appendix B to 10 CFR Part 50 quality assurance program before their use in a safety-related application, which would, if the CFSI were detected, prevent their use. However, the benefit to addressing this issue is not considered low because information may not be shared with other entities who may encounter a similar item. Additionally, the INPO and EPRI databases are potential means to communicate this CFSI information.

- Costs—In order to address this issue, the NRC could conduct rulemaking to expand the scope of 10 CFR Part 21 or create a new CFSI reporting rule. The latter may require a change to the NRC's statutory authority. These activities have a high internal cost and would have a moderate-to-high cost to regulated entities. The NRC could work to endorse the industry's voluntary initiatives and issue generic communications. The costs associated with these activities would be low to moderate internally and externally.

Recommendations

The NRC should establish periodic meetings with the industry to formalize the ongoing voluntary information-sharing efforts such as the EPRI CFSI database. Section 10.0, Recommendation 1 captures this action.

6.4 Issue 12: Nonconformance and Corrective Action Programs

Criteria XV and XVI of Appendix B to 10 CFR Part 50 and current guidance do not explicitly require licensees and vendors to enter CFSI occurrences identified during receipt inspection and dedication processes in their nonconformance or corrective action programs.

Description

Criterion XV of Appendix B to 10 CFR Part 50 requires measures to "control materials, parts, or components which do not conform to requirements." As mentioned above (Issue 10), Criterion XVI of Appendix B to 10 CFR Part 50 provides "deficiencies, deviations, defective material and equipment" as examples of conditions adverse to quality. The work group maintains that CFSI fall into these categories; however, the agency has not issued guidance to address this subject.

As mentioned in the discussion about Issue 11 in Section 6.3 above, during the CFSI public meeting on June 30, 2011, the industry, represented by NEI, stated that the nonconformance and corrective action programs could be used before the acceptance of a basic component or the completion of the dedication process.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—The safety benefit of addressing this issue was determined to be low because the industry stated that CFSI fall into nonconformance and corrective action programs as nonconformances and conditions adverse to quality. However, the staff has never documented its position on the subject.

- Costs—The internal costs of issuing guidance to address this issue are low. The external implementation costs are also low because the industry should not have to change its current process.

Recommendations

The NRC should address this issue by incorporating guidance into the ongoing 10 CFR Part 21 rulemaking effort. Section 10.0, Recommendation 4 captures this action.

6.5 Issue 13: CFSI Repository

The NRC staff is unaware of an information repository that licensees and suppliers can refer to during receipt inspection and dedication for examples of confirmed fraudulent items.

Description

The work group noted that one best practice in CFSI prevention is comparing incoming and suspect items to known authentic and known counterfeits during receipt inspection and dedication. These examples can be obtained from past successful procurements, OEMs, other entities covered by Appendix B to 10 CFR Part 50, and NRC generic communications. The work group is unaware of a central information repository that licensee and vendor procurement personnel could use to accomplish this task.

During the CFSI public meeting on June 30, 2011, EPRI informed the NRC staff that it is developing a CFSI database. The EPRI database could contain information to help receipt inspectors. EPRI indicated that it would be willing to work with the NRC to continue to develop the database and promote its use.

Analysis

The task force assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—The safety benefit of addressing this issue was determined to be medium because using known authentic and counterfeit examples is a strong tool to prevent the introduction of CFSI. Although the existing controls under Appendix B to 10 CFR Part 50 already require that entities verify that items conform to the procurement documents and are capable of performing their intended safety function, the implementation of this requirement could be improved.

- Costs—The NRC could work to endorse the industry's voluntary initiatives and issue generic communications. The costs associated with these activities would be low to moderate internally and externally.

Recommendations

The NRC should establish periodic meetings with industry to formalize the ongoing voluntary information-sharing efforts such as the EPRI CFSI database. Recommendation 1 captures this action.

The NRC will continue to issue generic communications or otherwise notify the industry of suspected item trends or confirmed CFSI that the agency is made aware of through the operating and construction experience programs or through the NSIR Threat Assessment Team. Section 10.0, Recommendation 5 captures this action.

6.6 Issue 14: CFSI Information Evaluation and Sharing

The NRC does not have internal guidance or instructions explicitly addressing how the staff evaluates and shares CFSI operating experience information (1) internally to management and affected staff and (2) externally to licensees and vendors; other domestic, Federal, and international agencies; and stakeholders.

Description

The NRC has a high-quality operating experience program documented in Management Directive 8.7, "Reactor Operating Experience Program," dated September 28, 2006, and office-level procedures such as NRR Office Instruction LIC-401, "NRR Reactor Operating Experience Program," dated December 27, 2010, and NRO Office Instruction NRO-REG-112, "New Reactor Construction Experience Program," dated December 31, 2010. These programs gather, screen, and evaluate information from industry and take appropriate action. These programs communicate at each step of the process internally and externally as necessary, such as to the allegations program for further evaluation and appropriate action.

Information relating to CFSI has certain sensitivities that existing guidance does not explicitly address. By definition, CFSI is potentially related to a future, ongoing, or completed wrongdoing allegation or investigation. Suspect item information, by its nature, is unverified and could adversely affect the business of the alleged entity. At the same time, there could be instances in which CFSI information needs to be communicated to affected entities in a timely fashion to prevent its spread into safety-significant applications.

Additionally, the NRC receives information from other domestic Federal and international agencies. Some of this information could clearly impact the domestic power reactor fleet. However, much of the information is vague or unsubstantiated, and it is unclear whether U.S. facilities could be affected. The staff needs a method to screen this information.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—The safety benefit of addressing this issue was determined to be high because of the generic impacts of failure to communicate about CFSI. Although the work group recognized that the NRC has processes in place to communicate operating experience information, these processes could be refined to better handle CFSI information. Also, affected entities have quality programs in place to prevent CFSI introduction, and industry efforts are in progress to share information among industry members, such as the INPO and EPRI databases.

- Costs—The internal costs for revising guidance are low. There are no direct external costs.

Recommendations

The NRC should expand on its current operating experience and construction experience programs by incorporating CFSI information from the commercial nuclear industry, outside industries, and other agencies (domestic and international) that could apply to U.S. commercial nuclear facilities. The agency should revise affected directives and implementing procedures as necessary. Recommendation 7 captures this action. In conjunction with directive and procedure revisions, the NRC should conduct appropriate training on changes and CFSI awareness. Recommendation 6 captures this action.

The NRC should promote information sharing through outreach efforts with appropriate U.S. government and international agencies and revise affected directives and implementing procedures as necessary. Section 10.0, Recommendation 15 captures this action.

6.7 Issue 15: Cause Determinations

Criterion XVI of Appendix B to 10 CFR Part 50 does not require cause determination for conditions adverse to quality.

Description

Criterion XVI of Appendix B to 10 CFR Part 50 requires that the cause of the condition be determined and corrective action taken to preclude repetition for significant conditions adverse to quality. For nonsignificant conditions adverse to quality, the condition only need be corrected. The work group noted from experience that only a small percentage of conditions rise to the level of "significant" at a licensee or vendor facility. The potential exists that CFSI may go undetected as a causal factor associated with a rejected item or an equipment failure without sufficient CFSI training and causal analyses.

During the CFSI public meeting on June 30, 2011, the industry, represented by NEI, noted that, although root cause analyses are not frequently performed, apparent cause analyses are performed more frequently. NEI also noted that these causal analyses are not necessarily limited to safety-related components and equipment. Additionally, licensees have trending programs that have the potential to identify CFSI trends.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—The safety benefit of addressing this issue was determined to be low because other portions of the quality assurance program prevent the introduction of CFSI. In addition, the industry in some cases exceeds the requirements of Criterion XVI by conducting apparent or root cause analyses or both on conditions adverse to quality that are not determined to be significant.

- Costs—The internal costs associated with promoting training and awareness are low. The staff can discuss these issues at regularly held and attended conferences such at the NRC vendor workshop led by NRO, Nuclear Utility Procurement Issues Committee meetings, and EPRI Joint Utility Task Force meetings.

  The external costs are low to medium depending on the extent of training developed and implemented by licensees and vendors. The costs associated with instituting a new CFSI rule on the other hand, are significantly greater for both the NRC and the industry. The need for a new rule at this time was not evident, given the existing quality programs currently in place, and in recognition of the fact that there have been no recent reports of a counterfeit or fraudulent item being installed into a safety related application.

Recommendations

The NRC can encourage more training and awareness for the industry to be aware of CFSI during procurement activities and to evaluate component failures for CFSI. The NRC should encourage industry awareness of inspection techniques for complex components. External industry centers of excellence may be sources of educational content, particularly for inspection techniques for complex components. The collective efforts of the U.S. Government's Anti-Counterfeiting Working Group (via the Intellectual Property Enforcement Coordinator (IPEC)) would also be a likely source of educational subject matter. The NRC should periodically benchmark developments in CFSI for consideration for future implementation. Section 10.0, Recommendation 2 captures these actions.

7.0 RESPONSE PROTOCOLS WORKING GROUP

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. This group discussed the following topics:

- actions necessary to effectively engage the agency in communicating, inspecting, and possibly investigating CFSI at NRC-regulated activities
- the various internal organizations that would need to be engaged
- Federal agencies that should be notified for prosecuting those engaged in knowingly trafficking in CFSI
- jurisdictional limitations when foreign suppliers are used
- response protocols involving foreign suppliers

7.1 Issue 16: Lack of Response Guidance for the NRC Staff

The NRC currently has no staff guidance for agency actions when a licensee, supplier, distributor, or manufacturer identifies CFSI and the NRC becomes aware of it.

Description

The regulations in 10 CFR 40.10, 50.5, 70.10, 71.8, 76.10, 72.12, 52.4, and 110.7b discuss deliberate misconduct as it applies to NRC-regulated activities. The NRC staff receives allegation training. Although deliberate misconduct, which is implied by CFSI, should be treated as an allegation, use of the allegation process is not intuitive with CFSI. The NRC staff has experience that demonstrates that some staff members are uncertain about how information regarding a CFSI should be treated.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—Licensees or vendors have identified safety-related components; therefore, the safety benefit of addressing this issue is medium. Deliberate misconduct and the need to establish the trustworthiness of the suppliers of safety-related components elevate the significance.
- Costs—Use of the current NRC allegations process has a low cost since the program is in place and adequately addresses CFSI. No direct external costs are associated with addressing this issue.

Recommendations

The NRC should provide clear guidance on the treatment of CFSI information in the current NRC allegation process, if CFSI cannot be reported to the NRC using the existing methods of reporting. The agency should include specific examples of processing a CFSI-related allegation in training. It should provide periodic training to keep inspectors mindful of the potential for CFSI. Section 10.0, Recommendation 6 captures this action.

7.2 Issue 17: Quarantine of CFSI

The NRC has no requirement for a licensee facility or vendor to quarantine suspected CFSI materials for further analysis, regulatory, or law enforcement purposes.

Description

When a licensee or vendor identifies CFSI, it is expected to enter the item into a nonconformance or corrective action program. Once done, the licensee or vendor only has to prevent use of the item to comply with regulations. The item could be returned to the supplier, who could also be the counterfeiter or trafficker of CFSI. If returned, the item could reenter the supply chain and be sold to an unsuspecting vendor or licensee who may be less capable of identifying CFSI than the licensee or vendor who first identified the item as CFSI. Quarantining a suspected item prevents the item from reentering the supply chain and allows the item to be inspected or investigated and used as evidence by law enforcement. OI has the authority request that a licensee quarantine and surrender custody of safety-related CFSI for the purpose of investigations.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—Quarantining CFSI has three effects: (1) it removes a suspect item from possible use, (2) it prevents it from reentering the supply chain, and (3) it provides a basis to document and collect evidence to support further enforcement and legal actions. Therefore, the safety benefit of addressing this issue was determined to be medium.

- Costs—The costs to stakeholders depend on the cost of the specific component and occur when a licensee or vendor is unable to return the component for credit or a replacement part. Nonetheless, such costs are expected to be low to moderate. Industry practices exist that can alleviate the cost, such as using a third-party escrow for major purchases, in which the terms of payment would include receipt of a component of proper quality that does not contain CFSI.

Recommendations

The NRC should issue generic communications that share proactive industry strategies, including the practice of quarantine. Periodic meetings with industry leaders would allow the NRC staff to share information and to encourage their use of best practices. Section 10.0, Recommendation 3 captures this action.

7.3 Issue 18: Lack of NRC Inspections of Procurement and Dedication

The NRC does not currently perform routine procurement, commercial-grade dedication, or 10 CFR Part 21 inspections at operating power plants to ensure that licensees are adequately screening for CFSI during receipt inspection and commercial-grade dedication activities.

Description

Often, licensees identify CFSI upon receipt inspection or while dedicating a commercial-grade item for safety-related use. CFSI practices are not routinely inspected in the Reactor Oversight Process (ROP). Given that the endpoint for all safety-related components is at the licensees' facilities, NRC inspections of licensees' procurement activities could be more comprehensive.

The NRC does not specifically inspect the licensees anti-CFSI measures at their facilities, although it does review 10 CFR Part 21 reports involving the site during problem identification and resolution inspections. As such, these inspections are not of the licensee's program to evaluate CFSI but instead focus primarily on how the licensee has responded to 10 CFR Part 21 reports (i.e., issuing corrective actions). OIG also noted the lack of 10 CFR Part 21 inspections as a weakness in its recent audit of the NRR 10 CFR Part 21 program (see OIG-11-A-08).

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—The safety benefit of addressing this issue was determined to be medium to high because the agency has little information about how effectively licensees are handling CFSI during receipt inspections and commercial-grade dedication.

- Costs—The internal costs to address this issue would be high. The agency would need to write or revise inspection procedures, adjust the ROP, and train inspectors before implementation. During implementation, resources would be needed for inspectors to plan, conduct, and report inspections. Implementation costs may be fee billable.

Recommendations

The NRC should develop 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. Afterwards, the agency should determine whether to incorporate similar inspections into the ROP permanently. Section 10.0, Recommendation 8 captures this action.

7.4 Issue 19: Lack of CFSI Discussion in Inspection Guidance

NRC inspection guidance does not specifically address CFSI or direct NRC inspectors to look at a vendor's or licensee's program for detecting and preventing CFSI.

Description

With the exception of Inspection Procedure 43002, "Routine Inspections of Nuclear Vendors," which mentions fraudulent parts as examples of what else to look for in reviewing nonconformances, NRC inspection procedures or inspection guidance documents do not mention CFSI. The NRC has no guidance to inspect a licensee's or vendor's program for the presence of an adequate CFSI program.

Analysis

The work group assessed the stated issue against each of the following predetermined assessment factors.

- Safety Benefit—NRC inspectors already look at vendor and licensee programs for nonconformance, deviations, deficiencies, failures, malfunctions, and defective material and equipment. Therefore, the safety benefit of addressing this issue is low.

- Costs—The NRC would need to make minor changes to inspection procedures and inspector training; the cost would be low. The cost for the training would be slightly higher than procedural changes but still kept relatively low. Costs to licensees and vendors are negligible.

Recommendations

The NRC should clarify guidance in agency inspection procedures to include an awareness of CFSI and assess prevention measures at licensee and vendor facilities. Inspectors should continue to relate findings to regulations, such as the quality assurance requirements in Appendix B to 10 CFR Part 50. The agency should develop training for NRC inspectors to increase their awareness of CFSI and industry practices to address CFSI. Section 10.0, Recommendations 9 and 10 capture these actions.

7.5 Issue 20: Lack of NRC Jurisdiction beyond U.S. Borders

NRC inspectors and investigators lack jurisdictional authority outside the United States, which can limit the NRC's ability to take action against suppliers of CFSI outside U.S. borders.

Description

It can be difficult for NRC inspectors and NRC OI agents to inspect, investigate, and enforce requirements related to counterfeit or fraudulent parts provided by a supplier located solely in a foreign country. OI has available for its use, various law enforcement techniques which may be employed through the criminal investigation process. This will be coordinated with DOJ in compliance with applicable treaties and agreements. These processes are not necessarily straightforward in every case.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—The safety benefit of addressing this issue was determined to be low because the NRC can order licensees and vendors not to use that foreign supplier.

- Costs—Revising jurisdictional authorities would require a statutory change involving signing of a treaty or international agreement, which would be costly to the NRC and to the Federal Government as a whole for all of the work required. The NRC has fairly low-cost options, such as generic communications and orders, to prevent foreign CFSI from affecting U.S. plants. External costs would depend on the availability of components from other vendors if the foreign vendor was using CFSI and the NRC gave a licensee or vendor an order not to use that vendor.

Recommendations

The NRC should promote international information sharing in order to leverage other countries' regulators to assist in limiting CFSI in the supply chain for everyone's best interest. The NRC should use the Committee on Nuclear Regulatory Activities' Multinational Design Evaluation Program pilot program for CFSI, which is already under discussion at the international level. Also, the NRC should work with other Federal agencies on a case-by-case basis as needed to assist in dealing with foreign wrongdoers. Section 10.0, Recommendations 7 and 15 capture these actions.

8.0 CYBER SECURITY SUPPLY CHAIN OVERSIGHT WORKING GROUP

This working group focused on regulations, guidance, and industry practices for oversight of cyber security as they relate to supply chain oversight of critical digital assets (CDAs). Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," provides a framework to aid in the identification of those digital assets that must be protected from cyber attacks (i.e., CDAs). Currently, NSIR oversees cyber security policy, guidance, and licensing activities for NRC licensees. 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 between NRO and NSIR is necessary to address cyber threats. Representatives from both 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. Specifically, the working group identified four issues in the cyber security supply chain. Below is a summary of each issue, a brief summary of the current regulatory structure, the issue analysis, and detailed recommendations.

8.1 Issue 21: Guidance on Cyber Security

NRC inspection guidance is needed to instruct inspectors on how suppliers of CDAs within the scope of 10 CFR 73.54 should be implementing the System and Service Acquisition security controls that maintain the integrity and security of the acquired systems.

Description

In 10 CFR 73.54, the NRC requires that each licensee and license applicant for a nuclear power plant to submit a cyber security plan that provides high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. Regulatory Guide 5.71 provides an acceptable approach for licensees and applicants to comply with the above requirement.

The NRC has regulatory authority to inspect suppliers of basic components under 10 CFR Part 21, including suppliers of safety-related CDAs. The NRC performs such inspections on a sampling basis using Inspection Procedure 43002. Although the inspection procedure gives guidance about inspecting supplier quality assurance programs to verify compliance with Appendix B to 10 CFR Part 50 and 10 CFR Part 21, the inspection procedure does not contain guidance associated with how to inspect the specific aspects of supplier programs relevant to the high assurance controls passed down from the licensees' cyber security plans.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit— When safety-related CDAs are compromised, consequences could result that challenge the protection of digital computer and communication systems and networks. Licensees and suppliers have policies and/or programs in place to ensure CDAs are not compromised at the supplier level and licensees are required to have defense-in-depth in their operational programs (73.54(b)(2)) to respond and recover from cyber attacks.

Ineffective controls at suppliers of CDAs could open up pathways for malicious code to reach licensees that would be difficult, if not impossible, to detect through licensee operational programs. Without specific inspection guidance, NRC inspectors may not have detailed knowledge of the actual processes that need to be in place and inspected in order to provide high assurance that safety-related CDAs are adequately protected against cyber attacks. Therefore, the safety significance is determined to be medium.

- Costs—The NRC would have to develop guidance for inspectors to use. Such guidance could either be put into a new inspection procedure or into existing procedures. The costs of developing and issuing such guidance would likely be low to medium.

Recommendations

The NRC should develop inspection guidance that is focused on vendor inspections for suppliers of safety-related CDAs. This procedure should include guidance on how to inspect the Service and System Acquisition security controls contained in licensee cyber security plans. The agency should implement the inspection procedure on a sample basis in accordance with the NRC's overall prioritization scheme for conducting vendor inspections. In addition, the industry and NRC staff are working together to ensure that guidance is available to appropriately implement System and Services Acquisition security controls to ensure that CDAs are adequately protected. Recommendations 11 and 12 capture these actions.

8.2 Issue 22: Inspection Authority over Suppliers of Critical Digital Assets

Although the NRC has the authority needed to inspect licensees and applicants for implementation of the cyber security rule, the NRC has no direct inspection authority in accordance with 10 CFR Part 21 to inspect suppliers for cyber security controls passed down to them for CDAs beyond those that are basic components.

Description

The regulation in 10 CFR 73.54(a)(1) requires a licensee to protect, with high assurance, digital computer and communications systems and networks associated with safety-related, important-to-safety, security, and emergency preparedness functions, including offsite communications, and support systems and equipment that, if compromised, would adversely impact safety, security, or emergency preparedness functions. Licensee cyber security plans implemented cyber security controls comparable to those outlined in Regulatory Guide 5.71 and refer to digital assets that must be protected from cyber attacks as CDAs.

The cyber security rule requires the protection of such systems and networks from those cyber attacks that would act to modify, destroy, or compromise the integrity or confidentiality of data or software; deny access to systems, services, or data; and impact the operation of systems, networks, and equipment. In SECY-10-0153, "Cyber Security—Implementation of the Commission's Determination of Systems and Equipment within the Scope of Title 10 of the *Code of Federal Regulations*, Section 73.54," dated November 19, 2010, the staff further explained that "important to safety" would generally include any balance of plant (e.g., nonsafety-related) equipment that directly or indirectly could affect the reactivity of a nuclear power plant. This would include equipment out to the first intertie with the offsite distribution system. Regulatory Guide 5.71 provides an acceptable approach for complying with the required high assurance of adequate protection for CDAs.

Regulatory Position C.3.3.3.1, "System and Service Acquisition," of Regulatory Guide 5.71 describes what would be considered an acceptable approach to system and service acquisition controls, including controls to be imposed on suppliers of CDAs. Section C.12, "System and Service Acquisition," of Appendix C to Regulatory Guide 5.71 discusses controls, including development of testing programs to ensure that products are free from malicious code, establishment of trusted distribution paths, and the qualification of tools used in the development of digital instrumentation and control systems.
Although 10 CFR Part 21.41, "Inspections," gives NRC inspectors authority at suppliers of safety-related equipment, the authority is applicable only to suppliers of basic components as defined in 10 CFR 21.2, "Scope." The NRC lacks inspection authority at suppliers of CDAs that are not being procured as basic components. Although licensees will impose and credit controls on suppliers of all CDAs to ensure adequate protection, the NRC lacks authority to verify that such controls are properly implemented at the supplier level for CDAs not being procured as basic components.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—Only items that are not supplied as basic components are affected. Failure of CDAs whose functions and systems are not safety-related could cause a challenge to the plant that could require activation of safety systems. Nonetheless, direct NRC inspections, as such, would result in an insignificant change in the current rate of such challenges. Even without NRC inspection authority at suppliers of CDAs whose functions and systems are not safety related and procured as basic components, licensees would have rights to inspect under their commercial purchase contracts that are sufficient to ensure adequate supplier controls. The NRC has authority under 10 CFR 73.54(f) to inspect licensees' implementation of cyber security program elements in accordance with the licensees' approved cyber security plans. Therefore, the safety benefit of addressing this issue was determined to be low.

- Costs—The NRC would have to institute rulemaking to modify inspection authorization requirements. Such an effort would require extensive internal resources. Once such a rule was passed, the NRC would have to implement inspections at suppliers of equipment not procured as basic components. This would result in high costs to the NRC, licensees, and other stakeholders.

Recommendations

The work group recommends no immediate regulatory actions to modify inspection authority. Through NRC inspections of licensees and applicants, the staff will evaluate the adequacy of licensee efforts to ensure that the appropriate supplier controls passed down to suppliers of all CDAs are, in fact, properly implemented. The NRC should discuss initiatives with the industry such as promoting contractual provisions that permit NRC inspection at suppliers of CDAs. The NRC staff will perform inspections at suppliers of safety-related CDAs. The agency should use the results of the inspections, along with those of industry initiatives, to determine the need for seeking changes to the regulations. Section 10.0, Recommendations 13 and 14 capture these actions.

8.3 Issue 23: Inspection Guidance for Cyber Security Programs with Respect to Supplier Controls

The NRC has not developed specific inspection guidance for use by agency inspectors to evaluate the adequacy of licensee cyber security programs with respect to supplier controls.

Description

In 10 CFR 73.54, the NRC requires that each licensee and license applicant for a nuclear power plant submit to the NRC a cyber security plan that provides for the protection of safety-related, important-to-safety, security, and emergency preparedness functions. The rule requires protection against cyber attacks that would act to modify, destroy, or compromise the integrity or confidentiality of data or software; deny access to systems services or data; and impact the operation of systems, networks, and equipment.

The regulation in 10 CFR 73.54(f) requires that licensees develop and maintain written policies and procedures to implement the cyber security plan. Licensees need not submit policies, implementing procedures, site-specific analysis, and other supporting technical information that it uses to the agency for Commission review and approval as part of the cyber security plan, but this information is subject to inspection by NRC staff on a periodic basis.

Regulatory Guide 5.71 provides an approach that the NRC staff has deemed acceptable for complying with the above requirements. Regulatory Position C.3.3.3.1 of Regulatory Guide 5.71 provides guidance on an acceptable approach to system and service acquisition controls, including controls to be imposed on suppliers of CDA equipment. Section C.12 of Appendix C to the regulatory guide details these controls, including the development of testing programs to ensure that products are free from malicious code, the establishment of trusted distribution paths, and the qualification of tools used in the development of digital instrumentation and control systems.

Because of the recent implementation of these requirements, the NRC has not fully developed inspection guidance to evaluate the adequacy of licensee cyber security programs with respect to supplier controls.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—Without specific inspection guidance, NRC inspectors will not have clear direction about how to consistently verify the adequacy of supplier controls in licensee cyber security programs. Ineffective controls at suppliers of CDAs could open up pathways for malicious code to reach licensees that would be difficult, if not impossible, to detect though licensee operational programs. A compromise of such safety-related CDAs could result in safety-significant consequences to the power plant. Therefore, the safety benefit of addressing this issue was determined to be medium.

- Costs—The NRC would have to develop guidance for inspectors in new inspection procedures or as part of existing procedures. The cost of developing and issuing such guidance would likely be low to medium.

Recommendations

NSIR should continue to develop and implement an inspection procedure focused on the licensee's implementation of its cyber security program. This procedure should include guidance on inspecting the System and Services Acquisition security controls, such as the contractual provisions contained in procurement documents, trusted distribution paths, validation of suppliers, and any additional controls included in the licensee cyber security plan. In addition, NSIR is developing detailed guidance on controls that the cyber security plan should address. Recommendations 12 and 16 capture these actions.

8.4 Issue 24: Treatment of Critical Digital Assets

The NRC has not completed development of additional guidance on how licensees and applicants should, from a quality assurance perspective, treat non-safety related CDAs to establish, maintain, and successfully integrate the security controls required to be addressed in the cyber security plan.

Description

Appendix B to 10 CFR Part 50 applies to all activities affecting the safety-related functions of SSCs to ensure safe operation. These quality assurance criteria include design control, traceability, shipping, and inspection to ensure control of the quality of the material, structure, component, or system to predetermined requirements.

The regulation in 10 CFR 73.54(a)(1) requires the licensee to protect digital computer and communications systems and networks associated with safety-related, important-to-safety, security, and emergency preparedness functions, including offsite communications, and support systems and equipment that, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Regulatory Guide 5.71 contains a cyber security plan template and provides an approach that the NRC staff has deemed acceptable for complying with the above requirements. Section A.4, "Maintaining the Cyber Security Program," of Appendix A to Regulatory Guide 5.71 establishes the programmatic elements necessary to maintain security throughout the life cycle of CDAs.

Many industry guidance documents establish and implement quality assurance programs for nuclear facility applications, including the American National Standards Institute (ANSI)/American Society of Mechanical Engineers (ASME) N45.2-series standards and the ANSI/ASME NQA-1 standards; the NRC has approved these specific standards, in part, in regulatory guides. However, the NRC does not have specific guidance on how to treat, from a quality assurance perspective, CDAs, especially CDAs that are not safety-related and therefore do not fall under the quality assurance criteria in Appendix B to 10 CFR Part 50. Consequently, although licensees will impose and credit a programmatic approach to deal with the potential cyber risks to CDAs, no widely accepted guidance is available on what program is sufficient.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—Currently, licensees must submit for NRC review and approval a cyber security plan that satisfies the requirements for high assurance and adequate protection of CDAs. Even without additional guidance on how to address this issue, licensees would have to develop a program to meet the commitments of their cyber security plans and the requirements in 10 CFR 73.54 with respect to the treatment of CDAs and their protection against cyber attacks. Therefore, the safety benefit of addressing this issue was determined to be low.

- Costs—The NRC would need to develop guidance to specifically address CDAs from a quality assurance perspective and to address controls to protect against cyber attacks; the cost to the NRC and the industry would be moderate. Additional guidance could potentially lessen the burden to individual licensees by creating a widely accepted programmatic approach to meet the requirements of 10 CFR 73.54 and commitments to licensee cyber security plans for CDAs.

Recommendations

The work group recommends no immediate NRC action. Licensees are required to meet 10 CFR 73.54 and their cyber security plans that include provisions that assure the application of appropriate security controls. If the agency identifies deficiencies during the periodic inspections, additional NRC and industry guidance may be needed. Section 10.0, Recommendations 12 and 16 capture these actions.

Analysis

The work group assessed this issue against each of the following predetermined assessment factors.

- Safety Benefit—Currently, licensees must submit for NRC review and approval a cyber security plan that satisfies the requirements for high assurance and adequate protection of CDAs. Even without additional guidance on how to address this issue, licensees would have to develop a program to meet the commitments of their cyber security plans and the requirements in 10 CFR 73.54 with respect to the treatment of CDAs and their protection against cyber attacks. Therefore, the safety benefit of addressing this issue was determined to be low.

- Costs—The NRC would need to develop guidance to specifically address CDAs from a quality assurance perspective and to address controls to protect against cyber attacks; the cost to the NRC and the industry would be moderate. Additional guidance could potentially lessen the burden to individual licensees by creating a widely accepted programmatic approach to meet the requirements of 10 CFR 73.54 and commitments to licensee cyber security plans for CDAs.

Recommendations

The work group recommends no immediate NRC action. Licensees are required to meet 10 CFR 73.54 and their cyber security plans that include provisions that assure the application of appropriate security controls. If the agency identifies deficiencies during the periodic inspections, additional NRC and industry guidance may be needed. Section 10.0, Recommendations 12 and 16 capture these actions.

ADAMS Accession No.: ML112130293

OFFICE	NRO/DCIP/CQVB	NRO/DCIP/CQVB	NRO/DCIP	OIP	OE
NAME	DPasquale	RRasmussen	LDudes	MDoane	RZimmerman
DATE	9/15/11	9/20 /11	9/ 23/11	10/03/2011	10/12/2011
OFFICE	FSME	NMSS	OI	NSIR	NRR
NAME	CCarpenter	CHaney	CMcCrary	JWiggins	ELeeds
DATE	09/27/2011	10/13/2011	10/05/2011	10/17/2011	10/12/2011
OFFICE	QTE	OGC			
NAME	*JDougherty	SBurns			
DATE	09/06/2011	10/18/2011			

OFFICIAL RECORD COPY

9.0 ISSUES TABLE

ISSUE No. [1]	DESCRIPTION	IDENTIFYING WORKING GROUP
Issue 1	The NRC currently has no regulatory guidance or requirements for the authentication and testing of components necessary to identify a counterfeit or fraudulently identified item.	Supply Chain Oversight Working Group
Recommendation(s)	2, 3	
Issue 2	The NRC has no guidance that specifically addresses the need for licensees or suppliers to implement programs to identify fraudulent documentation.	Supply Chain Oversight Working Group
Recommendation(s)	3	
Issue 3	Current NRC requirements do not mandate that licensees pass down contractual requirements for supplier CFSI programs to identify and eliminate fraudulent goods obtained from subsuppliers.	Supply Chain Oversight Working Group
Recommendation(s)	2, 3	
Issue 4	The NRC currently has no regulatory guidance for implementing measures to prevent CFSI associated with the regulatory treatment of nonsafety systems (RTNSS).	Supply Chain Oversight Working Group
Recommendation(s)	2	
Issue 5	The NRC does not have regulatory requirements associated with preventing CFSI in the procurement of nonsafety-related critical infrastructure equipment.	Supply Chain Oversight Working Group
Recommendation(s)	1	
Issue 6	The NRC has no regulations or guidance documents that define explicit controls for the prevention of CFSI in the procurement of NRC-regulated, nonreactor items (e.g., IROFS, SSCs important to safety).	Supply Chain Oversight Working Group
Recommendation(s)	18, 19	
Issue 7	The NRC has no regulatory requirements specifically targeted at preventing, detecting, or communicating incidences of CFSI at fuel cycle facilities and in spent fuel storage and radioactive material transportation activities.	Supply Chain Oversight Working Group
Recommendation(s)	18, 19	

ISSUE No. [1]	DESCRIPTION	IDENTIFYING WORKING GROUP
Issue 8	The NRC has no regulations or guidance documents that define explicit controls for the prevention of CFSI in the procurement of NRC-regulated medical and industrial items.	Supply Chain Oversight Working Group
Recommendation(s)	17, 19	
Issue 9	Current reporting requirements only mandate the reporting of defects and failures to comply that could lead to a substantial safety hazard and significant events driven by equipment failures. Basic components that are determined to be CFSI but do not constitute a substantial safety hazard or cause a reportable event would not be required to be reported.	Communication Working Group
Recommendation(s)	1, 4	
Issue 10	There is lack of clarity about whether CFSI constitutes a deviation, failure to comply, or condition adverse to quality as defined in existing rules and guidance: (1) evaluation under 10 CFR Part 21 may not be conducted for basic components (2) corrective action may not be taken and repetition may not be precluded for issues that do not rise to the level of a significant condition adverse to quality (SCAQ)	Communication Working Group
Recommendation(s)	3, 4	
Issue 11	The current interpretation of 10 CFR Part 21 only applies to basic components (including items that have completed the commercial-grade dedication process) after product acceptance. CFSI identified during receipt inspection and commercial-grade dedication activities may not be evaluated for reportability under 10 CFR Part 21.	Communication Working Group
Recommendation(s)	1	
Issue 12	Criteria XV and XVI of Appendix B to 10 CFR Part 50 and current guidance do not explicitly require licensees and vendors to enter CFSI occurrences identified during receipt inspection and dedication processes in their nonconformance or corrective action programs.	Communication Working Group
Recommendation(s)	4	

ISSUE No. [1]	DESCRIPTION	IDENTIFYING WORKING GROUP
Issue 13	The NRC staff is unaware of an information repository that licensees and suppliers can refer to during receipt inspection and dedication for examples of confirmed fraudulent items.	Communication Working Group
Recommendation(s)	1, 5	
Issue 14	The NRC does not have internal guidance or instructions explicitly addressing how the staff evaluates and shares CFSI operating experience information (1) internally to management and affected staff and (2) externally to licensees and vendors; other domestic, Federal, and international agencies; and stakeholders.	Communication Working Group
Recommendation(s)	6, 7, 15	
Issue 15	Criterion XVI of Appendix B to 10 CFR Part 50 does not require cause determination for conditions adverse to quality.	Communication Working Group
Recommendation(s)	2	
Issue 16	The current staff guidance is not explicit for including CFSI into the allegations process as a potential wrongdoing activity. Once documented in the allegations system, the procedures governing the roles and responsibilities will dictate a defined and orderly execution of the appropriate events needed to appropriately disposition the issue.	Response Protocols Working Group
Recommendation(s)	6	
Issue 17	The NRC has no requirement for a licensee facility or vendor to quarantine suspected CFSI materials for further analysis, regulatory, or law enforcement purposes.	Response Protocols Working Group
Recommendation(s)	3	
Issue 18	The NRC does not currently perform procurement, commercial-grade dedication, or 10 CFR Part 21 inspections at operating power plants to ensure that licensees are adequately screening for CFSI during receipt inspection and commercial-grade dedication activities.	Response Protocols Working Group
Recommendation(s)	8	

ISSUE No. (1)	DESCRIPTION	IDENTIFYING WORKING GROUP
Issue 19 Recommendation(s)	NRC inspection guidance does not specifically address CFSI or direct NRC inspectors to look at a vendor's or licensee's program for detecting and preventing CFSI. 9, 10	Response Protocols Working Group
Issue 20 Recommendation(s)	NRC inspectors and investigators lack jurisdictional authority outside the United States, which can limit the NRC's ability to take action against suppliers of CFSI outside U.S. borders. 7, 15	Response Protocols Working Group
Issue 21 Recommendation(s)	Both NRC inspection guidance and industry guidance are needed to address how suppliers of CDAs, and the systems and functions required to be addressed in the cyber security plan, implement the supplier controls that maintain the integrity and security of the acquired systems. 11, 12	Cyber Security Supply Chain Oversight Working Group
Issue 22 Recommendation(s)	The NRC has no direct inspection authority for cyber security controls passed down to suppliers of CDAs that are not supplied as basic components, or for the systems and functions required to be addressed in the cyber security plan. 13, 14	Cyber Security Supply Chain Oversight Working Group
Issue 23 Recommendation(s)	The NRC has not developed specific inspection guidance for use by agency inspectors to evaluate the adequacy of licensee cyber security programs with respect to supplier controls. 12, 16	Cyber Security Supply Chain Oversight Working Group
Issue 24 Recommendation(s)	The NRC has not completed additonal guidance on how licensees and applicants programmatically treat CDAs to establish, maintain, and successfully integrate the security controls required to be addressed in the cyber security plan. 12, 16	Cyber Security Supply Chain Oversight Working Group
Note: (1)	A single recommendation may be used to resolve multiple issues.	

10.0 RECOMMENDATION TABLE

No. [1]	PLANNED ACTION	ISSUE	TIME TO IMPLEMENT	OFFICE
1.	Establish periodic meetings between the NRC and industry 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 focus of these meetings will include discussions of the following: • sharing CFSI information, including issues identified during receipt inspection and during commercial-grade dedication • using the corrective action programs and nonconformance programs for entering CFSI related to safety-related components • entering all CFSI (including nonsafety related) into the corrective action program • using operating experience that has been discovered through expansion of the NRC operating experience program to capture CFSI that could affect the U.S. nuclear fleet • alignment with ASME NQA-1 CFSI initiatives • establish an industry CFSI database (INPO and EPRI databases in development)	5, 9, 11, 13	6 mo	NRO, NRR, NMSS
2.	Communicate with industry via the NRC's existing generic communications program about any potential CFSI training or applicable informational sources that could increase awareness of CFSI. This information will be useful during procurement activities to better assess component failures for possible CFSI intrusion and for evolving inspection techniques for complex components. External industry centers of excellence may be sources of educational content, particularly for inspection techniques for complex components. A likely source for educational subject matter is the collective efforts of the U.S. Government's Anti-Counterfeiting Working Group (via IPEC). The NRC should periodically benchmark developments in CFSI for consideration for future implementation.	1, 3, 4, 15	Continuous	NRO, NRR

No. [1]	PLANNED ACTION	ISSUE	TIME TO IMPLEMENT	OFFICE
3.	Issue generic communications to inform industry of any best practices related to proactive industry strategies, such as the following: • Quarantine CFSI items or remove them from the supply chain and NOT return them to the supplier. • Inform the industry of CFSI trends. • Promote enhanced commercial-grade dedication, and receipt inspection practices. • Give authentication guidance to provide more assurance in preventing CFSI. • Consider the use of batch sampling for authentication testing. • Promote the industry's use of standardized anti-CFSI language in procurement documents.	1, 2, 3, 10, 17	1 yr	NRO, NRR, NMSS
4.	Coordinate with the 10 CFR Part 21 rulemaking team to provide guidance for specifically defining CFSI as a deviation that requires evaluation under 10 CFR Part 21 and a condition adverse to quality under Criterion XVI of Appendix B to 10 CFR Part 50.	9, 10, 12		NRO, NRR
5.	Continue to issue generic communications or otherwise to notify the industry of suspected item trends or confirmed CFSI that the NRC identifies through the operating and construction experience programs or through the NSIR Threat Information Assessment Team.	13	Continuous	NRO, NRR, NSIR, NMSS
6.	Provide clear guidance through the NRC's allegations training module for using the allegation process when a licensee, a supplier, or an NRC staff member identifies CFSI.	14, 16	1 yr	OE, NRO, NRR
7.	Expand on the current NRC operating experience and construction experience programs by incorporating CFSI information from appropriate sources (domestic and international) and related industry organizations that could apply to U.S. commercial nuclear facilities.	14, 20	1 yr	NRO, NRR, NMSS, OI, OIP
8.	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 ROP.	18	FY 2012	NRR, NRO

No. [1]	PLANNED ACTION	ISSUE	TIME TO IMPLEMENT	OFFICE
9.	Evaluate the need to provide additional guidance in NRC inspection procedures to inspect for CFSI identification and prevention processes at all affected licensees' facilities pertaining to NRC-regulated activities, including the following: • licensee facilities • supplier inspections • Quality and Vendor Branch third-party observations	19	IAW routine procedure updates to be completed in 3 yr	NRO, NRR, NSIR, NMSS
10.	Develop training for NRC inspectors to assist them in inspecting and to increase their awareness of CFSI and effective industry identification and detection practices.	19	1 yr	NRO, HR
11.	Develop a new inspection procedure focused on suppliers of safety-related CDAs contained in the cyber security plan.	21	1 yr	NRO, NRR, NSIR
12.	The NRC has approved implementation schedules for each site to be in compliance with commitments and regulations for the cyber security rule. The results of NSIR's cyber security plan inspections will be evaluated to determine the need to address further controls to address the treatment of CDAs that are not safety related.	21, 23, 24	TBD	NSIR, NRO
13.	The licensees committed to inspect suppliers as part of their cyber security plan. If issues arise, the NRC has inspection authority over the licensees (under 10 CFR 73.54(f)).	22	Continuous	NSIR, NRO, NRR
14.	Conduct NRC vendor inspections at suppliers of safety-related CDAs. Evaluate the results of these inspections to determine the need to expand the inspection sample to suppliers and subsuppliers of nonsafety-related CDAs.	22	In support of licensee procurement schedules	NRO, NRR, NSIR
15.	Promote information sharing through outreach efforts with appropriate U.S. government and international agencies. Revise affected directives and implementing procedures as necessary.	14, 20	Ongoing	NRO, NRR, IP, OI
16.	Continue NSIR development of a temporary instruction to inspect/verify licensee's implementation of its cyber security program, including commitments for supplier oversight. NSIR has issued Regulatory	23, 24	1 yr	NSIR, NRO, NRR

No. (1)	PLANNED ACTION	ISSUE	TIME TO IMPLEMENT	OFFICE
	Guide 5.71 as an acceptable approach for licensees to meet the cyber security rule requirements.			
17.	Continue to periodically inspect licensees and work with the Agreement States and the FDA. Perform an agencywide reassessment in the future to determine if any additional effort is needed.	8	Ongoing	FSME
18.	Continue with existing NRC fuel cycle facility oversight programs and spent fuel storage and radioactive material transportation activities, which include QA controls such as management measures that can contribute to the identification and prevention of CSFI. NRC will continue to inspect these facilities periodically, include the issue in a generic communication that also addresses other issues identified in the CFSI working groups, and monitor CFSI activities such as periodic meetings, to integrate as necessary.	6, 7	Ongoing	NMSS
19.	Perform an agencywide reassessment to determine the effectiveness of the implemented measures and pilot programs and to determine the need to implement additional CFSI countermeasures.	All	FY 2014	NRO, NRR, NSIR, NMSS, FSME
Note (1)	A single recommendation may be used to resolve multiple issues.			

11.0 CFSI WORKING GROUP DIAGRAM