June 9, 2015

MEMORANDUM TO: Brian Anderson, Branch Chief
ITAAC and Generic Communication Branch
Division of Construction Inspection
and Operational Programs
Office of New Reactors

FROM: James Gaslevic, Reactor Operations Engineer ***/RA/***
ITAAC and Generic Communication Branch
Division of Construction Inspection
and Operational Programs
Office of New Reactors

SUBJECT: RESPONSE TO PUBLIC COMMENTS ON DRAFT REGULATORY ISSUE SUMMARY 2014-XX, "OVERSIGHT OF COUNTERFEIT, FRAUDULENT, AND SUSPECT ITEMS IN THE NUCLEAR INDUSTRY"

A notice of opportunity for public comment on the subject regulatory issue summary was published in the *Federal Register* (79 FR 59521) on October 2, 2014. Comments were received from the University of Florida (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14297A154), Roger Johnston (ADAMS Accession No. ML14309A247), the Nuclear Energy Institute (ADAMS Accession No. ML14311A039), Dominion Resources Services, Inc. (ADAMS Accession No. ML14316A410), and anonymous submittals (ADAMS Accession No.'s ML14297A153, ML14297A155, ML14302A077, and ML14304A540). Enclosed are the NRC responses to all public comments.

Enclosure:
NRC Responses to Public Comment

CONTACT: James Gaslevic, NRO/DCIP/IGCB
301-415-2776

June 9, 2015

MEMORANDUM TO: Brian Anderson, Branch Chief
ITAAC and Generic Communication Branch
Division of Construction Inspection
and Operational Programs
Office of New Reactors

FROM: James Gaslevic, Reactor Operations Engineer ***/ra/***
ITAAC and Generic Communication Branch
Division of Construction Inspection
and Operational Programs
Office of New Reactors

SUBJECT: RESPONSE TO PUBLIC COMMENTS ON DRAFT REGULATORY ISSUE SUMMARY 2014-XX, "OVERSIGHT OF COUNTERFEIT, FRAUDULENT, AND SUSPECT ITEMS IN THE NUCLEAR INDUSTRY"

A notice of opportunity for public comment on the subject regulatory issue summary was published in the *Federal Register* (79 FR 59521) on October 2, 2014. Comments were received from the University of Florida (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14297A154), Roger Johnston (ADAMS Accession No. ML14309A247), the Nuclear Energy Institute (ADAMS Accession No. ML14311A039), Dominion Resources Services, Inc. (ADAMS Accession No. ML14316A410), and anonymous submittals (ADAMS Accession No.'s ML14297A153, ML14297A155, ML14302A077, and ML14304A540). Enclosed are the NRC responses to all public comments.

Enclosure:
NRC Responses to Public Comment

CONTACT: James Gaslevic, NRO/DCIP/IGCB
301-415-2776

ADAMS Accession No.: ML15008A192 *concurred via e-mail

OFFICE	NRR/DPR/PGCB*	NRO/DCIP/IGCB	NRO/DCIP/IGCB
NAME	ELee	JGaslevic*	BAnderson*
DATE	2/26/2015	3/3/2015	6/09/2015

OFFICIAL RECORD COPY

Analysis of Public Comments on
DRAFT NRC REGULATORY ISSUE SUMMARY 2014-XX
"OVERSIGHT OF COUNTERFEIT, FRAUDULENT, AND SUSPECT ITEMS IN THE NUCLEAR INDUSTRY" (ML14192B407)

Comments on the subject draft regulatory issue summary are available electronically at the U.S. Nuclear Regulatory Commission's (NRC's) electronic Reading Room at http://www.nrc.gov/reading-rm/adams.html. From this page, the public can gain entry into Agencywide Documents Access and Management System (ADAMS), which provides text and image files of NRC's public documents. Comments were received from the following individuals or groups:

Letter No.	ADAMS Accession No.	Commenter Affiliation	Commenter Name
1	ML14297A153	No Known Affiliation	Anonymous
2	ML14297A154	University of Florida Training Reactor	Daniel Cronin
3	ML14297A155	No Known Affiliation	Anonymous
4	ML14302A077	No Known Affiliation	Anonymous
5	ML14304A540	No Known Affiliation	Anonymous
6	ML14309A247	No Known Affiliation	Roger Johnston
7	ML14311A039	Nuclear Energy Institute (NEI)	Russell Bell
8	ML14316A410	Dominion Resources Services, Inc.	T.R. Huber

This document lists each public comment by letter number. For each comment, the NRC has repeated the comment as written by the commenter followed by the NRC's response. In some instances, the comment was broken down into segments for clarity. Each comment is referred to by letter number listed above and each comment from the corresponding letter.

Comment No.s 1-1, 3-1, and 5-1

1-1: The NRC states that it "is issuing this regulatory issue summary (RIS) to heighten awareness of the existing NRC regulations and how they apply to counterfeit, fraudulent, and suspect items (CFSI) within the scope of NRCs regulatory jurisdiction."

The RIS includes a discussion of the NRCs Safety Culture Policy Statement. Although safety culture is an important part of emphasizing safety over other priorities, it is not a 'regulation' of the NRC. A discussion of safety culture isn't appropriate for a RIS that is heightening awareness of existing "regulations."

Does NRC intend to include safety culture in all RIS publications? If not, why is the issue of CFSI important enough to need a separate discussion of safety culture?

3-1: Why does this document mention safety culture? This document is supposed to discuss NRC regulations. Safety culture is not a regulation. Is NRC planning to discuss safety culture in all of its publications?

5-1: I noted that the draft document includes a paragraph about nuclear safety culture.

This implies that a licensee's identification of a counterfeit item means there's a safety culture problem at that facility. Is that what the NRC is saying here?

This type of NRC document (Regulatory Issue Summary) doesn't usually discuss safety culture. What's so special about this topic to warrant a special mention of safety culture?

NRC Response

The NRC agrees that the NRC's position on nuclear safety culture is not defined in NRC regulations. The NRC promulgated its position on Safety Culture through a Commission Policy Statement that was published in the June 14, 2011 *Federal Register* (76 FR 34773). The purpose of referencing safety culture in the RIS, as the RIS states, is merely to assert that "certain attributes of a positive safety culture may assist efforts in identifying and dispositioning CFSI." For example, as described in the RIS, industry guidance in the area of quality assurance states that nuclear power plant licensees should consider applicable operating experience when performing audits of quality assurance programs. This is not a regulatory requirement; however, with the understanding that other industries are being challenged by counterfeit and fraudulent components, prudence and continuous learning—a safety culture trait—dictate that licensees should consider reviewing and applying applicable lessons learned (i.e. operating experience) from affected industries.

The NRC does not agree that the mere identification of a counterfeit or fraudulent item at an NRC-regulated entity is indicative of a deficient safety culture. It is worthy to note that, as it relates to nuclear power plant licensees, NRC Inspection Manual Chapter 0310 (ADAMS Accession No. ML14337A018) specifically states that current NRC practice is to only "draw conclusions about safety culture based on the results of licensee and NRC safety culture assessments conducted by qualified staff."

The NRC has not regularly discussed safety culture in past generic communications and there is no initiative to do so in the future. However, when the NRC determines that safety culture aspects relate to a particular issue, the NRC can elect to highlight those observations in communications to the regulated community.

No change was made to the RIS in response to the comment.

Comment No. 2-1

The staff should consider splitting out the non-power reactor information from the power reactor information to prevent confusion.

Within the NUCLEAR REACTORS section, only the 5th paragraph on page 4 is directly applicable to nonpower reactors. Essentially, everything else in this section applies to power reactors only. Separating out the non-power reactor information, or adding a sub header for non-power reactors, would be beneficial for both staff and licensees in calling awareness to the applicable existing regulations while minimizing the likelihood of misinterpretation.

NRC Response

The NRC agrees with the comment. The subject paragraph was relocated to the end of the Nuclear Reactors section to better call attention to the subject's differences, and a sub-header was added.

Comment No. 4-1

The research and test reactors discussion on page 4 should be better highlighted for the reader. I recommend creating a separate section/header for RTRs.

NRC Response

The NRC agrees with the comment. The subject paragraph was relocated to the end of the Nuclear Reactors section to better call attention to the subject's differences, and a sub-header was added.

Comment No. 6-1

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

NRC Response

The NRC disagrees with the commenter's recommendation to change the content on page 3 because the comment goes beyond the scope of the RIS. The intent for issuing this RIS is to heighten awareness of the existing NRC regulations and how they apply to CFSI. Items (1) and (2) cited above are tasks more closely associated with industry's implementation of these regulations. Regarding item (3), the NRC has an allegation process which allows anyone to provide a tip to the regulator. For information, please see NUREG/BR-0240, "Reporting Safety Concerns to the NRC".

No change was made to the RIS in response to the comment.

Comment No. 6-2

Quality control/assurance is emphasized throughout the document as the way to tackle CFSI, but this hasn't worked well in other industries in the past and it won't work well in the nuclear arena. Detecting CFSI should be a separate program with independent people who are more proactive and less passive to the problem than QC/QA/Procurement people, and who conduct proactive threat and vulnerability analyses, or coordinate with others who do this. (They would also have fewer conflicts of interest because the discovery of CFSI is usually taken to be a failure of the QC/QA/Procurement departments.)

NRC Response

The NRC disagrees with the commenter's recommendation to separate CFSI from the QA/QC programs. CFSI detection and response is part of quality assurance. Actions required to perform these tasks are performed by QA/QC personnel. The need for developing a separate program for CFSI is not seen as a requirement.

No change was made to the RIS in response to the comment.

Comment No. 6-3

Formalistic, objective evidence of the failure of a product to perform to spec--which this document emphasizes--is a poor way to head off problems with CFSI (or with deliberate sabotage of hardware or software, for that matter).

NRC Response:

The NRC disagrees with the commenter's statement that failure of a product to perform as specified is a poor way to head off problems associated with CFSI, or with deliberate sabotage. Owners and operators of nuclear power plants licensed by the NRC are responsible for assessing and managing the potential for adverse effects on safety, security, and emergency preparedness functions, including those posed by cyber security threats, so as to provide high assurance that critical functions are protected. Effectively implementing a quality assurance program in compliance with the requirements of 10 CFR Part 50 Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," includes accounting for special controls, processes, test equipment, and skills needed to attain the required quality, and also for the verification of quality by inspection and test (Criterion II, "Quality Assurance Program").

No change was made to the RIS in response to the comment.

Comment No. 6-4

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

NRC Response:

The NRC agrees with the comment that departure from technical requirements is not the best way or only way to detect CFSI. Other indicia, such as irregular documentation or shipment from a source with a documented history of providing CFSI, may be effective ways of detecting CFSI. However, the NRC believes that the commenter misunderstood the NRC's intent in the discussion at issue, which was to explain ways that compliance with NRC requirements can aid in the successful management of CFSI issues.

No change was made to the RIS in response to the comment.

Comment No. 6-5

Also on page 7, the situation seems to be that if I didn't know something was CFSI, I'm off the hook. This would seem to be a strong incentive for see-no-evil, hear-no-evil, speak-no-evil.

NRC Response:

The NRC disagrees. Consistent with existing NRC regulations, it is a licensee's responsibility to provide reasonable assurance that the items and components designated as safety significant will perform their intended safety function. As discussed in the RIS, NRC regulations impose positive obligations on applicants and licensees, which if implemented, can successfully identify CFSI. Failures to comply with and effectively implement NRC requirements are grounds for enforcement action and possible criminal referrals. For example, 10 CFR 50.5, "Deliberate misconduct" prohibits engaging in conduct that causes a licensee or applicant to be in violation of any rule, regulation, or order; or any term, condition, or limitation of any license issued by the Commission. Thus, compliance with existing NRC requirements effectively preludes applicants and licensees from deliberately ignoring and failing to adequately address CFSI issues with respect to NRC-regulated activities.

Finally, as discussed in the response to comments 1-1, 3-1 and 5-1, a positive safety culture supports an effective approach to managing CFSI.

No change was made to the RIS in response to the comment.

Comment No. 6-6

The encouragement on page 7 to voluntarily report CFSI issues thus seems a little naive. This is one way an anonymous tip line could help.

NRC Response

The NRC disagrees because as noted on page 3 of the final RIS (previously appeared on page 8 of the draft RIS), CFSI issues, like other safety issues, may be reported anonymously through the NRC's safety hotline. Concerned individuals also have the option to report issues through the NRC's Allegations Program, which also provides the option for anonymity.

No change was made to the RIS in response to the comment.

Comment 6-7

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

NRC Response

The NRC disagrees with the comment. The Cyber Security Directorate (CSD) and Intelligence Liaison and Threat Assessment Branch (ILTAB) in the Office of Nuclear Security and Incident Response work closely in parallel to manage agency-wide activities related to cyber security threats at NRC licensee facilities. CSD frequently conducts technical reviews of licensee cyber security plans in order to evaluate industry compliance with regulations and develops guidance for the review of license applications. ILTAB assesses the threat environment affecting regulated activities, performs rapid assessment of the credibility of threats and security events, coordinates with the intelligence and law enforcement communities, assesses illicit trafficking events, and reviews the adequacy of NRC's design basis threats based on domestic and foreign events and intelligence information.

Together, they work with other federal agencies, including other independent regulatory agencies, and nongovernmental entities to investigate cyber incidents, share best practices, reduce burdens, and address potential issues in this rapidly evolving field to ensure proactive measures are taken against new cyber threats. The NRC has also joined the Department of Homeland Security's National Intellectual Property Rights Coordination Center (NIPRCC). The NIPRCC leverages the combined resources, skills and authorities of the partner agencies to better combat intellectual property theft and identify and dismantle the criminal organizations that seek to profit from the manufacturing, importation and sale of counterfeit items.

The RIS also references Information Notice 2012-22, "Counterfeit, Fraudulent, Suspect Items (CFSI) Training Offerings," (ADAMS Accession No. ML12137A248) which provides a list of training resources that can be used for educating personnel involved in NRC-regulated activities on current trends in CFSI and techniques to prevent the use of CFSI parts. Table 1 of Information Notice 2012-22 includes 28 training sources, many with multiple courses on different topics. The topic descriptions include various attributes such as an emphasis on hands-on training, for example.

No change was made to the RIS in response to the comment.

Comment 6-8

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

NRC Response

The NRC agrees with the comment. NRC licensees subject to enforcement may or may not necessarily receive an enforcement action, depending on the circumstances of each individual case. Therefore, whether a person or entity is subject to enforcement action is based on the decisions reached through the implementation of the NRC's Enforcement Policy.

For clarity, the sentence was revised as follows:

> "Any organization or individual who provides counterfeit or fraudulent material to an NRC-regulated entity in violation of the NRC's requirements may be subject to inspection, investigation, enforcement, and possible criminal prosecution."

Comment No. 7-1

The draft RIS provides a sound summary of the regulations that are relevant to the issue of CFI and supports the conclusion that existing regulations, including 10 CFR Part 50, Appendix B, and the actions the industry takes to comply with these regulations and provide reasonable assurance of adequate protection to the public health and safety. We recommend that the final RIS clearly state this important conclusion.

NRC Response

The NRC agrees with the comment. Under the Summary of Issue section, the second sentence of the first paragraph was revised as follows:

> "Although supply chains for other industrial sectors may be substantially affected by CFSI events, it is the NRC's position that adherence to existing NRC regulations provides adequate protection of the public health and safety."

Comment No. 7-2(a)

Discussion of the NRC's cyber security rule (10 CFR 73.54) for operating power reactors in the draft RIS is unnecessary and confusing, and we recommend that discussion of it be deleted.

NRC Response:

The NRC disagrees with the recommendation to delete the discussion of the cyber security rule (10 CFR 73.54) from CFSI. The NRC believes that malicious code embedded into an electronic device and delivered to a licensee as an item for use in a safety or security related application is a potential safety or security related issue. Such an activity could potentially affect both the quality of a procured component important to safety, and pose a risk that the licensee adequately protect a critical digital asset. Appendix B to 10 CFR 50 adequately addresses the conventional quality assurance characteristics associated with the design, manufacture, and construction of the item. However, as stated in Regulatory Guide 5.71, if a licensee or applicant chooses to address 10 CFR 73.54 through the use of design features, then details of any design features of the safety system intended to meet a cyber security provision of 10 CFR 73.54, must be submitted to NRC for review and approval. Embedded malicious code risk characteristic of digital electronic devices is prominently presented in Appendix C; Section C.3.3, "Malicious Code Protection," of Regulatory Guide 5.71, "Cyber Security Programs For Nuclear Facilities."

No change was made to the RIS in response to the comment.

Comment No. 7-2(b)

Cyber security threats are not a subset of counterfeit and fraudulent items, and the draft RIS conflates these two separate topics. As an example, on page 4, the draft RIS identifies the potential for a digital asset to contain malicious code. However, that potential exists regardless of whether the part is authentic or is a CFI.

NRC Response:

The NRC agrees that cyber security threats are not a subset of counterfeit and fraudulent items. However, to the extent that the comment suggests that these are unrelated, the NRC disagrees.

Cyber security threats can be introduced in any number of ways, including the use of counterfeit and fraudulent items which contain malicious or incorrect code.

No change was made to the RIS in response to the comment.

Comment No.s 7-2(c) and 7-2.2

7-2(c):We are also concerned that the draft RIS's discussion of malicious code appears to introduce a new regulatory position, which is inconsistent with the intent stated in the draft RIS. We do not believe malicious code embedded in the software of digital electronic devices is a new or unique failure mode. We are also are unaware of any prior NRC communication of this conclusion, and the draft RIS does not contain any further basis for the statement.

7-2.2: On page 4, second paragraph, second sentence: The first half of the sentence stating that "With the exception of potentially malicious code embedded in the software of digital electronic devices (a regulatory issue under 10 CF 73.54)," should be deleted. We agree with the second half of the sentence, that CFI does not create any new or unique failure mode, and believe it should be retained in the draft RIS.

NRC Response:

The NRC agrees that malicious code embedded in the software of digital electronic devices is not a new or unique failure mode. The NRC disagrees with the comment that the draft RIS's discussion of malicious code appears to introduce a new regulatory position, inasmuch as the RIS simply reiterates NRC regulatory requirements . However, upon consideration of this comment, the NRC will make some clarifying revisions to the RIS.

The NRC agrees with the recommendation to delete the first half of the sentence in question regarding embedded software in digital electronic devices for the reasons stated above. The RIS was revised as follows:

Under the Nuclear Reactors section, the third paragraph (previously the second paragraph under the Nuclear Reactors section of the draft RIS) was revised as follows:

"CFSI can result in noncompliance with regulatory requirements. While potentially malicious code embedded in the software of digital electronic components does not constitute a new failure mode for these devices, this form of tampering (embedded software coding) is unique to digital electronic devices where it can prevent the device from performing its intended safety function, or cause other safety related components to fail to perform their intended safety function(s). However, neither industry nor the NRC has identified a new or unique failure mode associated with a counterfeit or fraudulent item that could not be reasonably identified or eliminated by an effective NRC-approved quality assurance program. Thus, adherence to effective QA programs should be effective in addressing CFSI for digital hardware. When embedded code is inserted in hardware, additional risks to safety and security may arise. Regulatory Guide 5.71, Appendix C, "Operational and Management Security Controls", specifically section C.3.3, "Malicious Code Protection", section C.3.7, "Software and Information Integrity", and section C.12, " System and Service Acquisition", address malicious code controls and provide guidance for acceptable methods for meeting the requirements of 10 CFR 73.54." Thus, cyber security programs can also be effective in addressing CFSI for embedded code inserted in hardware.

Comment No. 7-2(d)

If the NRC has concerns about cyber security, or believes that the regulatory treatment of cyber security deserves further clarification, then it should be addressed outside of the RIS for CFI.

NRC Response:

The NRC disagrees with the recommendation to disassociate cyber threats from counterfeit and fraudulent items for reasons stated above. Additionally, the NRC continually strives to assure that the current regulatory framework is effective in addressing issues that potentially challenge the Agency's mission to license and regulate the Nation's civilian use of radioactive materials to protect public health and safety, promote the common defense and security, and protect the environment.

No change was made to the RIS in response to the comment.

Comment No. 7-2(e)

Specific mention of digital assets in the RIS is not necessary, as they are adequately addressed in the RIS through the discussion of the applicable regulations, for example Appendix B to 10 CFR Part 50. For these reasons, the discussion of cyber security and digital assets in the three places in the draft RIS should be deleted:

NRC Response

The NRC disagrees that the discussions on cyber security and digital assets should be deleted from this RIS. The discussions offered in the RIS on cyber security and digital assets related to 10 CFR 73.54 have similarities to purchasing and operation

requirements for safety related items. These similarities include fraudulent misrepresentations of quality of those items. The risks of a cyber-attack from within the supply chain are appropriately associated with the cyber rule, 10 CFR 73.54, and serve to augment product and service quality requirements specified in 10 CFR 50, Appendix B.

No change was made to the RIS in response to the comment.

Comment No. 7-2.1

On page 1, second paragraph, second sentence: The sentence should be deleted.

NRC Response

The NRC disagrees with the recommendation to delete the sentence. Cyber security threats can potentially be introduced through counterfeit and fraudulent items for the reasons stated in the response above.

No change was made to the RIS in response to the comment.

Comment No. 7-2.3

On page 7, third full paragraph: The entire paragraph discussing cyber security and digital assets should be deleted. We further note that Regulatory Guide 5.71 is not applicable to the topic of procuring safety-related digital assets; rather, Regulatory Guide 1.152, Revision 3, is more relevant to this topic.

NRC Response

The NRC agrees that Regulatory Guide 1.152, Revision 3, is more relevant to this topic, but still considers Regulatory Guide 5.71 applicable to the topic of procuring safety-related digital assets. Regulatory Guide 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” is more appropriately focused towards software applications developed to perform specific safety related functions. However, as stated in Regulatory Guide 5.71, if a licensee or applicant chooses to address 10 CFR 73.54 through the use of design features, then details of any design features of the safety system intended to meet a cyber security provision of 10 CFR 73.54 must be submitted to NRC for review and approval. Regulatory Guide 5.71 provides guidance for one method of acquiring systems and/or services of items subject to the applicable requirements of the cyber security rule, 10 CFR 73.54. Specific reference to the threat of malicious code embedded within these devices can be found in Appendix C of Regulatory Guide 5.71, “Operational and Management Security Controls”, specifically section C.3.3, “Malicious Code Protection,” section C.3.7, “Software and Information Integrity,” and section C.12, “System and Service Acquisition.”

No change was made to the RIS in response to the comment.

Comment No. 7-3

On a related note, NRC has not promulgated a cyber security rule applicable to fuel cycle facilities or other non-power reactor materials licensees. Rather, a staff options paper is expected to be submitted to the Commission in the near term and an NRC decision on the path forward for cyber security at fuel facilities is forthcoming, e.g., issuance of orders or rulemaking. Therefore, the NRC should be mindful of this related programmatic direction when providing CFI guidance applicable to various categories of NRC licensees.

NRC Response

The NRC agrees with the comment that, at the present time, the NRC has not promulgated a cyber security rule applicable to fuel cycle facilities or other materials licensees. In March 2015, the Commission directed the staff to initiate a cyber security rulemaking for fuel cycle facilities that should be completed and implemented in an expeditious manner.

No change was made to the RIS in response to the comment.

Comment No. 7-4

Finally, on page 7, second full paragraph, second sentence: The NRC states that licensees, applicants and vendors "may want to consider submitting" voluntary reports. It should be stated more clearly that this is an option, and the staff should use alternative wording such as "may submit."

NRC Response

The NRC agrees that the wording of this sentence can be enhanced by making the recommended change without affecting the statement's intended message. The RIS was revised as follows:

> "Nonetheless, licensees, applicants and vendors may submit voluntary reports to communicate significant deviations from procurement specifications with potentially generic implications since in most cases safety significance must be determined on a plant specific basis."

Additional clarification was made by moving the last sentence of the subject paragraph regarding reporting through the NRC's Allegations program to the Background section, due to its applicability to nuclear reactors, nuclear materials, and radioactive waste.

Comment No. 8-1

Page 5 of 13 - Third paragraph - Second sentence states . . . "For example, Criteria II ("Quality Assurance Program") and XVIII ("Audits") in Appendix B require self-assessments and audits of quality assurance programs, respectively." However, the term "self-assessments" is not mentioned in Criteria II or XVIII. The associated sentence

in Criteria II states that... "Management of other organizations participating in the quality assurance program shall regularly review the status and adequacy of that part of the quality assurance program which they are executing."

The term "self-assessment" has other specific meanings within the nuclear industry. "Self-Assessment" is typically recognized as an Institute of Nuclear Power Operations term which does not require independence in its implementation from the organization or activity being evaluated. Use of this term in the proposed manner can be confusing.

We recommend modification of the terminology to avoid the confusion that could be caused by the use of the term "self-assessment."

NRC Response

The NRC agrees with the comment. Appendix B to 10 CFR 50 does not require self-assessments, and Regulatory Guide 1.28, “Quality Assurance Requirements for Nuclear Facility Applications”, does not use the term “self-assessments”. Criterion II of Appendix B requires that “the applicant shall regularly review the status and adequacy of the quality assurance program and Management of other organizations participating in the quality assurance program shall regularly review the status and adequacy of that part of the quality assurance program which they are executing." Criterion XVIII of Appendix B requires that “a comprehensive system of planned and periodic audits shall be carried out to verify compliance with all aspects of the quality assurance program and to determine the effectiveness”.

The second and third sentences of the paragraph were revised as follows:

> “Criterion II (“Quality Assurance Program”) states that regular reviews of the status and adequacy of quality assurance programs shall be performed, and Criterion XVIII (“Audits”) states that periodic audits of quality assurance programs shall be carried out. Industry guidance, to which some licensees have committed within their quality assurance programs, suggests that recent industry experience should be used to inform the processes for conducting both internal and external audits.”

Comment No. 8-2

Page 6 of 13 - Middle of paragraph beginning with Criterion XV.

ASME NQA-1-2008 was endorsed by RG 1.28 in July 2009 with the 2009 Addenda. However, the sentence as written does not, but should, include reference to the 2009 Addenda to be current and avoid confusion.

NRC Response

The NRC agrees with the comment. Regulatory Guide 1.28, “Quality Assurance Requirements for Nuclear Facility Applications”, Revision 4 identifies both ASME NQA-1-2008 and ASME NQA-1a-2009 Addenda.

The sentence was revised as follows:

> "ASME NQA-1-2008 and ASME NQA-1a-2009 Addenda, "Quality Assurance Requirements for Nuclear Facility Applications"—approved for use in RG 1.28, "Quality Assurance Program Criteria (Design and Construction)" in July 2009—provides additional acceptable approaches for this area."