Comment Resolution Summary
Resolution of Comments for
Manual Chapter 1245 Appendix C-14 cyber Security Inspector Technical Proficiency Training and Qualification Journal

Source	Section	Page #	Comment	Added	Remarks
NRO	Required Reactor CSI Training Curriculum	1	M1: Where does somebody sign up for these courses? They are not in iLearn. Also, do they have numbers associated with them? (H-101, etc),if so, it might be nice to include those.	N	This is a new program and courses are yet to be developed and entered into iLearn. Hence, why we are developing a 1245 Qualification to justify getting courses created.
NRO	Required Reactor CSI Training Curriculum	1	M2: Same comment as above	N	Same comment as above
NRO	Topic	3	M3: Might want to call it Security CFR since all you address is CFR related to Security.	Y	Added
NRO	References	3	M4: How would a student get access to this document since it is safeguards info?	N	Documents availvable with a neeed to know, not dependent on your clearance level.
NRO	Evaluation Criteria	4	M5: You are asking him to discuss NEI 08-09, but it is not in the documents reviewed for this ISA. Suggest move it to another ISA.	Y	NEI 08-09 is included in the References section for ISA on Cyber Security Plan and Implementing Procedures. Individuals will be required to obtain a copy of the documents in the Reference section and become familiar with it.
NRO	Tasks	4	M6: Provide more definitions that you would like student to be aware of. Too Vague – this is a common theme throughout this document.	N	IMC do not include definitions
NRO	Tasks	4	M7: Should this be CFR 73 vs. 72?	N	Removed section from document
NRO	Tasks	4	M8: Should be Reg. Guide 5.69 vs. 5.59	N	Removed section from document
NRO	References	5	M9: How do you obtain a copy of a licensee's cyber security plan?	Y	Added: To obtain cyber security plans perform a search in ADAMS.
NRO	References	5	M10: Suggest adding ML # for this document.	Y	The ADAMS # is recorded in Attachment 1.

Source	Section	Page #	Comment	Added	Remarks
NRO	Evaluation Criteria	5	M11: Too vague – should have more detail what you expect student to know.	N	The given evaluation criteria and task provides what the expectation are of a student. The ISA and OJT's have been reviewed by SR Cyber Security Specialist
NRO	Evaluation Criteria	5	M12: Too vague – what definitions do you want the student to know? Specify. Might be a good idea to get a Sr. Cyber Security Inspector's input because they would know what is important.	N	The given evaluation criteria and task provides what the expectation are of a student. The ISA and OJT's have been reviewed by SR Cyber Security Specialist
NRO	References	7	M13: Note this ML # does not give you NEI 10-04, it gives you comments on the document.	Y	Added the correct ML #.
NRO	Evaluation Criteria	7	M14: Again – very vague – suggest sitting down with a Cyber security inspector and documenting what a new person needs to know.	N	The given evaluation criteria and task provides what the expectation are of a student. The ISA and OJT's have been reviewed by SR Cyber Security Specialist
NRO	Tasks	7	M15: Words like read and understand are not good training words. These are not specific or objective.	N	Do not find an issue with the wording as it is.
NRO	Evaluation Criteria	9	M16: Same comment as previous ISA. Also it is weird to have an ISA with only one evaluation criteria and only one task.	N	No useful information from this comment
NRO	Tasks	9	M17: Same comment as previous ISA	N	No useful information from this comment
NRO	Evaluation Criteria	10	M18: Good Criteria – make more criteria like this vs. Discuss general content	Y	Accepted
NRO	Tasks	11	M19: Same comment as on previous ISA	Y	Accepted
NRO	Evaluation Criteria	13	M20: I'm not sure how you would identify a licensee identified finding via IMC 0612 – Issue screening. Maybe you could say, given an issue of concern take it through 0612 and screen it.	Y	Accepted

Source	Section	Page #	Comment	Added	Remarks
NRO	Tasks	13	M21: What appendix address Cyber SDP? I did not see it in 0609?	Y	Appendix E Part IV
NRO	Tasks	13	M22: Good tasks!!	Y	Thanks.
NRO	Tasks	13	M23: Suggest eliminating the word violation statement and just make - violation. Be able to write a cyber security violation. (This includes …	N	ISA-CS-6: Changed Task 3 to wording provided by comment from Region III (SA19)
NRO	References	15	M24: Reg Guide 5.81 actually reads Target Set Identification and Development for Nuclear Power Reactors (OUO-SRI)	Y	Added the word "Power" and "(OUO-SRI)"
NRO	References	15	M25: What is this?	N	Do not understand the comment.
NRO	References	15	M26: What is this?	N	Do not understand the comment.
NRO	Tasks	15	M27: Need more than 1 task – get input from a Cyber Security Inspector	Y	More tasks added
NRO	CSI Individual Study Activity	17	M28: Wouldn't this be an On the Job Training activity (OJT) vs. ISA?	N	Do no know which ISA is being referred to.
NRO	Documentation	18	M29: Maybe discuss with a Sr. Cyber Security Inspector on additional OJT that might be useful.	N	At this stage in the cyber security program, two OJT's have been determined to be sufficient
NRO	Documentation	18	M30: I notice that there are only 2 OJT activities – doesn't seem like a lot. Should there be an activity to go on a Cyber Security Inspection and do …?	N	At this stage in the cyber security program, two OJT's have been determined to be sufficient
Region I			JR1: What would be nice is a summary of the history of the program.	N	IMC's are not the place to provide prgram history
Region I			JR2: An IST to learn the inspection procedure, which is not referenced at all here. It should proceed the SDP section. The inspection program currently exists in TI format and will eventually have a Triennial pace. But it could cover the procedure and the process for going from finding to NSIR concurrence. The section on SDP does lay out some of it, but asks no real questions.	N	Primary inspectoin procedures used is a temporary instruction and is not used as a reference in IMC

Source	Section	Page #	Comment	Added	Remarks
Region I			JR3: The OJT are interesting in that they are listed as individual activities, how about merging them into a Participate as Observer on a Cyber Inspection.	N	Attributes accomplished during inspection but not required
Region I			JR4: The area continues to develop with other guidance document NEI 13-10 Cyber Security Control Assessment. This lays out a framework to screen CDA as direct and indirect.	N	Nothing to add from this comment
Region I			JR5: The two courses listed, did present everything that the ISTs go over. In fact the first draft of this said to just attend the course. If the advanced courses are not available then the IST and OJT do make sense.	N	This is a new program and courses are yet to be developed and entered into iLearn. Hence, why we are developing a 1245 Qualification to justify getting courses created.
Region I			JR6: If there is ever a refresher component, then it should be limited to attending Cyber Inspector Workshops as approved by Supervisor. The last one that NSIR had my management wanted to limit the attendance to save travel money but the urgency of getting all the inspectors to align to better fend of NEIs attempts to do end a rounds with the Commission. In other words NEI said we were being mean and not implementing the requirements so NSIR committed to have an inspector workshop to resolve, boy did it backfire on NEI. Better trained inspectors is never a benefit to a licensee.	N	Nothing to add from this comment
Region II	Introduction	1	Daj1: ???	N	Do not understand the comment.

Source	Section	Page #	Comment	Added	Remarks
Region II	Required Reactor CSI Training Curriculum	2	R2: Will the Milestone 8 procedures be discussed?	N	Milestone 8 procedures are still being developed and tested via pilot programs
Region II	Evaluation Criteria	4	JP3: Since NEI 08-09 is not a reference for this topic, I do not think it should be an eval criteria for this topic.	N/Y	It is not specified in the evaluation criteria but it has been added to the references
Region II	Evaluation Criteria	4	JP4: Licensing activities include LAR and SERs which are not references for this topic.	N	LAR and SER's are extensions of the CSP which is part of the references
Region II	Tasks	4	R5: Do you mean part 73 here or Part 52 for New Reactors?	N	Part 73
Region II	References	5	JP6: Beneficial to include licensee LAR and NRC SER	Y	Added
Region II	References	7	M7: This document will also aid in defining what a CDA is.	N	Document not intended to define but to learn how to scope CDA
Region II	References	7	JP8: Belongs under topic CS-5	N	NEI 10-04 is not for cyber security controls; NEI 13-10 is specific to cyber security controls and is referenced
Region II	Evaluation Criteria	12	JP9: This eval criteria cannot be accomplished without a licensee procedure.	Y	Accepted
Region II	Tasks	12	JP10: These tasks do not seem to address the topic area. Another approach maybe to describe a sample of controls listed in Appendix D and E.	Y	Accepted
Region II	References	16	R11: Verify this is the reference that was intended.	Y	Accepted
Region II	References	16	R12: Should be part of the plan.	N	Too vague to add or comment on
Region II	Evaluation Criteria	20	R13: Wouldn't the controls be more applicable based upon the CDA? Suggest: Describe and categorize the cyber security controls implementation process based upon a sample of CDAs provided by senior inspector or branch chief.	N	Too vague to add or comment on

Source	Section	Page #	Comment	Added	Remarks
Region III	Introduction	1	SA1: Introduction: Considering the individual is certified inspector, this should be an Appendix D certification.	N	Appendix D is refresher training for existing inspectors. The Cyber Security inspector qualification is a specialty that requires additional skills similar to other Appendix C specialized inspector qualifications. Cyber security will also have refresher training every 3 years to be developed for Appendix D.
Region III	Introduction	1	SA2: This contradicts the paragraph above. If the person is already certified in engineering or physical security (for example), they have already completed Appendix A and B…therefore, this paragraph is NOT needed.	Y	Will remove paragraph 2 duplicate wording, merge with paragraph 1
Region III	Required Reactor CSI Training Curriculum	1	SA3: Do we expect individuals to complete the Intro course BEFORE starting the ISAs? If so, please state.	N	Intro course is not offered very frequently, but as needed. ISAs can be started before Intro course.
Region III	Required Reactor CSI Training Curriculum	1	SA4: Add course numbers for Intro and Advanced Cyber Security course?	N	Intro course to be offered at TTC. Currently, there are no course numbers.
Region III	Required Reactor CSI Training Curriculum	2	SA5: Is this listing the course detail necessary? Bottom line….if the course changes, we would need to revise this list? Recommend removing this detail.	Y	Removed section from document
Region III	Post Qualification & Refresher Training	2	SA6: If this remains in Appendix C, we would need to think about post qual and refresher work…..and add to Appendix D-1 (non safeguards information). Recommend as stated above, make this an Appendix D certification	Y/N	Initial cyber security inspector qualification should remain in Appendix C. Refresher training will be developed, but is not designed yet to include any reference in Appendix C-14 at this time.
Region III	Topic	3	SA7: Format not consistent with Appendix C or D.	Y	Formatted indentation consistent with recent C Appendices

Source	Section	Page #	Comment	Added	Remarks
Region III	Evaluation Criteria	4	SA8: (ISA-CS-1) Consider an additional task to relate Evaluation Criteria #4 to the inspection objective of the inspection procedure.	N	It is too advanced to have the first ISA asking for inspection review of inspection procedures. That is for later ISAs.
Region III	Competency Area	5	SA9: (ISA-CS-2) Change Competency Area to "Regulatory Framework – Technical Area Expertise"	Y	Added REGULATORY FRAMEWORK to the competency area.
Region III	Evaluation Criteria	7	SA10: (ISA-CS-3, Evaluation Criteria): This is a bit broad. Would we expect the individual to articulate what is in scope, what is out of scope and why? If so, I recommend putting more detail with respect to the level of knowledge we expect as a result of this ISA. See comment in next ISA.	N	The ISA is for learning the basics, the reference material, and how to do the activity. The OJT provides a more appropriate place to show applied knowledge and understanding.
Region III	Tasks	7	SA11: (ISA-CS-3, Task 2): 2 tasks seems a bit light for what is described in the purpose section. Consider tasking the individual to review violations/findings in this area to gain a practical understanding on how to apply this knowledge (rules and procedures)	N	The ISA is for learning the basics, the reference material, and how to do the activity. The OJT provides a more appropriate place to show applied knowledge and understanding.
Region III	Evaluation Criteria	9	SA12: (ISA-CS-3, Evaluation Criteria): See comment above. Understand safeguards material is involved; however, we should include the actual knowledge expectations of the individual.	Y	Updated ISA-CS-3 to reflect the proposed knowledge expectations.
			For example:		
			1. Name the types of systems and networks the licensee is expected to protect		
			2. Name the types of cyber attacks the licensee is expected to protect against		

Source	Section	Page #	Comment	Added	Remarks
			3. Describe how a licensee can evaluate and manage cyber risk.		
			Etc.		
Region III	Topic	10	SA13: Is ISA-CS-5 “Cyber Security Controls” significantly different from ISA 2 “Cyber Security Plan”? These could be combined.	N	These are two different documents. The Cyber Security Plan is an outline. Cyber security controls describe how to implement countermeasures in the plan.
Region III	Evaluation Criteria	13	SA14-SA17: (ISA-CS-6), Evaluation Criteria): Criteria 1-4 are tasks and should be moved to Task section.	Y/N	Partly agree to include Criteria #1-4 under Tasks. Criteria #1-2 will also remain as evaluation criteria.
Region III	Evaluation Criteria	13	• SA18: Add proposed evaluation questions: *Discuss the thresholds for determining what findings should be documented in an inspection report.*	Y	Added
			• *Describe how to process a finding using the cyber security SDP appendix and the possible outcomes.*		
			• *For one of the issues reviewed in “Tasks”, describe your actions to assess color and efficacy of the licensee’s corrective actions.*		
Region III	Tasks	14	SA19: (ISA-CS-6, Task 3): Since this is a task revise to:	Y	Revised Task 3
			Given a violation of regulatory requirements and the enforcement policy and guidance, write the analysis and enforcement sections for a finding, a violation, and a non-cited violation. Include an assessment for the applicable safety culture cross-cutting aspect.		
Region III	Tasks	14	SA20: (ISA-CS-6, Task 3): Are these traditional enforcement? If not, replace with significance color.	N	Changed severity level to “performance bands”

Source	Section	Page #	Comment	Added	Remarks
Region III	Tasks	15	SA21: (ISA-CS-7): Need to develop at least one task -- Considering an individual may have no security background, perhaps one task could be to describe a target set.	N	Deleted ISA-CS-7
			For your reference site, review the licensee's target set CDAs and determine how…essentially, turn the evaluation 2 into a task.		
Region III	Topic	16	SA22: (OJT-CS-1) I don't understand why this is an OJT. It's not clear that this activity needs to be done on site or by observing a certified inspector. Recommend adding the tasks and evaluation criteria to ISA-CS-3.	N	It's an OJT because activity is to be done onsite while participating in an inspection.
Region III	References	18	SA23: (OJT-CS-2): Add inspection procedure as a reference	N	Primary inspectoin procedures used is a temporary instruction and is not used as a reference in IMC
Region III	Evaluation Criteria	19	SA24: (OJT-CS-2): This is already included in ISA-CS-6	N	ISA-CS-6 and OJT-CS-2 are two different activities
Region III	Tasks	19	SA25: (OJT-CS-2): Is there an expectation to observe or participate in an inspection? If so, recommend adding the following task:	Y	Added to Task 2
			Observe the activities performed by a qualified inspector during the completion of the planned inspection by doing the following:		
			a. observing implementation of inspection procedures		
			b. observing interviews/discussion with facility personnel		
			c. observing facility work activities		
			d. reviewing documentation and records		
			e. discussing inspection results with the lead inspector		

Source	Section	Page #	Comment	Added	Remarks
Region III	Tasks	19	SA26: (OJT-CS-2): Need to add a task to at least review the inspection procedure and demonstrate understanding of the inspection attributes.	Y	Added to OJT-CS-2 as Task 2 and shifted the rest of the Tasks down.