NRC INSPECTION MANUAL

CSB

INSPECTION MANUAL CHAPTER 1245 APPENDIX C-14

CYBERSECURITY INSPECTOR
TECHNICAL PROFICIENCY
TRAINING AND QUALIFICATION JOURNAL

Table of Contents

INTRODUCTION

Complete Inspection Manual Chapter 1245 (IMC 1245), Appendix A, “Basic Inspector Certification Journal” before completing any activities or courses in this journal. The General Proficiency requirements contained in IMC 1245, Appendix B may be completed together with the Technical Proficiency requirements outlined in this journal to obtain initial inspector qualification.

This journal includes the certification requirements for inspectors who have already qualified as inspectors in another technical proficiency areas such as engineering or physical security and are seeking to obtain qualification in cybersecurity, or inspector candidates who are aspiring to obtain initial qualification. The courses and technical proficiency areas applicable to each type of inspector are identified in the signature cards and equivalency justification forms for each type of inspector at the end of this appendix. The Introduction Course or equivalency must be completed before the advanced course.

CAUTION

Some documents referenced in this appendix may contain safeguards information and or licensee proprietary information and should be controlled accordingly.

Required Cybersecurity Inspector courses for both Headquarters and Regional Inspectors:

- S-119 Introduction to Cybersecurity Inspection Training for NRC Inspectors - Self Study, or demonstrate basic understanding of information technology (IT), or computer science obtained through formal education or training (bachelor’s degree, IT certifications, or IT formal training) that provides the fundamentals of understanding networking, boundary devices, IT hardware, and IT software, **or**

- A course or series of courses that provide the basic understanding or fundamentals of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), see Exhibit 1, **and**

- S-504 Advanced Cybersecurity Inspection Training for NRC Inspectors

NOTE: INFORMATION ABOUT THE S-119 AND S-504 COURSES CAN BE FOUND IN THE NRC TRAINING MANAGEMENT SYSTEM.

Cybersecurity Inspector Individual Study Activities

(ISA-CS-1) Code of Federal Regulations (CFRs)

PURPOSE:

The purpose of this activity is to familiarize you with the regulations having direct application to the NRC cybersecurity oversight program. The Nuclear Regulatory Commission (NRC) requires that power reactor licensees establish, operate, and maintain a cybersecurity program in accordance with prescribed requirements identified in Title 10 of the *Code of Federal Regulations* (10 CFR). The CFR's provide the content and scope that various licensees must comply with or receive NRC approval to deviate from the requirements. By ensuring that the facility licensee is in compliance with the provisions delineated in 10 CFR 73.54 or other power reactor future cybersecurity oversight rules, we determine whether a licensee is meeting the cybersecurity protection objectives. For this reason, it is mandatory that all cybersecurity inspectors gain a comprehensive knowledge of the contents of applicable cybersecurity requirements included in the specific sections of the 10 CFR listed in the references section below. This activity will provide the inspector with detailed knowledge of the contents of the requirements and how to apply the appropriate cybersecurity regulation requirements.

COMPETENCY AREA: Regulatory Requirements Technical Area Expertise

LEVEL OF EFFORT: 24 -28 hours (based on an average of ~ 2 hours per document)

REFERENCES:

1. 10 CFR 50.54(p), "Conditions of Licenses"
2. 10 CFR 73.1, "Purpose and Scope"
3. 10 CFR 73.2, "Definitions"
4. 10 CFR 73.5, "Specific Exemptions"
5. 10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements"
6. 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements"
7. 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks"
8. Staff Requirements – COMWCO-10-0001 – Regulation of Cyber Security at Nuclear Power Plants (ML102940009)
9. SECY-10-0153 Cybersecurity – Implementation of the Commission's Determination of Systems and Equipment Within the Scope of Title 10 of the C*ode of Federal Regulations* Section 73.54 (ML103490344)

10. Memorandum of Understanding Between the U.S. Nuclear Regulatory Commission and the North American Electric Reliability Corporation (ML093510905)

11. Memorandum of Agreement Between the U.S. Nuclear Regulatory Commission and the Federal Energy Regulatory Commission (ML15033A181)

12. 10 CFR 73.55, “Requirements for the Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage”

13. 10 CFR 73.56, “Personnel Access Authorization Requirements for Nuclear Power Plants”

14. 10 CFR 73.70, “Records”

15. 10 CFR 73.77, “Cybersecurity Event Notifications”

16. If the Commission approves future power reactor cybersecurity oversight rules, they should be included in this qualification process

EVALUATION CRITERIA: At the completion of this activity, you should be able to:

Explain the requirements licensees must comply with for making changes to a cybersecurity plan as provided in 10 CFR 50.54(p). Describe the design-basis threats (DBT) used to design safeguards systems to protect against acts of radiological sabotage 10 CFR 73.1.

1. Review and gain a good understanding of the references listed above

2. Review the definitions of terms in 10 CFR 73.2

3. Review NRC specific exemptions 10 CFR 73.5

4. Be aware of and discuss the specific requirements for the protection of safeguards information 10 CFR 73.21 and 10 CFR 73.22

5. Give an overview of the requirements in 10 CFR 73.54, specifically discuss the following:

   (a) Systems and equipment that must be protected from cyberattacks

   (b) The Commission’s determination of systems and equipment within the scope of 10 CFR 73.54

   (c) The design-basis threat (DBT) (cyberattack) to SSEP functions

   (d) What specific requirements are included in 10 CFR 73.54

   (e) The relationship between the physical and cybersecurity programs

   (f) The objectives of the cybersecurity program

   (g) The cybersecurity event notification requirements in 10 CFR 73.77

(h) Records retention requirements

6. Identify the areas intertwined between the physical and cybersecurity programs 10 CFR 73.55

7. Discuss the answers to the questions and tasks listed under the evaluation criteria section of this study guide with your supervisor or a C-14 qualified cybersecurity inspector. Also discuss how some of the requirements of 10 CFR 73.56 are applicable to the cybersecurity program.

TASKS:

1. Locate and review general and specific cybersecurity activities described in 10 CFR 73.54.

2. Review the definition of, safeguards information, and other sensitive information, and determine the appropriate control measures for SGI as required in 10 CFR 73.21 and 10 CFR 73.22.

3. Review the information in 10 CFR 73.54, 10 CFR 73.55, and 10 CFR 73.56 and understand the relationship between the physical protection of nuclear power reactors, access authorization, and cybersecurity.

4. Determine what types of licensing actions can be submitted by licensees using 10 CFR 50.54(p), 10 CFR 50.54(q) 10 CFR 73.55(r), and 10 CFR 73.5.

5. Review the description and application of the DBT as described in 10 CFR 73.1. When possible, attend the cyber intelligence briefs (secret or official use only) prepared and conducted by the Intelligence Liaison Threat Assessment Branch (ILTAB).

6. Discuss the answers to the questions and tasks listed under the evaluation criteria section of this study guide with your supervisor or a C-14 qualified inspector.

DOCUMENTATION: Cybersecurity Inspector Proficiency Level Qualification Signature Card Item ISA-CS-2

Cybersecurity Inspector Individual Study Activities

(ISA-CS-2) Cybersecurity Plan (CSP) and Changes to the CSP

PURPOSE:

Each power reactor licensee is required by 10 CFR 73.54 to submit for NRC review and approval a cybersecurity plan (CSP) which provides the basis for the implementation of the regulation. The purpose of this activity is to become familiar with the licensee's CSP and supporting documentation (licensee's procedures) required to establish and implement the requirements of 10 CFR 73.54. Cybersecurity inspectors should be familiar with a licensee's CSP and implementation procedures before conducting an inspection at the facility. This activity will provide information on how to review a facility's CSP and the implementing procedures, to assess if the licensee's cybersecurity program meets all the requirements of 10 CFR 73.54.

COMPETENCY AREA: Inspection Regulatory Framework Technical Area Expertise

LEVEL OF EFFORT: 20 - 22 Hours (Based on an average of ~ 2 hours per document)

REFERENCES:

1. NRC-approved CSP for a facility designated by your supervisor
2. 10 CFR 50.54(p), 10 CFR 50.54(q)
3. NRC Regulatory Issue Summary 2014-02 Withdrawal of NRC Generic Letter 95-08, "10 CFR 50.54(p) Process for Changes to Security Plans Without Prior NRC Approval," (ML13151A084)
4. NEI 11-08, "Guidance on Submitting Security Plan Changes," Rev 0. (ML12216A194)
5. Regulatory Guide 5.71, "Cybersecurity Programs for Nuclear Facilities" (ML090340159)
6. Regulatory Guide 5.69, "Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements" (Safeguards Information)
7. NRC Letter to NEI, "Nuclear Energy Institute 08-09, "Cybersecurity Plan Template", Rev. 6 (ML101550052)
8. NEI 08-09, Rev.6, Addendum 1, "Cybersecurity Plan for Nuclear Power Reactors" (ML17079A423)
9. NEI 08-09, Rev. 6, Addendum 2, "Cyber Attack Detection, Response, and Elimination" (ML17236A268)

10. NEI 08-09, Rev. 6, Addendum 3, “Systems and Services Acquisition” (ML17236A269)

11. NEI 08-09, Rev. 6, Addendum 4, “Physical and Operational Environment Protection” (ML17236A270)

12. NEI 08-09, Rev. 6, Addendum 5, “Cybersecurity Vulnerability and Risk Management” (ML18212A282)

EVALUATION CRITERIA: At the completion of this activity, you should be able to:

1. Discuss the general contents of the CSP and the regulatory basis.

2. Review the CSP and determine if changes were made in accordance with the process in 10 CFR 50.54(p) CFR and guidance documents.

3. Identify specific areas where you would expect the licensee to have developed more detailed implementing procedures such as methods to scope-in assets to be protected, security control assessments and application, and implementation of alternate controls or controls that are not applicable.

4. Review the definitions of the following terms provided in the NEI 08-09 and/or RG 5.71:

   (a) Adverse impact

   (b) Credible

   (c) Critical digital asset (CDA)

   (d) Critical system (CS)

   (e) Cyberattack

   (f) Defense-in-depth

   (g) Support equipment

   (h) Support system

   (i) Vulnerability

5. Describe how each NEI 08-09 Rev. 6 addendum applies to the licensee’s implementation of the cybersecurity program

TASKS:

1. Locate a copy of the CSP for the assigned facility

2. Identify changes to the CSP, and sections specific to the site.

3. When observing an inspection, identify all the licensee cybersecurity procedures developed to implement the CSP.

> CAUTION: Physical security documentation such as the Physical Security Plan, the Training and Qualification, the Safeguards Contingency Plan, and implementing procedures generally contain safeguards information and should be controlled accordingly.

4. Locate copies of the regulatory requirements and regulatory guides identified in the reference section above.

5. Read and understand the CSP, regulatory and guidance documents, and any other supporting documentation necessary to be able to discuss the topics identified in the Evaluation Criteria above.

6. Discuss the answers to the questions and tasks listed under the evaluation criteria section of this study guide with your supervisor or a C-14 qualified inspector.

DOCUMENTATION: Cybersecurity Inspector Proficiency Level Qualification Signature Card Item ISA-CS-2.

Cybersecurity Inspector Individual Study Activities

(ISA-CS-3) Identifying Assets Subject to the Cybersecurity Rule

PURPOSE:

The NRC requires that a licensee be able to correctly identify its critical systems (CS) and critical digital assets (CDAs) to implement a protective strategy and to manage the risk associated with CDAs to ensure these assets are adequately protected. It is essential that all cybersecurity inspectors gain a detailed knowledge of the processes that a licensee must complete to meet these requirements. This activity will provide cybersecurity inspectors with detailed knowledge of the scoping of CDAs and the process used by the licensee to manage risk to meet the requirements of the rule.

COMPETENCY AREAS: Technical Area Expertise

LEVEL OF EFFORT: 16 – 18 Hours (Based on an average of ~ 2 hours per document)

REFERENCES:

1. 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks"
2. Regulatory Guide 5.71, "Cybersecurity Programs for Nuclear Facilities" (ML090340159)
3. NRC-approved CSP for a facility designated by your supervisor
4. NEI 10-04, "Identifying Systems and Assets Subject to the Cybersecurity Rule", Rev. 3 (ML21342A168)
5. NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions," (ML20129J981, ML20126G492)
6. NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Safety Related and Important-to-Safety Functions," (ML20223A256, ML20199M368)
7. NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Balance-of-Plant (BOP) Functions," (ML20209A442, ML20205L604)
8. NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Physical Security Functions," (ML21140A140, ML21155A216)
9. NRC safety evaluation report for the specific plant

EVALUATION CRITERIA: At the completion of this activity, you should be able to:

1. Describe the licensee's scoping methodology and the regulatory requirements for the scoping of CDAs.

2. Determine from the licensee's safety evaluation report what critical systems and critical digital assets are within the scope of 10 CFR 73.54.

3. Identify if the licensee has planned or performed any digital upgrades of equipment that perform SSEP functions.

4. Review violations and or findings in this area identified during inspections to gain a practical understanding on how to apply this knowledge (rules and procedures).

5. Name the types of systems and networks the licensee is expected to protect.

6. Describe the types of cyberattacks the licensee is expected to protect against.

7. Upon observing an inspection, understand the process the licensee uses to perform digital upgrades or replacement of equipment that perform SSEP functions (CDAs).

TASKS:

1. Read and understand the regulatory requirements included in 10 CFR 73.54.

2. Read and understand licensee's procedures for scoping CDAs.

3. Read and understand licensee procedures for performing digital replacements or upgrades including engineering change plans or other licensee information related to upgrading or changing systems and equipment that perform SSEP functions.

4. Discuss the answers to the questions and tasks listed under the evaluation criteria section of this study guide with your supervisor or a C-14 qualified inspector.

DOCUMENTATION: Cybersecurity Inspector Proficiency Level Qualification Signature Card Item ISA-CS-3

Cybersecurity Inspector Individual Study Activities

(ISA-CS-4) Licensee Protective Strategies

PURPOSE:

The NRC requires that licensees establish and implement a cybersecurity program for the protection of CS and CDAs identified as requiring protection against cyberattacks. The cybersecurity program must be designed to implement security controls, apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, recover from and mitigate the adverse impacts of cyberattacks. As part of the cybersecurity program, the licensee shall also evaluate and manage cyber risks, ensure modification to assets are evaluated, maintain the capability for timely detection and response to cyberattacks, correct exploited vulnerabilities, restore affected networks, and/or equipment affected by cyberattacks, and establish a cyber training program for licensee staff and personnel. To ensure the cybersecurity program is implemented adequately, the licensee shall develop and maintain written policies and implementing procedures, site-specific analysis and other supporting technical information that is subject to review during inspections. It is essential that all cybersecurity inspectors gain a detailed knowledge of the actions that a licensee must complete to meet these requirements. This activity will provide cybersecurity inspectors with detailed knowledge of the contents of the rule requirements and the NRC-approved CSP for a facility designated by your supervisor.

COMPETENCY AREA: Technical Area Expertise

LEVEL OF EFFORT: 16 – 18 Hours (Based on an average of ~ 2 hours per document)

REFERENCES:

1. 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks”

2. 10 CFR 73.77, “Cybersecurity Event Notifications”

3. Regulatory Guide 5.71, “Cybersecurity Programs for Nuclear Facilities” (ML090340159)

4. NRC-approved CSP for a facility designated by your supervisor

5. Regulatory Guide 5.69, “Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements” (Safeguards Information)

6. NEI 13-10, “Cybersecurity Controls Assessments” Rev. 7 (ML21342A203)

7. NEI 08-09, Rev. 6, Addendum 2, “Cyber Attack Detection, Response and Elimination” (ML17236A268)

8. NEI 08-09, Rev. 6, Addendum 3, “System and Services Acquisition” (ML17236A269)

9. NEI 08-09, Rev. 6, Addendum 4, “Physical and Operational Environment Protection” (ML17236A270)

10. NEI 08-09, Rev. 6, Addendum 5, “Cybersecurity Vulnerability and Risk Management” (ML18212A282)

11. RG 5.83, “Cybersecurity Event Notifications” (ML14269A388)

12. NEI 15-09, “Cybersecurity Event Notifications” (ML16060A507)

While observing an inspection, become familiar with the licensee’s policies and implementing procedures used to implement the cybersecurity program. Examples of licensee’s policies and procedures are:

- Cybersecurity program policy,
- CDA scoping methodology,
- Cybersecurity training for licensee personnel and contractors,
- CDA access control,
- Control of portable media and mobile devices,
- Physical and operational environment protection,
- Configuration management,
- Evaluation and management of cyber risks,
- Cybersecurity event notifications,
- Cybersecurity incident response,
- Assessment of cybersecurity controls,
- Cybersecurity contingency plan,
- Vulnerability assessment and risk management, and
- Systems and services acquisition process

The list above is not all inclusive, but it is a starting point for the inspector to have a basic understanding of the licensee’s implementation methods and defensive strategy to meet the requirements of 10 CFR 73.54.

EVALUATION CRITERIA: At the completion of this activity, you should be able to:

1. Discuss the regulatory requirements for the design, development, and implementation of a cybersecurity protective strategy.

2. Assess and evaluate the licensee's cybersecurity program and licensee's protective strategy described in the CSP to ensure 10 CFR 73.54 requirements are met.

3. Describe how a licensee can evaluate and manage cybersecurity risks in order to maintain confidentiality, integrity, and availability of CDAs, ensure the effectiveness of security controls, and provide reasonable assurance that the licensee's defense-in-depth strategy is maintained.

TASKS:

1. Read and understand the regulatory requirements included in 10 CFR 73.54(c)(2).

2. Obtain a copy of IP 71130.10, "Cybersecurity," review and understand the inspection objectives, samples, background, inspection requirements, and the guidance for performance testing.

3. Discuss the answers to the questions and tasks listed under the evaluation criteria section of this study guide with your supervisor or a C-14 qualified inspector.

DOCUMENTATION: Cybersecurity Inspector Proficiency Level Qualification Signature Card Item ISA-CS-4.

Cybersecurity Inspector Individual Study Activities

(ISA-CS-5) Cybersecurity Controls

PURPOSE:

The NRC requires each power reactor licensee to establish and implement a defense-in-depth strategy that includes addressing or implementing cybersecurity controls or alternate controls in accordance with 10 CFR 73.54(c)(1) and the licensee's CSP. The licensee has also the flexibility to demonstrate an attack vector does not exist and therefore a security control may not be necessary to protect a CDA. It is essential that all cybersecurity inspectors gain a detailed knowledge of the actions that a licensee must complete to meet these requirements. A description of the security controls is provided in the facility's CSP. The way each control is addressed is described in the facility's CSP implementing procedures. This activity will provide information on how to review a facility's CSP, which are available at the facility during an inspection.

COMPETENCY AREAS: Technical Area Expertise Inspection

LEVEL OF EFFORT: 10 – 12 Hours (Based on An Average Of ~ 2 Hours Per Document)

REFERENCES:

1. NRC-approved CSP for a facility designated by your supervisor
2. 10 CFR 50.54(p)
3. 10 CFR 73.54(c)(1)
4. Regulatory Guide 5.71, "Cybersecurity Programs for Nuclear Facilities", Appendices B and C (ML090340159)
5. Regulatory Guide 5.69, "Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements," (Safeguards Information)
6. NEI 13-10, "Cybersecurity Controls Assessments," Rev. 7 (ML21342A203)

EVALUATION CRITERIA: At the Completion of This Activity, You Should Be Able To:

1. Discuss the general content of the applicable portions of the CSP related to cybersecurity controls and their regulatory basis.
2. Discuss specific areas where you would expect the licensee to have developed more detailed implementing procedures. For example:

    a. Documented basis and implementation of alternate security controls

  b. Documentation of the basis and other processes the licensee takes credit for to meet the requirements in the CSP

3. Discuss the concept of defense-in-depth to protect a CDA

4. Discuss how the concept of defense-in-depth drives the requirements for implementing alternate controls

5. Describe a sample of controls listed in the licensee's CSP. At least one technical, operational, and management cybersecurity controls should be reviewed.

TASKS:

1. Obtain a copy of the CSP for the assigned facility and become familiar with its contents

2. Evaluate security controls that are provided in the CSP.

3. Obtain a copy of NUREG/CR-7141 on security controls. Describe and categorize the cybersecurity controls implementation process based upon a sample of CDAs provided by senior inspector or branch chief.

4. Describe a sample of controls listed in the licensee's CSP.

5. Read and understand the CSP, guidance documents, and any other supporting documentation necessary to be able to discuss the topics identified in the Evaluation Criteria section, above.

6. Review NEI 13-10, "Cybersecurity Controls Assessments," Rev. 7, Appendix F, (ML21342A203)

7. Discuss the answers to the questions and tasks listed under the evaluation criteria section of this study guide with your supervisor or a C-14 qualified inspector.

DOCUMENTATION: Cybersecurity Inspector Proficiency Level Qualification Signature Card Item ISA-CS-5.

Cybersecurity Inspector Individual Study Activities

(ISA-CS-6) Cybersecurity Significance Determination Process and Documenting Findings

PURPOSE:

The Significance Determination Process (SDP), as described in Appendix E of Inspection Manual Chapter (IMC) 0609, Appendix E, Part IV aids NRC inspectors and staff in objectively determining the significance of inspection findings, including categorization of individual findings into one of four response bands. The purpose of this activity is for you to gain the requisite knowledge, understanding, and practical ability to be able to use the cybersecurity SDP to determine the significance of cybersecurity-related inspection findings.

COMPETENCY AREAS: Regulatory Framework Technical Area Expertise
Inspection Problem Analysis Assessment And Enforcement

LEVEL OF EFFORT: 12 – 14 Hours (Based on an average of ~ 2 hours per document)

REFERENCES:

1. NRC IMC-0305, “Operating Reactor Assessment Program”
2. NRC IMC 2201, “Security and Safeguards Inspection Program for Commercial Power Reactors”
3. NRC IMC-0609, “Significance Determination Process”
4. IMC-0609, Appendix E, Part IV, “Cybersecurity Significance Determination Process for Power Reactors”
5. NRC IMC-0612, “Issue Screening”
6. NEI 08-09, Rev. 6, Addendum 2 “Cyber Attack Detection, Response and Elimination” (ML17236A268)
7. Security Issues Forum Charter (ML091620477)
8. 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks”

EVALUATION CRITERIA: At the completion of this activity, you should be able to:

1. Disposition findings and non-compliance using IMC-0612, “Issue Screening”
2. Evaluate findings using Appendix E of NRC IMC-0609 and assign findings, using the cybersecurity SDP flow chart logic, into the correct performance bands: green, white, yellow, or red.

TASKS:

1. Review the IMC-0609, Appendix E, Part IV in its entirety and understand the use of the Baseline SDP flow chart logic diagrams.

2. Obtain from your supervisor or a senior cybersecurity inspector several dispositioned cybersecurity inspection findings (including one related to physical security) that have been evaluated with the cybersecurity SDP), and perform the following:

    a. Using IMC-0612, determine whether each of the issues have sufficient significance to warrant SDP analysis or documentation on an inspection report.

    b. Using the Baseline Security SDP flow chart logic of IMC-0609, Appendix E, determine an outcome as to the security significance category (green, white, yellow, red) for each of the above issues.

    c. Compare your conclusions with those provided by the actual findings or case studies.

    d. Discuss your results with your supervisor or a senior cybersecurity inspector.

3. Given a violation of regulatory requirements and the enforcement policy and guidance, write the analysis and enforcement sections for a finding, and a non-cited violation. (This includes restating requirements, “contrary to” statement, and severity level.) Obtain recent inspection reports issued by your region and/or reports that provide insights on security control or alternate control improper implementation. Include an assessment for the applicable safety culture cross-cutting aspect.

4. Attend a SIF meeting to understand the objectives of this process

5. Discuss the answers to the questions and tasks listed under the evaluation criteria section of this study guide with your supervisor or a C-14 qualified inspector.

DOCUMENTATION: Cybersecurity Inspector Proficiency Level Qualification Signature Card Item ISA-CS-6.

Cybersecurity Inspector On-the-Job Activities

(OJT-CS-1) Identifying Assets Subject to the Cybersecurity Rule

PURPOSE:

Nuclear Reactor facilities are required to identify digital assets subject to the requirements of 10 CFR 73.54. Licensees are required to develop and implement a method or methodology to identify digital assets known as critical digital assets (CDAs) for protection. Improper implementation of this cybersecurity program element reduces the licensee's ability to identify and protect CDAs. It is vital that the inspector obtain the necessary documentation to review to make a risk-informed and knowledgeable judgment regarding the effectiveness of the licensee's assets scoping method or methodology. These skills are best learned by participating in a cybersecurity inspection. Upon completion of this guide, you will be able to identify information sources that could be used to assess the adequacy and appropriateness of CDA scoping.

COMPETENCY AREA: Inspection

LEVEL OF EFFORT: 6 – 8 Hours

REFERENCES:

1. 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks"
2. NEI 10-04, "Identifying Systems and Assets Subject to the Cybersecurity Rule", Rev. 3 (ML21342A168)
3. Regulatory Guide 5.71, "Cybersecurity Programs for Nuclear Facilities", Appendices B and C (ML090340159)
4. NEI 08-09, Rev. 6, Addendum 1, "Cybersecurity Plan for Nuclear Power Reactors" (ML17079A423)
5. NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Emergency Preparedness Functions," (ML20129J981, ML20126G492).
6. NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Safety Related and Important-to-Safety Functions," (ML20223A256, ML20199M368)
7. NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Balance-of-Plant (BOP) Functions," (ML20209A442, ML20205L604)
8. NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Physical Security Functions," (ML21140A140, ML21155A216)

9. Licensee implementing procedures describing the scoping methodology. Examples of licensee’s policies and procedures are:

   (a) Cybersecurity program policy

   (b) CDA scoping methodology

   (c) Licensee’s critical system (CS)/critical digital asset (CDA) inventory list

EVALUATION CRITERIA: At the completion of this activity, you will be able to:

1. Determine CDAs that are required by regulations to be protected from cyberattacks.
2. Describe how you would verify the effectiveness of CDAs scoping.
3. Name which reference documents you would consult to verify that CDAs required to be protected were scoped, addressed, and maintained in accordance with commitments.
4. Describe how you would verify cybersecurity organization activities to evaluate the effectiveness of CDA scoping.

TASKS:

1. Participate as an observer in a cybersecurity inspection. Shadow a qualified inspector and participate in inspection activities such as walkdowns, interviews, briefings, and evaluate the licensee’s cybersecurity program to ensure 10 CFR 73.54 requirements are met.
2. Review licensee documents which describe the process for scoping CDAs and review the licensee’s network architecture diagrams.
3. Demonstrate the ability to review and evaluate a licensee’s overall CDAs scoping process. This should include an evaluation of the licensee’s methodology by assessing and determining if the results of the scoping methodology do not have any gaps.

DOCUMENTATION: Cybersecurity Inspector Proficiency Level Qualification Signature Card Item OJT-CS-1.

Cybersecurity Inspector On-the-Job Activities

(OJT-CS-2) Cybersecurity Controls and Protective Strategy

PURPOSE:

Nuclear facilities are required to implement cybersecurity controls in accordance with 10 CFR 73.54(c)(1), and to apply and maintain defense-in-depth protective strategies in accordance with 10 CFR 73.54(c)(2). Failure of these elements of the cybersecurity program compromises the ability to protect CDAs. It is vital that the inspector obtain the necessary information to make an informed and knowledgeable judgment regarding the implementation and effectiveness of security controls and the protective strategy. Upon completion of this guide, you will be able to identify information sources that could be used to assess the adequacy and appropriateness of countermeasures and defense-in-depth strategy to protect CDAs.

COMPETENCY AREA: Inspection

LEVEL OF EFFORT: 16 hours

REFERENCES:

1. NRC-approved CSP for a facility
2. Licensee Implementing Procedures
3. 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks”
4. NEI 13-10, “Cybersecurity Controls Assessments,” Rev. 7 (ML21342A203)

EVALUATION CRITERIA: At the completion of the activity, you should be able to:

1. Describe and categorize, according to the CSP and implementing procedures, cybersecurity controls that are required by regulations to be addressed and maintained.
2. Explain how you would verify the effectiveness and applicability of cybersecurity controls.
3. Discuss licensee’s CDAs and their implementation of its defensive strategy to protect these assets.
4. Name which reference documents you would consult to verify that cybersecurity controls were addressed and maintained in accordance with commitments.
5. Describe how you would verify cybersecurity organization activities to evaluate the effectiveness of cybersecurity controls.

6. Discuss the licensee’s protective strategy and its characteristics to include incident response, contingency planning, and recovery actions.

7. Demonstrate the ability to review and evaluate a licensee’s overall protective strategy. This should include an evaluation of the licensee’s abilities to respond to, mitigate the consequences of, and recover from a cyberattack by focusing on the licensee’s protective strategies implemented.

TASKS:

1. Review the licensee’s NRC-approved CSP to ascertain the cybersecurity controls to be addressed and maintained and verify that the controls are in conformance with regulatory requirements.

2. While observing an inspection, get with the experienced inspector or the contractor support staff to understand the licensee’s security control implementation method. If the licensee is using NEI 13-10, “Security Control Implementation,” discuss and understand Direct and Non-Direct CDAs and how NEI 13-10 is implemented.

3. While observing an inspection get with the experienced inspector or the contractor support staff to understand how to assess and evaluate CDA security control implementation to ensure the licensee has adequately protected the asset (for example, inspect group policy objects (GPOs) for hardening, VMs implementation and assessment). Ascertain whether the controls are adequate and appropriately configured for their intended function.

4. Interview selected licensee cybersecurity personnel to determine their duties and responsibilities related to cybersecurity controls testing, maintenance, incident response, contingency planning, recovery actions, and oversight.

5. Compare your evaluation results regarding cybersecurity control effectiveness against those reached by the licensee. If there are differences, discuss the differences with your supervisor or a senior cybersecurity inspector to understand why the difference exists

DOCUMENTATION: Cybersecurity Inspector Proficiency Level Qualification Signature Card Item OJT-CS-2.

Form 1: Regional/Headquarters Cybersecurity Inspector Technical Proficiency Level Signature Card and Certification

Inspector's Name:	Employee Initials / Date	Supervisor's Signature / Date
Required Training Courses		
Introduction to Cybersecurity Inspection		
Advanced Cybersecurity Inspection		
Individual Study Activities		
(ISA-CS-1) Code of Federal Regulations (CFRs)		
(ISA-CS-2) Cybersecurity Plan and Changes to the CSP		
(ISA-CS-3) Identifying Assets Subject to the Cybersecurity Rule		
(ISA-CS-4) Licensee Protective Strategies		
(ISA-CS-5) Cybersecurity Controls		
(ISA-CS-6) Cybersecurity Significance Determination Process (SDP)		
On-the-Job Activities		
(OJT-CS-1) Identifying Assets Subject to the Cybersecurity Rule		
(OJT-CS-2) Cybersecurity Controls and Protective Strategy		

Supervisor's signature indicates successful completion of all required courses and activities listed in this journal and readiness to appear before the Oral Board, if applicable.

Supervisor's Signature: ________________________________ Date: ____________

Form 2: Regional/Headquarters Cybersecurity Inspector Technical Proficiency Level Equivalency Justification

Required Training Courses	
Inspector Name:	Identify equivalent training and experience for which the inspector is to be given credit.
Introduction to Cybersecurity Inspection	
Advanced Cybersecurity Inspection	
Individual Study Activities	
(ISA-CS-1) Code of Federal Regulations (CFRs)	
(ISA-CS-2) Cybersecurity Plan and Changes to the CSP	
(ISA-CS-3) Identifying Assets Subject to the Cybersecurity Rule	
(ISA-CS-4) Licensee Protective Strategies	
(ISA-CS-5) Cybersecurity Controls	
(ISA-CS-6) Cybersecurity Significance Determination Process (SDP)	

Form 2: Regional/Headquarters Cybersecurity Inspector Technical Proficiency Level Equivalency Justification

On-the-Job Activities	
(OJT-CS-1) Identifying Assets Subject to the Cybersecurity Rule	
(OJT-CS-2) Cybersecurity Controls and Protective Strategy	

Supervisor's Recommendation: ______________________________ Date: ______________

Division Director's Approval: _________________________________ Date: ______________

Copies to: Inspector and official training file

END

Exhibit 1: Risk Management Framework

RG 5.71 describes a regulatory position that promotes a protective strategy consisting of an architecture that achieves defense-in-depth by implementing the necessary security controls based on standards provided in NIST SP 800-53 and NIST SP 800-82, “Guide to Industrial Control Systems Security,” dated September 29, 2008 (Ref. 13). NIST SP 800-53 and SP 800-82 are based on well-understood cyber threats, risks, and vulnerabilities, coupled with equally well-understood countermeasures and protective techniques. Furthermore, NIST developed SP 800-82 for use within industrial control system (ICS) environments, including common ICS environments in which the information technology (IT)/ICS convergence has created the need to consider application of these security controls. The cyber rule is based on the NIST Risk Management Framework (RMF) which provides a process that integrates different activities to protect digital computers, communications systems, and networks and therefore, it is important to understand the basic principles of the NIST RMF. The RMF encompasses six activities:

1. Categorize Systems
2. Select Cybersecurity Controls
3. Implement Cybersecurity Controls
4. Assessment of Cybersecurity Controls
5. Authorize Systems to Operate
6. Monitor Cybersecurity Control Implementation and Risks to Systems

This requirement may be met by taking a course (online or classroom) specifically designed to apply the NIST RMF process, typically offered by a third party, or by taking various cybersecurity courses (online or classroom) that provide knowledge about each of the six activities of the RMF, or by possessing an information technology (IT) certification(s) that fulfill the six RMF activities.

If taking various cybersecurity courses or if taking credit for a certification, identify equivalent training or courses taken that meet the curriculum below (see Table 1).

Table 1: Risk Management Framework Technical Proficiency Level Equivalency Justification

Inspector Name		
RMF Activity	RMF Activities Elements	Equivalent Course/Training/Certification
Categorize the System	System characteristics documentation	
	Security categorization of the system	
	Categorization decision reviewed/approved by authorizing official	
Security Control Selection	Control baseline selected and tailored	
	Controls allocated to specific system/components	
	System level continuous monitoring strategy	
Security Control Implementation	Controls specified in security plan implemented	
	Security plans updated to reflect controls as implemented	
Security Control Assessment	Assessment plan, strategy, developed and approved	
	Assessment of security controls conducted per the plan	
	Assessment results report and remediation actions	
Authorization of Systems to Operate	Cybersecurity plan, system security plan, assessment report, and plan of action review	
	Residual risk determined	
Cybersecurity Control Monitoring	System and environment monitored in accordance with monitoring strategy	
	Ongoing assessments of security controls effectiveness	
	Process in place to report security posture to management	
	Ensuring continuous ongoing monitoring activities	

Supervisor’s signature indicates successful completion of all required courses and activities listed in this journal and readiness to appear before the Oral Board, if applicable.

Supervisor’s Signature: _________________________________ Date: ____________

Exhibit 2: Table 2: Cybersecurity Frequently Asked Questions

SFAQ #	Title	Date	ADAMS Accession #	ADAMS Package #
10-05	IT Functions for the Critical Group	10/15/2010	ML102100070	ML102100087
10-06	Classification of Cybersecurity Information	10/28/2010	ML102090633	ML102090660
11-04	Target Set Review Documentation	03/08/2012	ML110960419	ML110960442
11-10	Clarification of CSP Implementation Schedule MS6	03/21/2012	ML112911454	ML112911443
12-05	NEI 03-12, Revision 7 - Contingency Event #21	04/12/2012	ML12065A366	ML12065A362
12-17	Cybersecurity Milestone 1	04/08/2013	ML13098A153	ML13098A224
12-18	Cybersecurity Milestone 2	04/08/2013	ML13098A155	ML13098A224
12-19	Cybersecurity Milestone 3	04/08/2013	ML13098A157	ML13098A224
12-20	Cybersecurity Milestone 4	04/08/2013	ML13098A170	ML13098A224
12-21	Cybersecurity Milestone 5	01/11/2013	ML12331A131	ML12331A032
12-22	Cybersecurity Milestone 6	04/08/2013	ML13098A174	ML13098A224
12-23	Cybersecurity Milestone 7	04/08/2013	ML13098A177	ML13098A224
14-01	Digital Indicator, Revision 1	06/29/2015	ML15029A517	ML15029A524
14-02	Unauthorized Person	12/19/2016	ML16088A242	ML16088A231
16-01	Data Integrity	01/30/2017	ML16196A302	ML16196A264
16-02	Deterministic Devices	01/30/2017	ML16208A222	ML16208A101
16-03	Treatment of Digital Maintenance and Test Equipment	03/08/2017	ML16350A056	ML16350A059
16-04	Access Authorization / PADS	11/01/2016	ML16209A095	ML16209A076
16-05	Moving Data between Security Levels	03/07/2017	ML16351A469	ML16351A470
16-06	Communications Attack Pathways	05/08/2017	ML16351A504	ML16351A501
17-04	Access Authorization / Access Authorization Systems (incorporated in NEI 13-10 Rev 7)	01/22/2018	ML18030A535	ML18030A534

Attachment 1: Revision History for IMC 1245 Appendix C-14

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Form Accession Number (Pre-Decisional, Non-Public Information)
N/A	ML14233A585 08/03/15 CN 15-014	First issuance. New training and qualification requirements for Cybersecurity Inspectors. Four-year historical search for commitments was conducted and found none.	None	ML15182A014
N/A	ML22063A091 10/13/22 CN 22-022	Major revision to update initial training course, revised guidance, to incorporate new developed industry guidance accepted for use by the NRC, and to remove OUO-SRI marking since the contents of this journal is not sensitive information.	None	ML22063A041