WILLIAM R. GROSS
Director, Incident Preparedness

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8123
wrg@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

June 04, 2021

Ms. Shana Helton
Director, Division of Physical and Cyber Security Policy
Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: NRC Review of NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Security," Dated June 2021

Project Number: 689

Dear Ms. Helton:

By letter dated July 27, 2012,[1] the Nuclear Regulatory Commission (NRC) found NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, dated July 2012, be acceptable for use by licensees to identify critical digital systems and critical digital assets.

By letter dated September 7, 2017,[2] the NRC found NEI 13-10, "Cyber Security Control Assessments," Revision 6, dated August 2017, acceptable for use by licensees to address the security controls provided in their cyber security plans.

Lessons learned through the implementation of cyber security programs indicate that guidance improvements are necessary to enhance clarity, enable efficient and consistent program implementation and to support NRC oversight activities.

Accordingly, the Nuclear Energy Institute (NEI),[3] on behalf of its members, is submitting the attached white paper proposing changes to NEI 10-04 and NEI 13-10 for NRC review and approval. The attached white

[1] ADAMS Accession No. ML12194A532
[2] ADAMS Accession No. ML17240A002
[3] The Nuclear Energy Institute (NEI) is the organization responsible for establishing unified industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations and entities involved in the nuclear energy industry.

paper addresses the NRC and stakeholder comments provided at the public meeting on January 8, 2021 and in an NRC response letter dated March 22, 2021.[4] The attached white paper describes proposed changes to previously approved NEI guidance for identifying and protecting Security Critical Digital Assets. The changes are intended to improve the efficiency of licensee cyber security programs while maintaining program effectiveness to protect against cyber attacks, up to and including the design basis threat. The attached document provides a technical basis for the changes and provides a markup of the relevant changes made to NEI 10-04 and NEI 13-10. The markup does not include all minor editorial and conforming changes. All changes will be incorporated into future revisions of NEI 10-04 and NEI 13-10.

NEI requests that the NRC review and approve the NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Security Functions," by July 09, 2021. While each licensee must review changes to their Commission-approved Cyber Security Plan in accordance with the requirements of 10 CFR 50.54(p), NEI requests that the NRC's review confirm that the changes proposed in this white paper do not decrease the effectiveness of the cyber security plan provided in NEI 08-09. If any revisions to this document are desired, please include suggested wording and the technical data to support the proposed change(s).

NRC's July 27, 2012 letter identified two exceptions to NEI 10-04, Revision 2. Consistent with the NRC review and response to previous cyber security white papers, NEI recommends these exceptions be fully evaluated when NEI 10-04, Revision 3 is submitted for NRC approval.

If you have any questions or require additional information, please contact Richard Mogavero, at (202) 739-8174 or rm@nei.org, or me.

Sincerely,

William R. Gross
Attachment

c: Mr. James D. Beardsley, NSIR/CSD, NRC
NRC Document Control Desk

[4] ADAMS Accession No. ML21069A155

1 INTRODUCTION

1.1 PURPOSE

This white paper describes proposed changes to NEI guidance for identifying and protecting Security Critical Digital Assets (CDAs). The changes are intended to improve the efficiency of licensee cyber security programs while maintaining program effectiveness to protect against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1, "Purpose and scope." The described changes affect and will be incorporated into a future revision to:

- NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, dated July 2012; and
- NEI 13-10, "Cyber Security Control Assessments," Revision 6, dated August 2017.

1.2 BACKGROUND

Title 10 of the Code of Federal Regulations (CFR), Part 73, "Physical Protection of Plants and Materials," 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," requires power reactor licensees to provide assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1, "Purpose and scope." Through implementation of the cyber security plans and programs required by 10 CFR 73.54, the industry has identified several lessons learned that warrant revisions to the guidance in NEI 10-04, Revision 2, and NEI 13-10, Revision 6. As such, this white paper describes proposed changes to NEI 10-04, Revision 2 and NEI 13-10, Revision 6, that would support more efficient performance of cyber security program activities and oversight, and promote consistent implementation of the requirements of 10 CFR 73.54 without compromising program efficacy.

2 DISCUSSION

As required by 10 CFR 73.54(a)(1)(ii) digital computer and communications systems and networks associated with security functions must be protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1. NEI 10-04 section 2.2, "Security Systems," documents the interface and integration of cyber security and physical security programs required to satisfy the physical protection program performance objectives of 10 CFR 73.55(b). 10 CFR 73.55(b)(3) requires that the physical protection program be designed to prevent significant core damage and spent fuel sabotage; that the program ensures that the capabilities to detect, assess, interdict, and neutralize threats up to and including the design basis threat of radiological sabotage as stated in 10 CFR 73.1, are maintained at all times; and that the program provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure the effectiveness of the physical protection program.

Industry experience and lessons learned from inspection activities have identified the need to enhance clarity related to the identification and protections of critical digital assets (CDAs) associated with security functions. These improvements are primarily needed to address the

following areas:

- Access Authorization (AA) – Classification and security controls for digital assets used to facilitate the implementation of the access authorization program as clarified in Security Frequency Asked Question (SFAQ) 17-04, "Access Authorization / Access Authorization Systems."
- Security Support Systems and Equipment – Security support systems, such as heating, ventilation and cooling (HVAC) systems, used to provide personnel comfort and equipment cooling for CDAs located in Central and Secondary Alarm Stations.
- Digital Security Tools – Tools and security personnel aids (e.g., firearm scopes, distance range finders, etc.) used in the course of security operations which, if compromised, would not adversely impact security functions.

3 COMPLIANCE WITH REGULATORY REQUIREMENTS

10 CFR 73.54(a)(1)(ii) and (iv) require that licensees protect against cyber attacks for those digital computer and communication systems and networks associated with security functions and support systems and equipment which, if compromised, would adversely impact SSEP (Safety-Related and Important-to-Safety, Security, and Emergency Preparedness) functions.

10 CFR 73.54(a)(2) requires in part licensees protect the systems and networks identified in paragraph (a)(1) from cyber attacks that would adversely impact the integrity or confidentiality of data and/or software.

10 CFR 73.54(b)(1) requires that licensees analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks to satisfy 10 CFR 73.54(a).

10 CFR 73.54(c)(1) requires the cyber security program must be designed to implement security controls to protect the assets identified by paragraph (b)(1) from cyber attacks.

10 CFR 73.55(b)(3) requires that the physical protection program must be designed to prevent significant core damage and spent fuel sabotage. Specifically, the program must:

(i) Ensure that the capabilities to detect, assess, interdict, and neutralize threats up to and including the design basis threat of radiological sabotage as stated in 10 CFR73.1, are maintained at all times.
(ii) Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure the effectiveness of the physical protection program.

10 CFR 73.56 includes the following two (2) regulatory requirements for Access Authorization systems:

10 CFR 73.56(m), "*Protection of information"* requires licensees establish and maintain a system of files and procedures to ensure personal information is not disclosed to unauthorized persons.

10 CFR 73.56(o), "*Records"* requires the method used to create electronic records prevents unauthorized access to the records and prevents the alteration of any archived data once it has been committed to storage.

Consistent with 10 CFR 73.54(a), 10 CFR 73.54(b), and the Cyber Security Plan (CSP), licensees are required to perform an analysis and determine those digital assets that, if compromised, would adversely impact safety, security and emergency preparedness functions and thus require protection. The analysis determines the assets that need to be protected and the applicable security controls that need to be addressed to provide assurance of adequate protection against cyber attacks.

Among the systems and equipment required to implement the physical protection program requirements in 10 CFR 73.55, digital assets used to facilitate the implementation of the Access Authorization (AA) program must be analyzed. Paragraphs 10 CFR 73.56(m) and (o) require licensees ensure the confidentiality and integrity of the AA system data. AA digital assets, software, and the data contained within those assets and software, must be evaluated as part of the 10 CFR 73.54(b)(1) analysis and, where necessary, protection be provided. Specific guidance is provided in the "AA System CDA Security Controls" section of this document.

10 CFR 73.54(b)(2) requires licensees establish, implement, and maintain a cyber security program for the protection of the assets identified in 10 CFR 73.54(b)(1).

With the incorporation of the proposed changes described in this document, a cyber security plan and program would ensure that:

a) Digital assets associated with security functions, and their respective support systems and equipment, described in 10 CFR 73.54(a)(1)(iii) and (iv), are analyzed as required by 10 CFR 73.54(b)(1).
b) Where the analysis determines that a cyber attack would adversely impact security functions, those digital assets would be protected against cyber attacks as required by 10 CFR 73.54(b)(2).

Implementation by a licensee of the changes discussed in this white paper will not decrease the effectiveness of a cyber security plan or affect compliance with the requirements of 10 CFR 73.54,[1] and the resulting cyber security program will protect digital computer and communication systems and networks against cyber attacks, up to and including the design basisthreat as described in 10 CFR73.1. The program will remain capable of protecting digital computer and communication systems and networks associated with security functions and support systems and equipment which, if compromised, would adversely impact security functions. The recommended changes of this document provide additional guidance and clarity. The changes support consistent industry implementation and regulatory oversight for scoping select digital assets associated with security functions, support systems and equipment which, if compromised, would adversely impact security functions.

In summary, it is expected that a licensee's evaluation of necessary changes to their Security

[1] This conclusion notwithstanding, depending upon site-specific security plan contents, a licensee may need to confirm this assessment through performance of a change evaluation in accordance with 10 CFR 50.54(p).

Plans would likely conclude:

- The change does not affect compliance with any regulatory requirement.
- The change does not decrease the effectiveness of the Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and/or Cyber Security Plan.
- The change does not decrease the overall capability of Cyber Security program to adequately protect against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1.

4 PROPOSED GUIDANCE DOCUMENT CHANGES

NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, provides guidance for determining whether a system and associated digital assets are subject to the requirements of 10 CFR 73.54. Licensees must analyze security systems and equipment, including support systems and equipment, described in 10 CFR 73.55. This analysis must include the digital systems and equipment used to facilitate the implementation of security programs specified in 10 CFR 73.55, for example, the Access Authorization program. This analysis would identify digital assets that must be protected against a cyber attack. Licensees must protect those digital assets that, if compromised, would adversely impact security functions. To address the changes described in section 2, "Discussion" of this paper, the following NEI 10-04 Rev. 2 sections require changes:

- Section 2.2 Security Systems (pages 5-7)
- Section 2.4 Support Systems and Equipment (page 16)
- Section 4 Methodology for Identifying and Classifying Plant Systems (page 20)
- Section 5 Methodology for Identifying Critical Digital Assets (pages 22-23)

NEI 13-10, "Cyber Security Control Assessments" Revision 6, provides guidance for addressing cyber security controls for CDAs consistent with the methodology described in section 3.1.6 of the Cyber Security Plan. The following NEI 13-10 Rev. 6 sections require changes:

- Add new section 7, "Access Authorization Assessment and Protections".

4.1 PROPOSED NEI 10-04 CHANGES

NEI 10-04 Rev. 2 section 2.2, "Security Systems," included a reference to Personnel Access Data System (PADS) System Administrator Bulletin 2012-02 to address NRC concerns regarding access authorization (AA) system data confidentiality and integrity concerns. Additional concerns were documented during licensee inspections that included not only PADS, but other AA systems and associated licensee processes.

Based upon current NRC and industry alignment as documented in SFAQ 17-04, "Access Authorization / Access Authorization Systems," NEI 10-04 Rev. 2 is being revised to provide licensees clear and consistent guidance to ensure access control functions are not adversely impacted by cyber attacks on AA systems. The revised guidance ensures AA systems are

adequately evaluated and protected in a manner consistent with the clarifications documented in SFAQ 17-04, "Access Authorization/Access Authorization Systems."

Additional guidance is recommended to section 2.2 to provide clarity for the screening and scoping of security support systems and digital tools and personnel aids.

Section 2.2 Security Systems

1. Insert the following paragraph after paragraph # 2:

   In the implementation of the licensee's protective strategy, security officers may use digital technologies, such as firearm scopes and distance range finders. Licensees must analyze these devices but need not classify them as CDAs if the licensee analysis demonstrates that a cyber attack on the device cannot adversely impact an SSEP function.

2. Delete the following text:

   ~~Additional requirements in 10 CFR 73.55 require licensees to, in part:~~

   ~~a) Establish, maintain, and implement a performance evaluation program;~~
   ~~b) Establish, maintain, and implement an access authorization program;~~
   ~~c) Establish, maintain, and implement an insider mitigation program; and~~
   ~~d) Use the site corrective action program to track, trend, correct and prevent recurrence of failures and deficiencies.~~

   ~~Licensees may use digital computing systems to facilitate the implementation of these other requirements in 10 CFR 73.55. These systems, however, are not a part of the onsite physical protection system, are not associated with the capability to detect, assess, interdict, and neutralize threats up to and including the design basis threat of radiological sabotage as stated in 10 CFR 73.1, and the failure or compromise of these information systems cannot lead to a radiological sabotage event. Accordingly, these systems are not within the scope of 10 CFR 73.54.~~

   ~~During the NRC's review of NEI 10-04 for endorsement, the NRC staff raised a concern regarding the cyber security status of the industry data-sharing mechanism, currently provided by the Personnel Access Data System (PADS). The concern regards a specific case for reinstatement of Unescorted Access Authorization/Unescorted Access (UAA/UA).~~

   ~~Subsequently, NEI issued System Administrator Bulletin 2012-02 to address the issue raised by the staff. The Bulletin requires the licensee companies to integrate actions consistent with the guidance in the Bulletin into their site procedures. These actions are designed to ensure that the PADS is not the sole source of information for making UAA/UA determinations. The guidance in the Bulletin will be incorporated into Revision 4, NEI 03-01, "Nuclear Power Plant Access Authorization Program." These actions ensure that the compromise of the PADS system would have no adverse impact on the access authorization program and, as the result, the PADS system remains out of the~~

~~scope of 10 CFR 73.54.~~

3. Replace the text above with the following:

   Consistent with 10 CFR 73.54(a), 10 CFR 73.54(b), and their CSP, licensees are required to perform an analysis and determine those digital assets that, if compromised, would cause an adverse impact to SSEP functions and thus require protection. 10 CFR 73.55(b)(7) requires licensees maintain an Access Authorization program in accordance with 10 CFR 73.56. Paragraphs 10 CFR 73.56(m) and (o) require licensees ensure the confidentiality and integrity of Access Authorization (AA) system data. For these reasons, AA digital assets and/or software, and the data contained within those assets and/or software, must also be analyzed in accordance with 10 CFR 73.54(b)(1). NEI 13-10 provides additional guidance licensees may use when analyzing AA digital assets.

4. Remove the following before "Security Systems":

   ~~Assets that must be analyzed in accordance with the requirements of 10 CFR 73.54(b)(1) include but are not limited to those associated with:~~

   Replace the text with:

   The following are the security functions that must be protected against adverse impacts from the radiological sabotage cyber attack.
   1. Physical barriers
   2. Access controls
   3. Search programs
   4. Detection and assessment systems
   5. Communication requirements
   6. Response requirements

5. Removed the words:
   ~~Security Systems~~

   Replaced the text with:

   Example list of the systems to be evaluated but not limited to:

6. Removed headers regarding the example list of systems to be evaluated.

   The following text was added:

   3. Access Authorization (73.56)

Section 2.4 Support Systems and Equipment

1. Insert the following text after paragraph #3:

Licensees are required to identify and evaluate those digital assets associated with security support systems whose failure or compromise as the result of a cyber attack would result in an adverse impact to an SSEP function. While implementing the licensee's protective strategy, security officers may use digital technologies. Examples include but are not limited to: officer efficiency aids, firearm scopes, and distance range finders. These devices should be analyzed but need not be classified as CDAs if licensee analysis demonstrates that a cyber attack on the device cannot adversely impact an SSEP function. Please see Section 5 of NEI 10-04 for considerations in determining if a digital asset is a CDA.

Section 4 Methodology for Identifying and Classifying Plant Systems

1. Delete all content under 'Security' beginning, "Is the system associated with…" through the end of the section.

Section 5 Methodology for Identifying Critical Digital Assets

1. Clarify (c) under 'A digital device should be identified…'with the following language:

   c) Support functions, (e.g., primary or back-up power, HVAC, fire protection, etc.) ~~whose~~ and, through analysis, demonstrate a compromise would adversely impact a SSEP function;

2. The following will be added as part of an updated Section 5 in the next revision (Revision 3) to NEI 10-04. Note in Revision 3, Section 5 will have specific headers for EP, BOP, SR/ITS, and Security. The criteria below will only be used to screen security support system digital assets and identify security CDAs. These criteria will not be used to screen and identify equipment that performs safety-related, important-to-safety, or emergency preparedness functions

   With respect to security support systems, this guidance provides a process for determining if an alternate means exists to maintain the capability of performing the security function in the event of a cyber attack. If the security support system only supports a security function, there is an alternate means to support the security function, and the alternate means is documented in plant procedures and trained on, the analysis could show the digital asset is not a CDA. Specifically, plants should address the following questions in the analysis:

   - Does the digital asset only perform a security support function?
   - Can the support function the support system provides be addressed by an alternate means?
   - Is there a means to identify that the digital asset performing the security support function is no longer functioning?
   - Is there sufficient time to implement the alternate means of performing the support function, before the failure or compromise impacts the security function?
   - Is the alternate means captured in plant procedures and trained on?

   If the answer to all above questions are yes, then the analysis should be documented in the digital asset analysis and the security support system digital asset is not a CDA.

4.2 PROPOSED NEI 13-10 CHANGES

NEI 13-10, "Cyber Security Control Assessments" Revision 6, provides guidance for addressing cyber security controls for CDAs consistent with the methodology described in section 3.1.6 of the Cyber Security Plan. NEI 13-10 Rev. 6 includes guidance for performing a consequence analysis to determine if a security support system or device meets the criteria to support classification as an indirect CDA. NEI 13-10 includes an example for security radios that demonstrates how to properly perform a consequence analysis that documents how 10 CFR 73.55(j) communications functions are not adversely impacted by the potential compromise or failure of security radios. The current NEI 13-10 Rev. 6 guidance is adequate for performing a consequence analysis for security support systems, digital tools, and personnel aids to determine the level of protection required for these assets. Existing NEI 13-10 guidance does not exist for performing an access authorization data confidentiality and integrity analysis nor does guidance exist to provide clarifying options for how to protect AA system data. Specifically, for precluding an unauthorized individual from obtaining unescorted access (UA) into the protected or vital areas of an NPP and impacting access control functions.

NEI 13-10 is being revised to communicate the need for licensees to perform an analysis that considers current requirements to ensure the confidentiality, integrity, and availability of AA systems and data [10 CFR 73.54(a)(2)], personal information is not disclosed to unauthorized persons [10 CFR 73.56(m)], prevent unauthorized access to AA records, ensure AA records cannot be altered once committed to storage [10 CFR 73.56(o)], and to incorporate the guidance agreed upon in SFAQ 16-04 and SFAQ 17-04.

SFAQ 16-04 documented that NEI PADS System Administrative Bulletin 2016-07, "Administrative Controls for PADS Data," provided acceptable levels of assurance to maintain access request integrity. Specifically, the Bulletin noted that it is the responsibility of the licensee's designated requestor to verify that the personnel for whom they are requesting UAA/UA (Unescorted Access Authorization / Unescorted Access) have a need for access. The four methods discussed are: (1) In Person; (2) A Signed Document; (3) Via Telephone Conversation; and (4) Digitally Signed E-mail Message.

SFAQ 17-04 documented that AA digital assets and/or software, and the data contained within those assets and/or software, must also be evaluated as part of the 10 CFR 73.54(b) analysis. The SFAQ further describes three approaches:

1) AA digital assets that reside on lower security levels of the site's network topology (e.g., levels not protected by a deterministic one-way device) would be identified as CDAs and in order to demonstrate adequate protection of these CDAs, licensees can take credit for (1) cyber security measures implemented under their corporate IT's cyber security program; (2) cyber security measures implemented under existing programs; and (3) alternative measures that comply with Section 3.1.6 of the CSP. At a minimum, licensees would have to address D1.16, D1.22, D3.6, D3.7, D3.9, D3.10, D3.11, D3.12, D3.19, D4.1, and D4.2.

2) AA digital asset that reside on higher security levels of the site's network topology (e.g., levels behind a deterministic one-way device) must be protected in a manner that is compliant with their CSP.

3) Alternate Method – licensees may use digital assets to transfer AA system data, but would perform a secondary non-digital verification of the data prior to it being used in the AA function (e.g., manual verification of AA system data prior to its entry into the PSCS). In these situations, the 10 CFR 73.54 analysis would determine that these digital assets are not CDAs because the digital assets, if compromised, would not result in modified information being entered into the PSCS.

The new Section 7 of NEI-13-10 is intended to document the information from these SFAQs and provide examples of implementation.

Insert the following new information as Section 7:

Section 7: Access Authorization Assessment and Protections

Licensees are required to evaluate digital assets used in the Access Authorization program in accordance with 10 CFR 73.54(b)(1), 10 CFR 73.55(b)(3), and 10 CFR 73.55(b)(7). Licensees are also required to ensure personal information is not disclosed to unauthorized persons [10 CFR 73.56(m)] and prevent unauthorized access to AA records and ensure AA records cannot be altered once committed to storage [10 CFR 73.56(o)]. This section provides licensees guidance on performing an analysis to identify digital assets that store and transmit AA data. Protection of AA data to prevent an adverse impact to security function may rely on manual data verification and/or cyber security controls. The purpose of this manual verification prior to entering elements of AA system data into the PSCS, is to ensure the confidentiality, integrity, and availability of data used to perform AA functions when digital assets storing and transmitting AA data are not required to be classified as critical digital assets.

Digital information systems and applications that store or transmit personally-identifiable information (PII) which is defined in NEI 03-01 (Nuclear Power Plant Access Authorization Program) as all information, unique to an individual, that is collected or developed during the implementation of the UAA or FFD program requirements, must be identified as digital AA assets. Licensee analysis of digital AA assets, used to facilitate the implementation of the AA program, will determine the security controls needed to comply with 10 CFR 73.54, while still meeting 10 CFR 73.55(b)(7), 10 CFR 73.56(m) and 10 CFR 73.56(o) requirements. The following information provides guidance for performing an AA analysis to addresses options for securing and protecting AA system data confidentiality, integrity, and availability.

1) Option 1 - AA digital assets reside on lower security levels (e.g., levels not protected by a deterministic one-way device) and are documented as CDAs.

In this option, licensees would classify the AA digital assets as CDAs and in order to demonstrate adequate protection, licensees can take credit for (1) cyber security measures implemented under their corporate IT's cyber security program; (2) cyber security

measures implemented under existing programs; and (3) alternative measures that comply with Section 3.1.6 of the CSP. At a minimum, licensees would have to address:

- D1.16: "Open/Insecure" Protocol Restrictions
- D1.22: Use of External Systems
- D3.6: Transmission Integrity
- D3.7: Transmission Confidentiality
- D3.9: Cryptographic Key Establishment and Management
- D3.10: Unauthorized Remote Activation of Services
- D3.11: Transmission of Security Parameters
- D3.12: Public Key Infrastructure Certificates
- D3.19: Confidentiality of Information at Rest
- D4.1: Identification and Authentication Policies and Procedures
- D4.2: User Identification and Authentication

2) Option 2 – AA digital assets reside on higher security levels (e.g., levels protected by a deterministic one-way device) and are documented as CDAs.

AA assets classified as CDAs under this option must be protected in a manner compliant with a licensee's Cyber Security Plan.

3) Option 3 – Alternate Method: AA digital assets used for AA functions not identified as CDAs, but changes to these digital assets are analyzed and documented per licensee procedures/policies.

Licensees can comply with 10 CFR 73.54(b)(1), by addressing the 10 CFR 73.56(m), and 10 CFR 73.56(o) requirements and implementing one of the following alternatives:

a. Using only validated printed AA records. Use of this option requires that AA records with personal information be physically secured and access to those records must be limited to authorized personnel only.
b. Use a combination of printed and/or secured digital AA records to store and transmit AA records. Use of this option requires a combination of manual data confidentiality and integrity verification checks and cyber security controls to protect and secure AA data confidentiality and integrity.

The following provides additional guidance for these two alternatives.

(a) AA System Printed Record Controls:

Licensees would use only printed documents or copies to store and transmit AA data. In these situations, the analysis required by 10 CFR 73.54 would determine the AA digital assets are not CDAs. The use of printed documents ensures the confidentiality, integrity, and availability of data used to perform AA functions (e.g., entering data into the PSCS and 'access determinations'). Documents should be printed in a timely manner to ensure

records are not altered between the time verification takes place and when the individual's access is processed. While the AA digital assets are not classified as CDAs, licensees should document in their analysis how the 10 CFR 73.56(m) and 10 CFR 73.56(o) requirements are being addressed on these AA Assets.

Option 3 Examples

(a) Manual Method

- Request for access is submitted, the request becomes a source document.
- A Personal History Questionnaire (PHQ) is sent to the applicant, who returns the PHQ to the utility.
- The PHQ is verified to match the request data and printed.
- True Identity verification of the applicant during the completion of elements. UAA granted after validating completion of elements in source document.
- True Identity verification prior to badging with the printed source documents.
- Badge data is sent to Security.
- Security validates information with Reviewing Official prior to activating UA.
- UA information validation requires concurrence prior to activation in Physical Security Computer System.

(b) AA System Printed and Digital Records Controls:

Licensees may use a combination of printed records along with existing digital assets on their administrative (lower security levels) network or stand-alone network to store and transmit AA data. In these situations, the 10 CFR 73.54 analysis would determine that these digital assets are not CDAs because the digital assets, if compromised, would not result in modified information being entered into the PSCS. Licensees must analyze and document changes to AA digital assets, including changes to the cyber security controls applied to them. The analysis should also document how the 10 CFR 73.56(m) and 10 CFR 73.56(o) requirements are being addressed. Using configuration management processes, licensees must evaluate future changes made to the AA digital assets to ensure that those assets can continue to provide their protected AA function per licensee procedures/policies. The cyber security controls and manual data verification steps in the process ensure the confidentiality, integrity, and availability of data by addressing the subset of controls outlined in the Example 3 Options below, and performing a secondary verification on the subset of data that is input into the PSCS prior to it being used in the AA function (e.g., manual verification of AA system data prior to its entry into the PSCS, UA/UAA). In these situations, the 10 CFR 73.54 analysis would determine that these digital assets are not CDAs because the digital assets, if compromised, would not result in

modified information being used to perform access authorization system functions. The following examples provide guidance on acceptable implementation of this option:

Example 3.b.1 (Manual and Digital Method: Stand-Alone/Non-Internet Connected Computer)

- Request for access is submitted, the request becomes a source document or secured offline file.
- A PHQ is sent to the applicant, who returns the PHQ to the utility.
- The PHQ is verified to match the request data.
- All AA data and information are manually transferred to, with appropriate cyber security controls, and stored on a stand-alone or non-internet connected computer.
- The process must be analyzed and protected by addressing, at a minimum, the following cyber security controls:
    - D1.16: "Open/Insecure" Protocol Restrictions
    - D1.22: Use of External Systems
    - D3.6: Transmission Integrity
    - D3.7: Transmission Confidentiality
    - D3.9: Cryptographic Key Establishment and Management
    - D3.10: Unauthorized Remote Activation of Services
    - D3.11: Transmission of Security Parameters
    - D3.12: Public Key Infrastructure Certificates
    - D3.19: Confidentiality of Information at Rest
    - D4.1: Identification and Authentication Policies and Procedures
    - D4.2: User Identification and Authentication
- True Identity verification during the completion of elements. UAA granted after validating completion of elements in source document or secured offline file.
- True Identity verification prior to badging.
- Badge data is verified against previously provided digital records.
- Security validates information with Reviewing Official prior to activating UA.
- UA information validation requires concurrence prior to activation in Physical Security Computer System.

Example 3.b.2 (Manual and Digital Method: Systems Residing on Lower Security Levels with AA data Secured)

- Request for access is submitted, the request becomes a source document or digitally secured source file using cryptographical technologies that ensure data integrity.
- A PHQ is sent to the applicant, who returns the PHQ to the utility.
- The PHQ is verified to match the request data.
- All AA data and information are protected on the computer systems residing on lower security levels, addressing appropriate cyber security controls.
- The process must be analyzed and protected by addressing, at a minimum, the following cyber security controls:

  - D1.16: “Open/Insecure” Protocol Restrictions
  - D1.22: Use of External Systems
  - D3.6: Transmission Integrity
  - D3.7: Transmission Confidentiality
  - D3.9: Cryptographic Key Establishment and Management
  - D3.10: Unauthorized Remote Activation of Services
  - D3.11: Transmission of Security Parameters
  - D3.12: Public Key Infrastructure Certificates
  - D3.19: Confidentiality of Information at Rest
  - D4.1: Identification and Authentication Policies and Procedures
  - D4.2: User Identification and Authentication
- True Identity verification during the completion of elements. UAA granted after validating completion of elements in source document.
- True Identity verification prior to badging.
- Badge data verified against previously provided digital records.
- Security validates information with Reviewing Official prior to activating UA.
- UA information validation requires concurrence prior to activation in Physical Security Computer System.

Example 3.b.3 (Manual and Digital Method: Systems Residing on Lower Security Levels with AA Data Transferred to Systems Residing on Higher Security Levels)

- Request for access is submitted, the request becomes a source document.
- A PHQ is sent to the applicant, who returns the PHQ to the utility.
- The PHQ is verified to match the request data.
- All AA data and information are transferred using appropriate cyber security protocols from the computer systems residing on lower security levels, to the computer systems residing on higher security levels (CDAs).
- The process must be analyzed and protected by addressing, at a minimum, the following cyber security controls:
  - D1.16: “Open/Insecure” Protocol Restrictions
  - D1.22: Use of External Systems
  - D3.6: Transmission Integrity
  - D3.7: Transmission Confidentiality
  - D3.9: Cryptographic Key Establishment and Management
  - D3.10: Unauthorized Remote Activation of Services
  - D3.11: Transmission of Security Parameters
  - D3.12: Public Key Infrastructure Certificates
  - D3.19: Confidentiality of Information at Rest
  - D4.1: Identification and Authentication Policies and Procedures
  - D4.2: User Identification and Authentication
- True Identity verification during the completion of elements. UAA granted after validating completion of elements in source document.
- True Identity verification prior to badging.
- Badge data verified against previously provided digital records.

- Security validates information with Reviewing Official prior to activating UA.
- UA information validation requires concurrence prior to activation in Physical Security Computer System.

When the process and one of the examples above are implemented, 10 CFR 73.55 (b)(3), 10 CFR 73.55(b)(7), and 10 CFR 73.56(m) and 10 CFR 73.56(o) requirements, as they relate to cyber security, are addressed by the following:

10 CFR 73.56(m) *Protection of information* requirements are addressed by the licensee's process for securing printed personnel files along with their process for granting, controlling and revoking access to AA information systems. Both processes establish and maintain a system of files and procedures to ensure personal information is not disclosed to unauthorized persons.

10 CFR 73.56(o) *Records* requirements are addressed by the processes for preventing unauthorized access to the records and the secondary verification steps used to verify AA data integrity prior to it being entered into the Plant Security Computer System (PSCS). These processes outlined in the examples prevent the alteration of any archived data once it has been committed to storage to being advanced in the process and entered into the PSCS.

Collectively the actions documented above ensure the confidentiality, integrity, and availability of data used to perform AA functions (e.g., grant UA/UAA) and the subset of data that is input into the PSCS.

