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

December 18, 2020

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 December 2020

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. The attached white paper describes

[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.

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 the NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Security Functions," dated December 2020, by February 5, 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
Ms. Michele Sampson, NSIR/CSD, NRC

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 an assessment and revision of the guidance in NEI 10-04, Revision 2, and NEI 13-10, Revision 6. 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 comprising 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). These objectives are provided in 10 CFR 73.55(b)(3), which requires: 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.

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 security 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 should determine 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. In certain configurations, if the data stored on AA digital assets is not protected, it is possible that modified information could be entered into the Plant Security Computer System (PSCS) in a manner that would allow an unauthorized individual to obtain unescorted access into the protected and/or vital areas of a nuclear power plant (NPP), which constitutes an adverse impact to the access control function. 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,[2] and the resulting cyber security program will protect digital computer and communication systems and networks against cyber attacks, up to and including the design basis

[2] 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).

threat 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 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. These devices should be analyzed but need not be classified as CDAs if the licensee analysis demonstrates that a cyber attack on the device cannot adversely impact a security 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:

   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. If the data stored on AA digital assets is not protected, it is possible that modified information could be entered into the PSCS in a manner that would allow an unauthorized individual to obtain unescorted access into the protected and/or vital areas of a nuclear power plant. This would be an adverse impact to access control functions. 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:

   When analyzing digital computer systems, the systems and equipment associated with the following security functions must be protected against adverse impact.

Section 2.4 Support Systems and Equipment

Insert the following text after paragraph #3:

Licensees are required to identify and evaluate those digital assets associated with Security support functions whose failure as the result of a cyber attack could result in an

adverse impact to a Security 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 (a) and (c) under 'A digital device should be identified…'with the following language:

   a) SSEP functions and, through analysis, determines a compromise would adversely impact a SSEP function;

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

2. Add the following under 'Licensees should note the following':

   3) Analysis, including operating experience, training, and procedures that demonstrate compensatory measures can be taken to preclude an adverse impact to SSEP functions, are sufficient to preclude classifying systems as CDAs. For example, CAS and SAS HVAC should be analyzed to determine the impact to the security functions. If licensees have compensatory measures that can be taken to preclude an adverse impact to the security function, then CAS and SAS HVAC need not be classified as 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 as documented in Figure 1 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 if they meet criteria for being classified as an indirect CDA. 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 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 ensuring 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 revision to NEI 13-10 will guide licensees to perform an analysis identifying digital assets that store and transmit AA data. Furthermore, NEI 13-10 will clarify the manual data verifications and/or cyber security controls required to protect AA data and prevent an adverse impact to physical security functions. To address this gap, a section will be added to address the Access Authorization requirements of 10 CFR 73.56(m) and 10 CFR 73.56(o).

1. 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. Manual data verifications and/or cyber security controls required to protect AA data will prevent an adverse impact to security functions.

   Identification:

   Digital information systems and applications that store or transmit personally-identifiable information (PII) which is defined in NEI 03-01 as all information, unique to an individual, that is collected or developed during the implementation of the UAA or FFD program requirements, should be identified as digital AA assets. Licensee analysis of digital AA assets, used to facilitate the implementation of the AA program, will determine if security controls are needed to comply with 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 and integrity.

   10 CFR 73.56 Compliance Alternatives:
   Licensees can comply with 10 CFR 73.56(m) and 10 CFR 73.56(o) requirements by fully implementing any one of the following options:

   1. Using only printed AA records. Use of this option requires AA records with PII and either a National Identification Number or government-issued identification must be physically secured and access to those records must be limited to authorized personnel only.
   2. Use a combination of printed and 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.
   3. Using only digital methods. Use of this option requires classifying AA assets as

CDAs and the application of cyber security controls to protect and secure AA data confidentiality and integrity.

The following section provides additional guidance for options (2) and (3) above.

Security Control Protections:

AA System Printed and Digital Records Controls:
Licensees may use a combination of printed records along with existing digital assets on their corporate network to store and transmit AA data. In these situations, the 10 CFR 73.54 analysis would determine the AA digital assets are not CDAs. The manual data verification steps in the process precludes compromised digital asset data from being entered into the Plant Security Computer System (PSCS). Verification should be addressed 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. Figure 1 documents a typical Access Authorization UAA/UA process workflow:

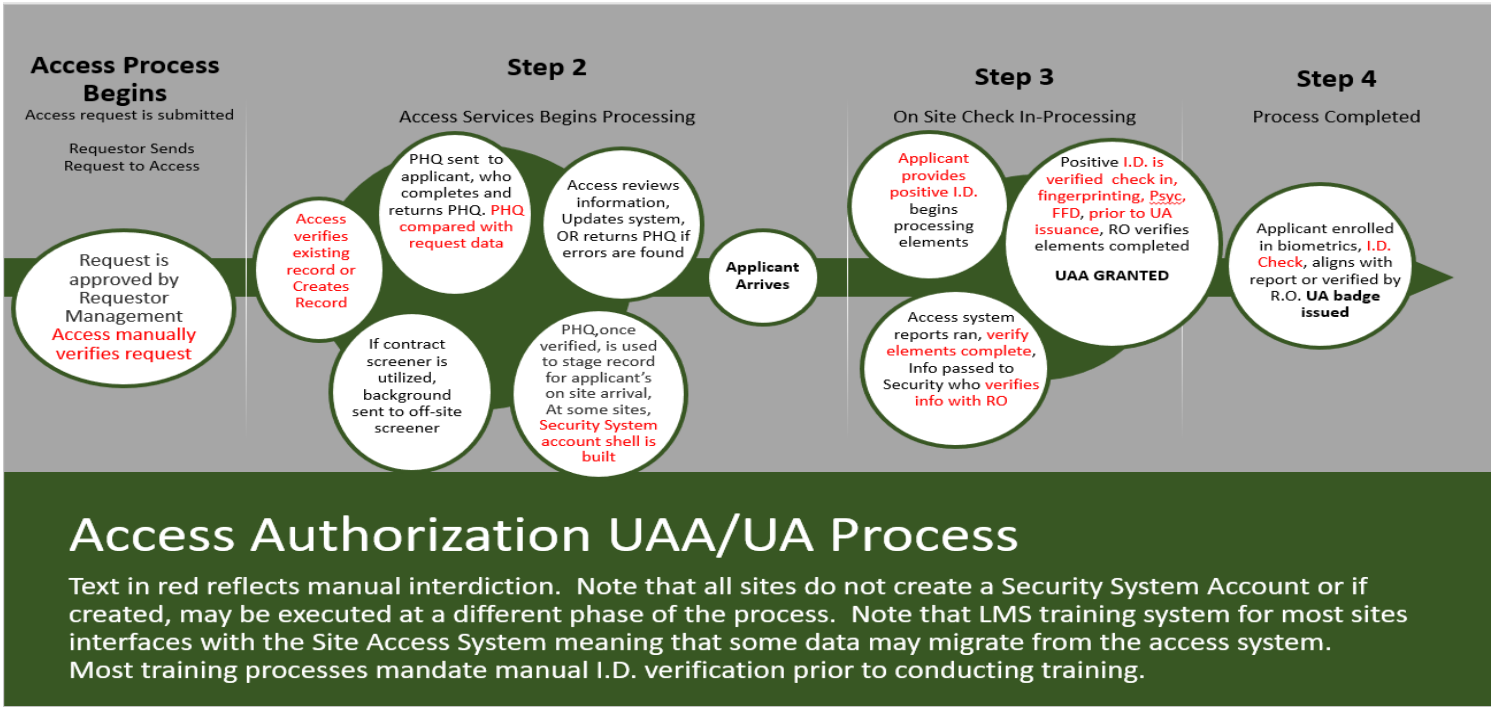

Figure 1 - Access Authorization UAA/UA Process

The red-colored text in Figure 1 document steps in the process that require manual verification to ensure data integrity. Listed below are three (3) acceptable methods that can be used to implement the Figure 1 manual data integrity verification steps.

Example #1 (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.
- Positive identification during the completion of elements. UAA granted after validating completion of elements in source file.
- Positive identification prior to badging.
- Badge data 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.

Example #2 (Manual and Digital)

- 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.
- Positive identification during the completion of elements. UAA granted after validating completion of elements in source file.
- Positive identification 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 (Digital)

- Request for access is submitted, the request data becomes the source document.
- A PHQ is provided to the applicant, who returns the PHQ to the utility.
- The PHQ is verified to match the request data.
- Positive identification during the completion of elements. UAA granted after validating completion of elements in source file.
- Positive identification prior to badging.
- Access or Security personnel verify badge data against source documents.
- 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 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, non-digital verification steps used to verify AA data integrity prior to it being entered into the Plant Security Computer System (PSCS). These processes are documented in Figure 1 and the examples above 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 modified information could not be entered into the PSCS in a manner that would allow an unauthorized individual to obtain unescorted access into the protected and/or vital areas of a nuclear power plant.

AA System CDA Security Controls:
Licensees that conduct an AA data analysis and classify their AA digital assets as critical digital assets (CDAs) have the option of positioning those AA digital assets on the higher level(s) of protection of their defensive model (e.g., security level 3 or 4 of their defensive architecture), as described in NEI 08-09 Rev. 6, section 4.3, "Defense-in-Depth Protective Strategies". AA assets classified as CDAs must be protected in a manner compliant with a licensee's Cyber Security Plan. When classified as CDAs, 10 CFR 73.54(c) requires licensees to:

- Implement security controls to protect the assets identified as within the scope of the Rule;
- Apply and maintain defense-in-depth protective strategies;
- Mitigate the adverse impact of cyber-attacks; and
- Ensure the functions of protected assets are not adversely impacted due to cyber attacks.

To ensure AA assets and digital records are protected to the level of a CDA and meet the 10 CFR 73.54(c) requirements listed above, the following cyber security controls must be addressed as described in NEI 08-09 section 3.1.6:

- 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

It may be appropriate for licensees to consider protecting to the level of a CDA when upgrading AA infrastructure and applications as it is less impactful to address and implement cyber security controls early in the design phase of the life cycle.