U.S. NUCLEAR REGULATORY COMMISSION

DRAFT REGULATORY GUIDE DG-5074

Proposed new Regulatory Guide 5.95, Revision 0

Issue Date: October 2024
Technical Lead: Brad Baxter

ACCESS AUTHORIZATION PROGRAM FOR COMMERCIAL NUCLEAR PLANTS

A. INTRODUCTION

Purpose

This regulatory guide (RG) describes a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for use by licensees to establish, maintain, and implement an access authorization program for commercial nuclear plants under the provisions of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 53, "Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Plants" (Ref. [1]).

Applicability[1]

This RG applies to each applicant licensed under the provisions of 10 CFR Part 53 that meets the criterion in 10 CFR 53.860(a)(2)(i), and that is required to establish, maintain, and implement an access authorization program under 10 CFR 73.120, "Access authorization program for commercial nuclear plants," (Ref. [2]), as part of its physical security plan.

Applicable Regulations

- 10 CFR Part 26, "Fitness for Duty Programs" (Ref. [3]), provides the requirements and standards for the establishment, implementation, and maintenance of fitness-for-duty programs.

- Subpart B, "Background Investigations and Access Authorization Program," of 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material" (Ref. [4]), provides the requirements for the physical protection program for any licensee that possesses an aggregated category 1 or category 2 quantity of radioactive materials. The specific requirements are as follows:
  - 10 CFR 37.23, "Access authorization program requirements," provides the requirements for granting initial or reinstated unescorted access (UA) authorization.

[1] Applicants not satisfying the criterion in 10 CFR 53.860(a)(2)(i) shall establish, implement, and maintain a full access authorization program, including an insider mitigation program, under 10 CFR 73.55(b)(7) and (b)(9), or 10 CFR 73.100(b)(7) and (b)(9).

This RG is being issued in draft form to involve the public in the development of regulatory guidance in this area. It has not received final staff review or approval and does not represent an NRC final staff position. Public comments are being solicited on this RG and its associated regulatory analysis. Comments should be accompanied by appropriate supporting data. Comments may be submitted through the Federal-rulemaking website, http://www.regulations.gov, by searching for draft regulatory guide DG-5074. Alternatively, comments may be submitted to Office of the Secretary, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, ATTN: Rulemakings and Adjudications Staff. Comments must be submitted by the date indicated in the *Federal Register* notice.

Electronic copies of this RG, previous versions of DGs, and other recently issued guides are available through the NRC's public website under the Regulatory Guides document collection of the NRC Library at https://www.nrc.gov/reading-rm/doc-collections/reg-guides/index.html. The RG is also available through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML22199A246. The regulatory analysis is associated with a rulemaking and may be found in ADAMS under Accession No. ML24095A166.

- 10 CFR 37.25, “Background investigations,” requires licensees to complete a background investigation (BI) of the individual seeking UA authorization.

- 10 CFR 37.27, “Requirements for criminal history records checks of individuals granted unescorted access to category 1 or category 2 quantities of radioactive material,” requires licensees to investigate individuals who are permitted UA to category 1 or category 2 radioactive material.

- 10 CFR 37.29, “Relief from fingerprinting, identification, and criminal history records checks and other elements of background investigations for designated categories of individuals permitted unescorted access to certain radioactive materials,” excludes licensees from performing fingerprinting, identification, and criminal history records checks for certain classes of individuals.

- 10 CFR 37.31, “Protection of information,” prohibits the licensee from disclosing the record or personal information collected and maintained.

- 10 CFR 37.33, “Access authorization program review,” requires the licensee to ensure that access authorization programs are reviewed to confirm compliance with the requirements and that comprehensive actions are taken to correct any noncompliance that is identified.

- 10 CFR Part 53 provides an alternative risk-informed and technology-inclusive regulatory framework for the licensing, construction, operation, and decommissioning of commercial nuclear plants.

  - 10 CFR 53.860, “Security programs,” requires, in part, that each holder of an operating license or combined license under Part 53 establish, implement, and maintain an access authorization program that meets the requirements in 10 CFR 73.120 if the criterion in 10 CFR 53.860(a)(2)(i) is met.

  - 10 CFR 53.860(a)(2)(i) provides an optional criterion for licensees to demonstrate that the radiological consequences from a design-basis-threat-initiated event involving the loss of engineered systems for decay heat removal and possible breaches in physical structures surrounding the reactor, spent fuel, and other inventories of radioactive materials result in offsite doses below the values in 10 CFR 53.210, “Safety criteria for design-basis accidents.”

  - 10 CFR 53.860(a)(2)(ii) requires the licensee to perform a site-specific analysis, including identification of target sets, to demonstrate that the criterion in 10 CFR 53.860(a)(2)(i) is met. The analysis must assume that licensee mitigation and recovery actions, including any operator action, are unavailable or ineffective. The licensee must maintain the analysis until the permanent cessation of operations and permanent removal of fuel from the reactor vessel as described under 10 CFR 53.1070, “Termination of license.”

  - 10 CFR 53.860(c) requires that each holder of an operating license or combined license under Part 53 develop, implement, and maintain an access authorization program that demonstrates compliance with the requirements in 10 CFR 73.120 if the criterion in 10 CFR 53.860(a)(2)(i) is met, or the requirements in 10 CFR 73.56, “Personnel access authorization requirements for nuclear power plants,” if the criterion is not met.

- 10 CFR Part 73, “Physical Protection of Plants and Materials,” requires licensees to establish and maintain a physical protection system that will have capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used.

  - 10 CFR 73.55, “Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage,” requires certain power reactor licensees to implement a physical protection program under the requirements of this section.

  - 10 CFR 73.56 requires certain power reactor licensees to establish, implement, and maintain an access authorization program under the requirements of this section.

  - 10 CFR 73.57, “Requirements for criminal history records checks of individuals granted unescorted access to a nuclear power facility, a non-power reactor, or access to Safeguards Information,” requires licensees to fingerprint each individual who is permitted UA to the nuclear power facility or the nonpower reactor facility, or access to safeguards information. The licensee will then review and use the information received from the Federal Bureau of Investigation (FBI) and, based on the provisions in this section, determine either to continue to grant or to deny that individual further UA to the nuclear power facility or the nonpower reactor facility, or access to safeguards information.

  - 10 CFR 73.100, “Technology-inclusive requirements for physical protection of licensed activities at commercial nuclear plants against radiological sabotage,” provides a performance-based regulatory framework for physical protection as an alternative to the prescriptive requirements of 10 CFR 73.55.

  - 10 CFR 73.120 establishes graded performance objectives as an alternative to compliance with 10 CFR 73.55, 10 CFR 73.56, and 10 CFR 73.57 for 10 CFR Part 53 licensees that meet the criterion in 10 CFR 53.860(a)(2)(i). The proposed rule affords 10 CFR Part 53 licensees additional flexibility in establishing an access authorization program that meets the performance objectives and requirements of this section.

Related Guidance

- NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition,” provides guidance to the NRC staff on performing safety reviews of construction permit or operating license applications (including requests for amendments) under 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities,” (Ref. [5]) and of early site permit, design certification, combined license, standard design approval, or manufacturing license applications under 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants” (Ref. [6]) (including requests for amendments). Specifically, NUREG-0800 provides the following:

  - Section 13.6.4, “Access Authorization for Operational Program” (Ref. [7]), identifies guidance describing applicable components of an access program, including the evaluation criteria for granting and maintaining UA authorization and for certifying and maintaining UA. The standards also provide details on reinstatement of access authorization, requirements for contractor/vendor (C/V) performance and trustworthiness and reliability, audits and corrective actions, protection of information, and required sharing of information between licensees and licensee C/Vs supporting a licensee access authorization program.

- RG 5.66, "Access Authorization Program for Nuclear Power Plants" (Ref. [8]), provides guidance on the access authorization program requirements in 10 CFR 73.56. RG 5.66 also endorses Revision 3 of Nuclear Energy Institute (NEI) 03-01, "Nuclear Power Plant Access Authorization Program," dated May 9, 2009, which contains security-related information in accordance with 10 CFR 2.390(d)(1) and therefore is not publicly available. The NEI guide describes an approach that the NRC staff has found acceptable for meeting the NRC requirements for an access authorization program.

Purpose of Regulatory Guides

The NRC issues RGs to describe methods that are acceptable to the staff for implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific issues or postulated events, and to describe information that the staff needs in its review of applications for permits and licenses. Regulatory guides are not NRC regulations and compliance with them is not required. Methods and solutions that differ from those set forth in RGs are acceptable if supported by a basis for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG provides voluntary guidance for implementing the mandatory information collections in 10 CFR Parts 26, 37, 53, and 73 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et. seq.). These information collections were approved by the Office of Management and Budget (OMB), under control numbers 3150-0146, 3150-0214, 3150-XXXX, and 3150-0002, respectively. Send comments regarding these information collections to the FOIA, Library, and Information Collections Branch (T6-A10M), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by email to Infocollects.Resource@nrc.gov, and to the OMB Office of Information and Regulatory Affairs, Attn: Desk Officer for the Nuclear Regulatory Commission, 725 17th Street, NW Washington, DC 20503.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the document requesting or requiring the collection displays a currently valid OMB control number.

TABLE OF CONTENTS

A. INTRODUCTION....1
Purpose1
Applicability....1
Applicable Regulations....1
Related Guidance....3
Purpose of Regulatory Guides....4
Paperwork Reduction Act....4
Public Protection Notification....4
B. DISCUSSION....7
Reason for Issuance....7
Background....7
Consideration of International Standards....8
C. STAFF REGULATORY GUIDANCE....9
Applicability: Individuals Subject to the Access Authorization Program....10
Program Elements....11
Reviewing Official....12
Initial Unescorted Access....14
Updated Unescorted Access....15
Maintaining Unescorted Access....16
Consent and Advisement....19
Personal History Questionnaire....20
Verification of True Identity....21
Employment/Unemployment History....22
Credit Check....29
Character and Reputation....30
Criminal History Inquiry....32
Reinvestigations....32
Behavioral Observation....33
Legal Action Reporting....36
Reviewing Official Annual Review....36
Unfavorable Employment Terminations....37
Other Required Background Screening....38
Background Investigation Screeners....38
Personnel Processing Applications....39
Licensee Shared Information....40
Request for Access Withdrawn....41
Individual Withdraws Consent....41
Individual in a Denied Status....42
Unescorted Access Denial Review Process....43
Individuals Currently Denied Access....44
Program Reliability....44
Backup or Manual Process for Sharing Information....45
Audits 45
Licensee Program Audits of Unescorted Access Program....46
Licensee-Approved Contractor/Vendor Screening and Background
Screening Company Programs....47

Contractor/Vendor Internal Audit and Contractor/Vendor Audit of Subcontractors....47
Records and Protection of Information....48
Records Retention....49
D. IMPLEMENTATION....51
GLOSSARY....52
APPENDIX A....1
BIBLIOGRAPHY....1

B. DISCUSSION

Reason for Issuance

The current application and licensing requirements, developed for large light-water and nonpower reactors, as outlined in 10 CFR Part 50 and 10 CFR Part 52, do not fully consider the variety of designs for commercial nuclear reactors; they may require extensive use of the exemption process for regulations that include prescriptive requirements specific to light-water reactors. Therefore, the NRC is proposing an alternative regulatory framework for licensing commercial nuclear reactors under 10 CFR Part 53. This document provides guidance and is one NRC-approved method (not the only method) for meeting regulatory requirements established under 10 CFR Part 53 and Part 73. The existing regulatory framework for access authorization under 10 CFR 73.55, 10 CFR 73.56, and 10 CFR 73.57 is sufficient to provide reasonable assurance that individuals subject to the program are trustworthy and reliable, so as not to constitute an unreasonable risk to public health and safety or the common defense and security, regardless of the reactor technology. The language in 10 CFR 73.120 provides flexibility by making available an alternate approach, commensurate with risk and consequence to public health and safety, for 10 CFR Part 53 applicants that can demonstrate in an analysis that the offsite consequences of a postulated event will meet the criterion defined in 10 CFR 53.860(a)(2)(i). The analysis must assume that licensee mitigation and recovery actions, including any operator action, are unavailable or ineffective. Under this proposed approach, should an applicant for a commercial nuclear reactor license demonstrate, pursuant to 10 CFR 53.860(a)(2)(i), that an offsite release would not exceed doses defined in the safety criteria of 10 CFR 53.210, the applicant may implement the access authorization program requirements under 10 CFR 73.120, instead of the requirements under 10 CFR 73.55 or 10 CFR 73.100, 10 CFR 73.56, and 10 CFR 73.57.

Background

Under 10 CFR 53.860, each licensee under 10 CFR Part 53 must establish, maintain, and implement a physical protection program meeting the following requirements:

- The licensee must (1) implement security requirements for the protection of special nuclear material, based on the form, enrichment, and quantity of special nuclear material, in accordance with 10 CFR Part 73, as applicable, and implement security requirements for the protection of category 1 and category 2 quantities of radioactive material in accordance with 10 CFR Part 37, as applicable, and (2) meet the provisions set forth in either 10 CFR 73.55 or 10 CFR 73.100, unless the licensee meets the following criteria:

    - The radiological consequences from a design-basis-threat-initiated event involving the loss of engineered systems for decay heat removal and possible breaches in physical structures surrounding the reactor, spent fuel, and other inventories of radioactive materials result in offsite doses below the values established in 10 CFR 53.210.

    - The licensee has performed a site-specific analysis to demonstrate that the criterion in 10 CFR 53.860(a)(2)(i) is met. The analysis must assume that licensee mitigation and recovery actions, including any operator action, are unavailable or ineffective. The licensee must maintain the analysis consistent with the requirements for maintaining licensing basis information in 10 CFR Part 53, Subpart I, “Maintaining and revising licensing basis information” until the permanent cessation of operations under 10 CFR 53.1070

For applicants satisfying 10 CFR 53.860(a)(2)(i), the proposed requirements are modeled on the existing access authorization programs for nonpower reactors and materials licensees; they also consider key elements of access authorization programs for power reactors under 10 CFR 73.56. Although the NRC regulations do not currently contain many access authorization requirements specific to nonpower reactors, other than those associated with fingerprinting of individuals for criminal history checks under 10 CFR 73.57(g), there are alternate security measures and license conditions in place for nonpower reactors that are applied in the proposed 10 CFR 73.120 for commercial nuclear reactors licensed under 10 CFR Part 53.

A commercial nuclear plant licensee under 10 CFR Part 53 that does not meet the criterion in 10 CFR 53.860(a)(2)(i) needs to implement the requirements of 10 CFR 73.55 or 10 CFR 73.100 through its physical security plan. The new section 10 CFR 73.100 provides a regulatory framework based on performance requirements that minimizes or eliminates prescriptive requirements (compared to 10 CFR 73.55) to permit the applicant or licensee maximum flexibility in designing and implementing the physical protection necessary to protect against the design-basis threat and to ensure plant security for activities involving nuclear material. The physical security requirements in 10 CFR 73.55 use a combination of performance criteria (e.g., the physical protection program must protect against the design basis threat for radiological sabotage as stated in 10 CFR 73.1, "Purpose and scope") and prescriptive requirements developed to achieve the performance objectives. In a performance-based approach to physical security, performance criteria and objectives are the primary basis for regulatory decision-making, giving the licensee the flexibility to determine how to meet the performance criteria for an effective physical protection program.

Consideration of International Standards

The International Atomic Energy Agency (IAEA) works with member states and other partners to promote the safe, secure, and peaceful use of nuclear technologies. The IAEA has established a series of security guides to address nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer, and other malicious acts involving nuclear material and other radioactive substances and their associated facilities. IAEA security guides present international good practices and increasingly reflect best practices to help users striving to achieve high levels of security. To inform its development of this RG, the NRC considered IAEA requirements and guides pursuant to the Commission's International Policy Statement (Ref. [9]) and Management Directive and Handbook 6.6, "Regulatory Guides" (Ref. [10]).

In developing this RG, the NRC considered the following IAEA documents, which largely recommend a risk-informed approach appropriate for the new regulatory framework:

- IAEA NSS No. 27-G, "Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5)," issued 2018 (Ref. [11])

- IAEA NSS No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," issued 2011 (Ref. [12])

C. STAFF REGULATORY GUIDANCE

Applicants satisfying the criterion in 10 CFR 53.860(a)(2)(i) shall establish, implement, and maintain their access authorization program under 10 CFR 73.120 as part of their physical security plan before initial fuel load into the reactor or initiating the physical removal of any one of the independent mechanisms to prevent criticality required under § 53.620(d)(1) of this chapter for a fueled manufactured reactor (under 10 CFR 53.610, "Construction").

1. If the criterion of 10 CFR 53.860(a)(2)(i) is not met, the licensee is required to implement a full access authorization program, including an insider mitigation program, as required in 10 CFR 73.55(b)(7) or 10 CFR 73.100(b)(7) and 10 CFR 73.56. In either case, the security program should include the establishment, maintenance, and implementation of the following:

    a. a fitness-for-duty program that meets the requirements of 10 CFR Part 26,

    b. an access authorization program with the following attributes:

        (1) meeting the requirements of 10 CFR 73.120 if the 10 CFR 53.860(a)(2)(i) criterion is met, and

        (2) meeting the requirements of 10 CFR 73.56, and of 10 CFR 73.55(b)(7) or 10 CFR 73.100(b)(7), if the 10 CFR 53.860(a)(2)(i) criteria are not met, and

    c. a cybersecurity program that meets the requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks" or 10 CFR 73.110, "Technology-inclusive requirements for protection of digital computer and communication systems and networks."

2. The following are general performance objectives and requirements for licensees and applicants satisfying the criterion in 10 CFR 53.830(a)(2)(i) and subject to 10 CFR 73.120:

    a. Each licensee's or applicant's access authorization program under 10 CFR 73.120 must demonstrate that the individuals specified in 10 CFR 73.120(b)(1)(i–iv) and (b)(2) are trustworthy and reliable, so that they do not constitute an unreasonable risk to public health and safety or the common defense and security. The requirements for the access authorization program include:

    b. Licensees and applicants satisfying the criterion in 10 CFR 53.860(a)(2)(i) shall establish, implement, and maintain their access authorization program under 10 CFR 73.120. The proposed language establishes general performance objectives and requirements providing reasonable assurance that the individuals who are specified in paragraph (b) of 10 CFR 73.120 are trustworthy and reliable.

        (1) background investigation (BI):

            i. personal history disclosure,
            ii. verification of true identity,
            iii. employment history evaluation,
            iv. unemployment/military service/education,
            v. credit history evaluation,

vi. character and reputation evaluation, and
vii. FBI identification and criminal history records check, and

(2) behavioral observation (BO),

(3) self-reporting of legal actions,

(4) unescorted access (UA),

(5) termination of UA,

(6) basis of determination for access,

(7) review procedures,

(8) protection of information,

(9) audits and corrective action, and

(10) records.

c. Licensees and applicants that implement the access authorization requirements of 10 CFR 73.120 and prepare their programs in accordance with this guidance should include the following statement in their physical security plans: "All elements of RG 5.95 have been implemented to satisfy the requirements of 10 CFR 73.120 related to granting UA and maintaining UA."

3. The remainder of this RG applies solely to the access authorization program under 10 CFR 73.120.

Applicability: Individuals Subject to the Access Authorization Program

4. The following individuals are subject to the access authorization program and should be screened in accordance with applicable sections of this document:

a. any individual to whom a licensee intends to grant UA to a commercial nuclear plant protected area, vital area, or controlled access area where licensed material is used or stored;

b. any individual whose duties and responsibilities permit them to take actions by electronic means, either on site or remotely, that could adversely affect the licensee's or applicant's operational safety, security, or emergency preparedness (e.g., critical group personnel, as defined later in the glossary);

c. any individual who has responsibilities for implementing a licensee's or applicant's protective strategy, including, but not limited to, armed security force officers, alarm station operators, and tactical response team leaders, but not including Federal, State, or local law enforcement personnel;

d. the reviewing official for a licensee's or C/V's access program;

e. other individuals, at the licensee's discretion, including C/V employees who are designated in access authorization program procedures;

f. background investigation screener personnel responsible for controlling, collecting, and processing information that the licensee reviewing official will use to make access determinations; and

g. personnel who evaluate information to process individuals for UA, who have unfettered access to the files and records of persons applying for or holding UA, or who are responsible for managing data upon which UA decisions may be based.

5. Licensees should grant UA to all individuals whom the NRC has certified, in writing, as suitable for such access.

6. Licensees should limit the access of any individual who was denied UA or terminated unfavorably from requirements greater than or equal to the access authorization requirements for commercial nuclear plants. Licensees should not permit such an individual to enter any commercial nuclear plant protected or vital area, , or controlled access area where licensed material is used or stored, under escort or otherwise, or to take actions by electronic means that could affect the licensee's operational safety, security, or emergency preparedness, under supervision or otherwise, until the individual is deemed trustworthy and reliable.

7. A licensee seeking to grant UA to an individual who is subject to another NRC-approved access authorization program or another access authorization program that complies with the requirements in this document may rely on those documented access authorization programs or access authorization program elements to comply with the requirements. In such a case, the licensee must document that the other access authorization program has maintained the program elements to be accepted, consistent with the requirements of this section.

8. All operating U.S. nuclear power plants and certain other licensees that collect data under requirements greater than or equal to access authorization requirements for commercial nuclear plants are subject to requirements similar to or more stringent than those described in this document. Therefore, licensees may share and rely upon information that has been collected and evaluated in accordance with the requirements of a nuclear power plant's approved access authorization program only if the personnel requesting UA has signed a self-disclosure agreement permitting the transfer or sharing of personally identifiable information.

Program Elements

9. The requirements for UA are separated into the following authorization categories:

a. initial UA (i.e., the first time an individual subject to 10 CFR 73.120 is granted UA to a commercial nuclear plant);

b. maintaining UA (i.e., maintaining continued UA without a break in service or employment; program elements include BO, background reinvestigation, and annual supervisor review); and

c. updated UA (i.e., UA that has been restored after access was terminated, under favorable conditions, more than 365 days but less than 10 years before restoration).

10. The following determining factors differentiate the use of these categories:

    a. whether the individual has previously held UA,
    b. whether less than 10 years has lapsed since the last investigation was conducted, and
    c. whether the previous UA was terminated favorably.

11. If applicable, licensees and C/Vs may rely upon information gathered by other licensees and C/Vs that are subject to 10 CFR 73.56 or 10 CFR 73.120 about individuals who have previously applied for UA, and upon information the other licensees and C/Vs have developed about individuals during periods in which the individuals maintained UA status.

12. For individuals whose last UA was terminated unfavorably or was suspended because of violation of a licensee program policy, or whose last UA or request for UA was denied, the individual's trustworthiness and reliability must be reestablished under the part of the licensee's or applicant's access authorization program applicable to initial UA.

Reviewing Official

13. Under 10 CFR 73.120(c)(6)(iii), the licensee is required to designate one or more individuals as reviewing officials, who will make access determinations based on an individual's trustworthiness and reliability. The designation should be in writing, and the designated reviewing official should have a demonstrated knowledge of all aspects of the access authorization program.

    a. Reviewing officials are the only individuals authorized to make UA determinations.

    b. Each licensee or applicant must name one or more individuals to be reviewing officials pursuant to the requirements of 10 CFR 37.23(b)(2).

14. In every case, the reviewing official should evaluate an individual's trustworthiness and reliability based on information gathered before the licensee grants UA. The individual should be informed of the basis for any denial of UA. Items to evaluate include the following:

    a. the self-disclosed and BI-developed activities of the individual;

    b. the consistency and completeness of self-disclosed and BI-developed information;

    c. the results of the true identity verification of the individual, such as a comparison of personal history questionnaire (PHQ) data to BI-developed information, the individual's credit report, validation of the Social Security number (SSN), criminal history check results, and other data sources; and

    d. the reason for any inconsistencies detected through review of collected information (i.e., whether inconsistencies are intentional, innocent, or an oversight), with willful or intentional acts of omission or untruthfulness being grounds for denial of UA.

15. Whenever an individual who has been granted UA is subsequently terminated unfavorably, the organization responsible for controlling access to the protected area, or controlled access area should be notified before or simultaneously with the unfavorable termination.

16. The individual should be notified in writing that any document they submit as part of the UA process must contain accurate, complete, and truthful information. The individual should also be notified in writing of the consequences for failure to meet this requirement.

17. The following actions related to providing and sharing the personal information required are sufficient cause for denial or unfavorable termination of UA:

    a. refusal to provide written consent for the suitable inquiry (SI);

    b. refusal to provide, or falsification of, any personal information, including, but not limited to, failure to report any previous denial or unfavorable termination of authorization;

    c. refusal to provide written consent for the sharing of personal information with other licensees or C/Vs; or

    d. failure to report any legal actions

18. The licensee reviewing official may determine that UA should be denied or terminated at any time based on disqualifying information, even if not all the information required by the licensee has been provided. However, UA should not be granted until all UA elements are completed and have been favorably evaluated by the licensee reviewing official.

19. The reviewing official should complete an evaluation of the information obtained from the reinvestigation's criminal history update before the end of the 10-year reinvestigation period. If the criminal history update and supervisory review (if applicable) have not been completed and the information evaluated by the reviewing official within the required 10-year period (or more frequently at the licensee's discretion or within the time period specified in the licensee's physical security plan), the reviewing official should administratively withdraw the individual's UA until these requirements have been met.

20. The results of the criminal history update and the supervisory review should support the reviewing official's determination of the individual's continued trustworthiness and reliability.

21. If the criminal history update and supervisory review (if applicable) have not been completed and the information evaluated by the licensee reviewing official within the required 10-year period (or more frequently at the licensee's discretion, or within the time period specified in the licensee's physical security plan), the reviewing official should administratively withdraw the individual's UA until these requirements have been met.

22. If an individual who has UA has not entered the protected area, or controlled access area for more than 30 continuous days, the individual's UA status should be suspended until the reviewing official has evaluated the lapse in time to reinstate UA status.

23. If a licensee is aware of information about an individual that characterizes them as untrustworthy or unreliable for UA, the reviewing official should evaluate the information and determine whether to grant UA to that individual.

Potentially Disqualifying Information That Has Not Been Reviewed

24. If potentially disqualifying information (PDI) is disclosed or discovered that has not been reviewed and favorably resolved by a previous licensee, if applicable, the discovering reviewing

official should suspend the individual's UA until the PDI has been reviewed and favorably resolved.

Initial Unescorted Access

25. Prior to granting an individual UA, a licensee should confirm the following:

    a. whether the individual has ever been granted UA, or

    b. whether the individual has held UA within the past 10 years at a commercial nuclear plant or other nuclear power reactor facility, and whether the last period of UA was terminated favorably.

26. Each individual applying for initial UA will undergo a BI for the past 7 years (or since their 18th birthday, whichever is shorter).

27. The reviewing official should complete and approve the following elements, as appropriate, before the licensee grants UA:

    a. Verify that the individual has completed and signed the following documents and has provided them to the licensee or an approved C/V, or an authorized agent of person requesting UA:

        (1) consent form,
        (2) PHQ, and
        (3) self-disclosure of PDI and legal actions.

    b. Verify the true identity of the individual, including demographic information (e.g., name, date of birth).

    c. Verify the individual's employment/unemployment history for the past 7 years (including education or military service in lieu of employment), as follows:

        (1) For the most recent year preceding the application, do the following:

            i. Verify every claimed employment (regardless of length), including the following:

                (1) the employer by whom the individual claims to have been employed on the day before they are completing the employment history, and

                (2) education or military service in lieu of employment as described in this section.

            ii. Conduct an SI, on a best effort basis, on every claimed employment.

            iii. Verify each unemployment period of 30 days or more (no SI is required during checks of unemployment periods).

        (2) For the remainder of the required 7-year period, do the following:

i. Verify the longest claimed period of employment (including self-employment) in any calendar month.

ii. Verify each period of unemployment of 30 days or more (no SI is required during checks of unemployment periods).

iii. If an individual claims two employments of the same length in the same month, only one needs to be selected for verification and SI.

iv. If equal periods of employment and unemployment are claimed, verify the employment and conduct the SI.

(3) Evaluate the individual's credit history, for the extent of the credit history disclosed by a national credit reporting agency.

(4) Verify the individual's character and reputation through contact with at least two developed references.

(5) Conduct an FBI criminal history inquiry and evaluate all information returned.

(6) Verify that the individual is aware of the legal action reporting requirements under BO.

(7) In every case, before certifying or granting UA, conduct an evaluation based on an accumulation of information that supports a determination that the individual is trustworthy and reliable.

Updated Unescorted Access

28. An updated UA BI is conducted before granting UA for an individual who last held UA that was terminated under favorable conditions more than 7 years, but less than 10 years, from the date UA was previously granted.

29. The reviewing official should complete and approve the following elements, as appropriate, before the licensee grants UA:

a. Verify that the individual has completed and signed the following documents and provided them to the licensee, an approved C/V, or an authorized agent of person requesting UA:

(1) consent that BI information will be updated and maintained,
(2) PHQ, and
(3) self-disclosure of legal actions.

b. Verify the true identity of the individual, including demographic information.

c. Verify the individual's employment/unemployment history (including education or military service in lieu of employment) since last UA, as follows:

(1) For the most recent year preceding the application, do the following:

i. Verify every claimed employment (regardless of length), including the following:

(1) the employer by whom the individual claims to have been employed on the day before they are completing the employment history, and
(2) military service or education in lieu of employment.

ii. Conduct an SI, on a best effort basis, on every claimed employment.

iii. Verify each unemployment period of 30 days or more (no SI is required during checks of unemployment periods).

(2) For the remainder of the required 7-year period, do the following:

i. Verify the longest claimed period of employment (including self-employment) in any calendar month.

ii. Verify each period of unemployment of 30 days or more (no SI is required during checks of unemployment periods).

iii. If an individual claims two employments of the same length in the same month, only one needs to be selected for verification and SI.

iv. If equal periods of employment and unemployment are claimed, verify the employment and conduct the SI.

(3) Evaluate the individual's credit history, for the extent of the credit history disclosed by a national credit reporting agency.

(4) Verify the individual's character and reputation through contact with at least two developed references.

(5) Conduct an FBI criminal history inquiry and evaluate all information returned.

(6) In every case, before certifying or granting UA, conduct an evaluation based on an accumulation of information that supports a determination that the individual is trustworthy and reliable.

Maintaining Unescorted Access

30. An individual maintains UA as long as the following are true:

a. The applicable elements of 10 CFR 73.120 are current.
b. The individual complies with the licensee's or C/V's policies and procedures.

31. Coverage by BO requires an individual to do the following:

a. Report legal actions.
b. Undergo an annual supervisory review.

Maintaining Unescorted Access Elements Current

32. To maintain current the criminal history and BI elements required for UA, the individual should do the following:

    a. Be subject to BO program roles and responsibilities, including being aware of legal reporting requirements.

    b. Have had applicable periodic reinvestigations conducted within established timeframes (10 years).

    c. Complete a self-disclosure form before the initial granting of UA.

To maintain UA current when transferring between commercial nuclear plants, the licensee should do the following:

33. Obtain consent when the individual travels between different licensee companies, if applicable.

34. Verify the true identity of the individual, including demographic information, if the individual is moving between licensee companies.

35. Verify that the individual complies with the licensee's or C/V's access authorization program policies and procedures to which they are subject, including the responsibility to report legal actions.

36. Verify that the individual has had the applicable periodic reinvestigations and annual supervisory reviews conducted as defined and within established timeframes.

37. Verify that the individual is under BO and that there have been no breaks of more than 30 continuous days.

To grant UA to an individual with current UA, the licensee should do the following:

38. Verify receipt of a request for UA.

39. Verify that the licensee reviewing official has completed the elements listed above to maintain the individual's UA.

Maintaining Unescorted Access with Potentially Disqualifying Information

40. To maintain UA if PDI is disclosed or discovered, the licensee should take applicable actions to determine whether there is a continued need to maintain UA during the evaluation period.

41. After granting UA, a licensee or C/V may develop information that brings into question the continued trustworthiness and reliability of the individual.

    a. PDI developed by or provided to a licensee or C/V should be promptly (on the day of discovery) reported to the appropriate level of management and to the licensee reviewing official for assessment.

b. The licensee should deny or administratively hold the individual's UA on the day that the licensee receives the information or implements an applicable process as defined in the licensee's procedure to evaluate the circumstance before reinstating UA.

c. The licensee reviewing official should determine whether the person continues to be trustworthy and reliable.

Licensee-Approved Programs (If Applicable, Through Contractual Agreements)

42. The licensee may accept, in whole or in part, the results of a UA program conducted by another licensee or an approved C/V, provided that the following are true:

    a. The program elements have been maintained and meet the requirements of 10 CFR 73.56 or 10 CFR 73.120 as described in an audit by the licensee. Upon request, the appropriate records should be made available for auditing by the licensee or its designated representatives and by representatives of the NRC.

    b. The C/V program features do not abrogate the licensee's ultimate responsibility for ensuring that individuals granted UA to the protected area, vital area or controlled access area where licensed material is used or stored are trustworthy and reliable.

43. In conjunction with the request for UA at a licensee facility, C/Vs should report to the receiving licensee all PDI disclosed or discovered during any review for initial UA or for maintaining UA.

44. If, during an update of UA, PDI not previously known to the licensee is disclosed to or discovered by the C/V, the C/V should report the PDI to the licensee with the request for UA.

45. While an individual holds UA, all PDI, disclosed or discovered, should be reported on the day of discovery to the licensee(s) with which the individual holds an active UA.

46. PDI disclosed or discovered after the termination of UA that would have affected a period of UA should be reported to the affected licensee(s) upon the day of discovery.

47. The licensee should deny or administratively withdraw the individual's UA on the day that the licensee receives the information from the C/V or implements an applicable process.

Administrative Process for Conducting Background Investigations

48. The investigation period is through the date on which the individual applies for UA, as documented by the date on which the individual signs the PHQ.

49. If, for any reason, the investigation is not completed within 30 days of the application, the licensee should have the individual update their original submittal to include the following:

    a. supplemental PHQ information, to include the time period in excess of 30 days,
    b. additional employment/unemployment periods, and
    c. any new self-disclosure information.

50. A licensee or C/V is not authorized to withhold from law enforcement officials any evidence of criminal conduct detected during the collection and verification of the elements specified in this section.

Consent and Advisement

51. No element of the UA program may be initiated without the knowledge and written consent of the individual applying for UA. The individual applying for UA should be informed in writing about the following:

    a. the types of records that may be produced and retained,

    b. where such records are normally maintained,

    c. the duration for which such records are to be retained,

    d. their right to review the results of the developed information, and to verify its accuracy and completeness,

    e. the fact that the following actions related to providing and sharing the personal information under this section are sufficient cause for denial or unfavorable termination of UA:

        (1) refusal to provide signed consent for the BI that includes the SI,

        (2) refusal to provide, or falsification of, any personal history information required under this section, including failure to report any previous denial or unfavorable termination of UA,

        (3) refusal to provide signed consent for the sharing of personal information with other licensees or C/Vs, or

        (4) failure to report any legal actions,

    f. their right to correct any incorrect or incomplete information, and

    g. the ability of licensees to share information developed during the application for UA with entities having a need to know of the information to perform their assigned responsibilities.

52. The individual has the right to challenge any PDI but does not have the right to know who provided and confirmed the PDI.

    a. PDI obtained from confidential/unnamed sources should be adjudicated by the reviewing official and the result documented.

    b. PDI from confidential/unnamed sources should be corroborated before the PDI can be used to deny access.

    c. The individual should be informed that the results of the investigation will be accessible for use in all power reactor licensee UA programs.

53. In addition, the individual should be informed that they may withdraw consent at any time and should be advised of the following:

a. Withdrawal of their consent will withdraw their current application for access authorization under the licensee's or C/V's access authorization program.

b. If applicable, other licensees making an access determination for the individual will have access to information documenting the withdrawal through an information-sharing mechanism. C/Vs and other entities may have the same access to the information, if they need such information to comply with requirements set forth in this document.

c. The withdrawal should be in writing and signed by the individual. When consent is withdrawn, no new processing may be initiated; however, steps in progress should be completed and documented.

54. If applicable, the elements of the industry's information-sharing mechanism consent form, taken directly from the information-sharing mechanism or database participation agreement, should be included as part of the licensee's or C/V's consent process.

55. When any licensee's or C/V's UA program (or that of their authorized agents) is legitimately seeking the information required for a UA decision and has obtained a signed release from the subject individual authorizing the disclosure of such information, a licensee or C/V should make available the UA information requested, including information upon which a denial or unfavorable termination of UA was based.

56. If an individual withdraws their consent, the licensee or C/V may not initiate any elements of the UA process that were not in progress at the time the individual withdrew their consent but should complete and document any elements that were in progress at the time consent is withdrawn.

57. Licensees or C/Vs should collect and maintain the following:

a. the individual's application for UA,
b. the individual's withdrawal of consent for the BI,
c. the reason given by the individual for the withdrawal, and
d. any pertinent information collected from the BI elements that were completed.

Personal History Questionnaire

58. Each individual seeking UA should do the following:

a. Complete a PHQ designed to gather the personal information for the period needed to complete the BI and SI elements.

b. Provide a self-disclosure of criminal history since their 18th birthday or since their last UA period, if terminated favorably within the past 3 years. The individual should describe in detail each legal action.

59. In making a trustworthiness or reliability determination, the willful omission, deception, or falsification of information submitted by the individual should be considered when evaluating trustworthiness and reliability of the individual to be granted UA.

60. Individuals applying for UA should be clearly informed of the potential consequences noted in regulatory guidance position C.61 of not providing complete and accurate information in their PHQ.

Note: Licensees and C/Vs should not require an individual to disclose an administrative withdrawal of UA unless the individual's UA is in an administratively withdrawn state at the time they are seeking UA, or the individual's UA was subsequently denied or terminated unfavorably by a licensee.

Verification of True Identity

61. The verification of true identity is intended to ensure that the individual being processed for UA is in fact the person they purport to be. The licensee or C/V should verify identity by doing the following:

    a. comparing valid (not expired) official photo identification (e.g., driver's license; passport; government-issued identification; State-, Province-, or country-issued certificate of birth) with the individual's physical characteristics;

    b. determining whether the results of the fingerprint check, if available, confirm the individual's claimed identity; and

    c. validating the claimed nonimmigration status and work eligibility of foreign nationals:

        (1) Licensees should confirm eligibility for employment through U.S. Citizenship and Immigration Services, verifying and ensuring, to the extent possible, the accuracy of an SSN or alien registration number.

        (2) The following U.S. Department of Homeland Security and U.S. Department of State webpages list visa categories and the attendant purposes of each visa:

            - Department of Homeland Security, "Nonimmigrant Classes of Admission" (Ref. [13]), available at https://www.dhs.gov/immigration-statistics/nonimmigrant/NonimmigrantCOA, and

            - Department of State, "Directory of Visa Categories" (Ref. [14]), available at https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/all-visa-categories.html

        (3) Because fraudulent documents in general are increasingly available, it is prudent for licensees to use a Federal database (e.g., the U.S. Department of Homeland Security's Systematic Alien Verification for Entitlements (SAVE), or E-Verify for C/Vs acting as the applicant's employer), in conjunction with the claimed nonimmigration status and work eligibility of any foreign national, to ensure the authenticity of their visa by verifying their employment eligibility and true identity.

62. The licensee or approved C/V may use its own company-issued identification to verify true identity during 10-year reinvestigations, provided the identification was issued in accordance with the requirements in 10 CFR 73.120.

Employment/Unemployment History

Employment/Unemployment Verification

63. Licensees verify employment/unemployment history for the past 7-year period, since age 18, or since the date when UA was last favorably terminated, whichever period is shortest. The licensee or C/V may obtain information and documents by electronic means, including, but not limited to, telephone, facsimile, or email. The licensee or C/V should keep records of the contents of telephone calls, as well as any documents or electronic files, for 3 years from the date when the individual no longer requires UA.

64. The verification should be conducted as follows:

    a. For initial UA, the licensee or C/V should do the following:

        (1) Verify every employment period (regardless of length) or unemployment period of 30 days or more for the most recent year preceding the application.

        (2) Verify the longest claimed period of employment for each month during years 2 and 3, as appropriate.

        (3) Conduct an SI for each month during years 2 and 3, as appropriate.

    b. For updated UA (more than 7 years but less than 10 years), the licensee or C/V should do the following:

        (1) Verify every employment period (regardless of length) or unemployment period of 30 days or more for the most recent year.

        (2) Verify the longest claimed period of employment for each month during years 2 and 3, as appropriate, preceding the application.

        (3) Conduct an SI as appropriate for the time period.

65. If an individual claims two employments of the same length in the same month, only one needs to be selected for verification. If equal periods of employment and unemployment are claimed, verify the employment period, and conduct an SI as appropriate for the time period listed.

66. For periods when the individual claims to have been on active military duty or enrolled as a student in lieu of employment, the licensee or C/V should verify military service as employment or education in lieu of employment.

67. Licensees should verify the length and nature of employment through contact with previous employers on a best effort basis. The purpose of the verification is to collect sufficient information to support a determination that the individual is trustworthy and reliable, by investigating various aspects of the employment relationship. The following information should be developed to the best of the source's ability and documented in the BI report:

    a. inclusive dates of employment period(s),

    b. for employments other than self-employment—

(1) the conditions under which the individual left the employment,

(2) reason for termination,

(3) eligibility for rehire (this criterion is not applicable if the worker is still employed by the employer listed on the application for UA when that application is completed), and

(4) any disciplinary history or other information that could affect the trustworthiness/reliability decision for UA.

c. Periods of self-employment may be verified by any reasonable method, usually one of the following:

(1) self-employment tax records,

(2) bookkeeper, accountant, or attorney,

(3) clients,

(4) employees,

(5) references,

(6) coworkers, or

(7) relatives, who may be used after methods (1)–(6) have failed to yield the information needed to verify the self-employment claim (the licensee should document the specifics of the efforts conducted for (1)–(6) before using relatives)

68. Licensees should conduct an SI of employers for the appropriate timeframe, as specified, and ask the employer the following questions:

a. For an initial UA, verify any claimed employment history and conduct an SI covering the past 3 years or since age 18, whichever period is shorter.

b. For an updated UA, verify applicable claimed employment history and conduct an SI covering the time period since the last favorably terminated UA or since age 18, whichever period is shorter.

c. While employed with [Name of Company]—

(1) Has the individual violated a licensee's or employer's policy or procedures?

(2) Has the individual been denied or terminated unfavorably from any place of employment or commercial nuclear plant for any reason?

(3) Has the individual been subject to a law enforcement authority or court of law action for any legal actions?

69. Licensees should verify activities during periods of unemployment of 30 days or more through references or relatives. SI questions need not be asked.

70. If a company or employer provides a confirmation of employment that includes the time period of the employment, or an educational institution provides a confirmation of enrollment that includes the time period of enrollment, and the company, employer, or educational institution has answered all questions in accordance with its policy on providing information, the response received from the company, employer, or educational institution should satisfy the employment verification and SI requirement if the information gained supports a positive determination of trustworthiness and reliability. All questions listed above on employment/unemployment history should be asked. The BI report should document all responses from a company, employer, or educational institution, together with the name and telephone number of each individual providing information.

    NOTE: A positive determination of trustworthiness and reliability is made when all BI elements are reviewed in context with licensee criteria and support certifying or granting UA.

71. If a company, employer, or educational institution does not meet the employment/educational verification requirements, an alternate source should be contacted and a best effort attempt made. All questions listed above on employment/unemployment history should also be asked. The BI report should document all responses from alternate sources, together with the name and telephone number of each individual providing information.

Best Effort

72. Best effort is satisfied under the following conditions, provided that the licensee has developed sufficient information upon which a trustworthiness and reliability determination can be made:

    a. A company, previous employer, or educational institution to which a request for information has been directed refuses to provide information, and this refusal is documented in the licensee's or C/V's record of the individual's BI.

    b. A company, previous employer, or educational institution to which a request for information has been directed is unable or unwilling to provide the requested information, or fails to respond. This is reflected in the licensee's or C/V's record of the individual's BI.

    c. In the event of a or b above, the licensee or C/V has documented the refusal or unwillingness in the record of investigation and has obtained a confirmation of employment or educational enrollment and attendance from at least one alternate source that the licensee or C/V has not previously used to obtain information about the individual's character. The alternate sources have answered related employment and SI questions to the best of their ability. Alternate sources may include, but are not limited to, the following:

        (1) coworkers,

        (2) supervisors, and

        (3) references (those not previously used as developed references on the current application).

d. If the licensee or C/V uses an alternate source because the requested information is not obtained from the initial request to the company, employer, or educational institution, the licensee need not delay granting an individual UA. However, the licensee or C/V should evaluate and document the response when it is received, if applicable.

e. If a source (company, employer, or educational institution) is unable to or refuses to provide requested information, and a request for information has been initiated and documented, and an alternate source (coworker, supervisor, or reference) cannot be located, one of the following secondary sources, provided by the individual or an agent of the individual, may be used to develop the length and nature of claimed employment or enrollment:

(1) pay stubs,

(2) W-2 form,

(3) wage and benefit statement,

(4) educational institution transcripts,

(5) business records confirming periods of employment or enrollment, or

(6) union contribution records used in determination of employee retirement benefits.

f. When a company, previous employer, or educational institution repeatedly refuses to provide or has a policy of not providing requested information, licensees or C/Vs are not required to continuously contact that company, previous employer, or educational institution, provided that the refusal is documented and maintained in the licensee, C/V, or BI screening company files. As an option to avoid repeatedly contacting an uncooperative employer or educational institution, the licensee or C/V may develop, or authorize a BI screening company to develop, a log of companies, employers, and educational institutions refusing to provide information. If the log is developed, it should be maintained and documented as follows:

(1) Company, Employer, and Educational Institution Policy for Verification Refusals

i. To develop the length and nature of claimed employments and education, best effort contact should be made with each company, employer, and educational institution.

ii. Initial contact with a company, employer, or educational institution to verify its policy should be documented.

iii. If a company, employer, or educational institution refuses to provide information, or has a policy of not providing information, then the licensee, C/V, or BI screening company should document the following information in a log:

(1) entity name and address,

(2) entity contact name and title,
(3) entity policy on verification requests,
(4) reason for refusal to verify,
(5) date of contact,
(6) quarterly reverification date and verification status, and
(7) entity removal date (if applicable).

iv. If the initial contact with a company, employer, or educational institution to verify information results in a refusal and is documented, the licensee should complete the best effort by initiating contact with an alternate source for verification and evaluating the resulting information. Subsequent requests for information to the same company, employer, or educational institution are not required. Alternate-source verification may be conducted immediately in lieu of contacting the company, employer, or educational institution indefinitely to complete the best effort process, as long as the refusal is reverified on a quarterly basis.

(2) Maintenance of Company, Employer, and Educational Institution Policy for Verification Refusals

i. In this context, on a quarterly basis, the licensee, C/V, or, if authorized, BI screening company should reverify the previously documented company, employer, or educational institution's refusal to provide or policy of not providing information and should document in the log the company, employer, or educational institution's current policy. In this context, quarterly is defined as once in each calendar quarter and between 60 and 120 days after the previous verification date. If the company, employer, or educational institution is no longer to be used, then its name should be crossed out in the log, and the entry should be annotated with the time/date and the initials of the individual making the removal.

ii. A licensee or approved C/V may maintain, or authorize a BI screening company to maintain, a log of companies, employers, and educational institutions that refuse to provide information or have a policy of not providing information. This log will enable the licensee to use alternate sources (as defined in regulatory guidance position C.72.c) to develop the length and nature of claimed employment or education. Licensees and C/Vs should explicitly define a process for maintaining and using such logs and should approve the logs developed by their BI screening companies. At a minimum, the process should do the following:

(1) Define how companies, employers, or educational institutions will be added to, maintained on, and removed from the list.

(2) Require verification and documentation of each entity's refusal to provide information or policy of not providing information, before the entity is added to the list.

(3) Before use, require verification that the entity's refusal to provide information or policy of not providing information has been updated quarterly.

(3) If an alternate source is used because information is not forthcoming from a given company, employer, or educational institution, no additional time is required to wait for any employer response.

(4) If a company, employer, or educational institution responds after 3 business days, the licensee should evaluate the information received.

Military Service as Employment

73. For individuals applying for UA, it is not necessary to check military service if the individual served in the Reserves or National Guard, unless the individual served on active duty beyond the annual reserve active-duty requirements as their employment.

a. Licensees should conduct an SI of the active military service period for the appropriate timeframe, as specified, by contacting the last duty station and asking the military source about the individual's service. For an initial UA, the answers should cover the past 7-year period or the period since the individual turned 18, whichever is shorter. For an updated UA, the answers should cover the period since the last favorably terminated UA. The following questions should be asked:

(1) What are the inclusive dates of the individual's military service?

(2) Under what conditions (characterization of service, e.g., honorable) did the individual separate from the military? What was the reason for separation?

(3) Would the individual be eligible to serve again?

(4) While on military duty, did the individual ever receive a court-martial or nonjudicial punishment? If so, for what reason?

(5) While serving with the [applicable branch of service]—

i. Did the individual ever violate licensee, employer, or military policy or procedures?

ii. Was the individual ever denied reenlistment or terminated unfavorably for any reason, or discharged from any military assignment for any reason?

74. The licensee or C/V should request a hand-carried copy of DD Form 214 (Ref. [15]) (or its equivalent for foreign military service) to be presented by the veteran, which on its face appears legitimate. A hand-carried copy of DD Form 214, when received, reviewed, and determined not to contain PDI that would affect the individual's trustworthiness and reliability, may be used to complete the provision for military service as employment.

a. The reviewing official should review the DD Form 214 and the SI information and compare them to the information provided by the individual on the PHQ. If there is no

PDI that would affect the individual's trustworthiness and reliability, the individual may be certified or granted UA.

75. If the individual cannot provide the requested DD Form 214, but the SI has been completed and there is no PDI that would affect the individual's trustworthiness or reliability, the individual may be granted UA if the information gained supports a positive determination of trustworthiness and reliability. Where the individual cannot provide DD Form 214, the licensee should request a copy of their DD Form 214 (or equivalent) from a custodian of military records, to complete the requirement for military service as employment.

NOTE: A positive determination of trustworthiness and reliability is made when all BI elements are reviewed in context with licensee criteria and support certifying or granting UA.

76. If the reviewing official determines that the hand-carried copy of DD Form 214 (or its equivalent) appears to have been altered in any way, the licensee should withhold UA, contact the custodian of military records, and request a certified copy of the veteran's DD Form 214 (or its equivalent).

77. If the DD Form 214 is received from the custodian of military records, the reviewing official should evaluate whether the information on it continues to support a positive determination of trustworthiness and reliability, and whether the individual's UA should be maintained.

78. Criteria for obtaining a DD Form 214 using Standard Form 180, "Request Pertaining to Military Records" (Ref. [16]), are online. If the individual's discharge, based on the DD Form 214, was an involuntary separation or anything other than honorable discharge, the licensee should investigate further.

79. In addition to verification of military service, all employments, including part-time employments and education in lieu of employment, should be verified for the most recent year for all initial and updated authorizations.

Education in Lieu of Employment

80. To verify education in lieu of employment, the licensee should conduct an SI of the relevant educational institution for the appropriate timeframe and should do the following:

    a. For an initial UA, verify education history and conduct an SI to confirm that the individual was registered for classes and received grades that indicate that they actively participated in the educational process, in lieu of employment, during the claimed period. The verification should cover either the past 7 years, or the period since the individual turned 18, whichever is shorter.

    b. For an updated UA, verify education history and conduct an SI to confirm that the individual was registered for classes and received grades that indicate that they actively participated in the educational process, in lieu of employment, during the claimed period or in the period since the last favorably terminated UA, whichever is shorter.

    c. Ask the educational source the following questions about the individual's activities while attending [name of institution]:

(1) What are the inclusive dates of the individual's attendance, that is, the dates when the individual was registered for classes and received grades at the educational institution?

(2) Under what conditions did the individual leave the educational institution? Would the individual be eligible to enroll again?

(3) Did the individual ever receive any nonacademic discipline?

(4) Did the individual violate any school or educational institution policy or procedures?

(5) Was the individual removed from the educational institution for any reason?

(6) Has the individual been subject to legal actions taken by a law enforcement authority or court of law?

81. If the educational institution will not release the requested information, this refusal should be documented, and an alternate source may be used to confirm educational institution enrollment and attendance.

82. A hand-carried copy of the individual's official transcript from the educational institution that contains the dates of attendance, courses attempted, and grades will serve to verify that the individual was registered for classes, received grades, and participated in the educational process.

83. If the reviewing official determines that the hand-carried copy of the transcript appears to have been altered in any way, the licensee should withhold UA until an official copy of the individual's transcript can be obtained from the educational institution and reviewed.

Credit Check

84. The reviewing official can use the information from a credit history check together with other BI information to evaluate an individual's reliability and trustworthiness. Credit checks are typically conducted through a U.S. national credit reporting agency and reviewed for the duration of history provided. For U.S. credit agencies, the report should include an inquiry to detect potential fraud or misuse of SSNs or other financial identifiers.

85. The information provided in a credit report may cover a different period than that specified for the BI. If the credit report does not cover the entire period specified for the BI, the interval it does cover is nevertheless sufficient; conversely, the licensee should evaluate the entire period covered by the credit report, even if it is not contained within the BI period.

86. The data in a credit report should be compared to the information in the individual's PHQ to further corroborate the employment and residence periods reported by the individual.

87. For U.S. citizens and for foreign nationals working in the United States who have established credit in the United States within the past 7 years, the licensee should conduct a credit check through a U.S. national credit reporting agency and review the information returned for the duration of history provided.

a. Licensees or C/Vs should ensure that the information provided by the credit reporting agency or source is consistent with the information provided by the individual.

b. If a discrepancy exists, further evaluation is needed. Poor repayment data alone are not typically disqualifying. However, if these data, when considered in context or jointly with other information, indicate a potential lack of integrity such that the individual's trustworthiness and reliability are not assured, then the reviewing official should deny the UA application.

c. If an individual, either a foreign national and or a U.S. citizen, has resided outside the United States and does not have an established credit history that covers at least their most recent 7 years in the United States, the licensee or C/V should document all attempts to obtain information on the individual's credit history and financial responsibility from some relevant entity located in the country or countries of the individual's residence.

Character and Reputation

88. The character and reputation of an individual is ascertained by conducting reference checks with coworkers, neighbors, or friends.

a. To ensure a broad overview of the period under investigation, persons used to verify employment/unemployment information should not be used as character references for the purposes of this check.

b. Individuals listed in the reference section of the PHQ should not be used as developed references.

89. The reference checks focus on emotional stability, trustworthiness, and reliability and are conducted as follows:

a. The individual's reputation for emotional stability, reliability, and trustworthiness is examined through interviews with at least two developed references.

(1) These references are typically developed through contact with one or more of the references listed by the individual.

(2) Developed references can be established using information provided on the PHQ (e.g., past or present employers, schools, neighborhoods, coworkers, clubs, churches).

b. An individual used as a developed reference should not have any of the following attributes:

(1) Be listed in the reference section of the PHQ.

(2) Be a known close relative (e.g., spouse, parent, sibling, or child) of the individual applying for UA.

(3) Live in the same permanent household as the individual applying for UA, a listed reference, or another developed reference at the time the application for UA is made.

c. It is not necessary for references, either individually or collectively, to have known the individual over the entire 3-year retrospective period.

(1) The references' (individual or collective) association with the individual should be substantive enough to provide meaningful information.

(2) The reference should have known the individual for at least 6 months and had at least one contact with the individual in the past 6 months.

d. Records of developed reference checks should include the following:

(1) the name of the reference,

(2) sufficient information to determine that the developed reference does not reside with individual,

(3) the length of time known,

(4) the frequency and type of association,

(5) any adverse or discrepant information,

(6) last date of contact,

(7) a statement as to whether or not the reference resides in the same household as the individual applying for UA, or sufficient information to differentiate the address of the developed and listed references from that of the applicant at the time of the application,

(8) the name of the investigator conducting the interview, and

(9) the name and phone number of the source used to obtain the developed reference's name.

e. The development of a personal reference through the use of nonperson sources (e.g., internet directories) should be fully explained in the BI record.

f. References are to be asked about their awareness of issues relating to or indications by the individual of the following:

(1) behavioral problems,
(2) unlawful/criminal activities, and
(3) any other conduct related to potential untrustworthiness or unreliability.

Criminal History Inquiry

90. Only licensee employees assigned to process UA applications may access or review FBI criminal history record information (CHRI). The licensee process should preclude other individuals (e.g., contractor or vendors who are not licensee employees) from accessing, reviewing, and disseminating the FBI CHRI.

    NOTE: This is based on a letter to the NRC dated October 24, 1997 (ML12110A327) (Ref. [17]), from the FBI Criminal Justice Information Services Division, and on the access authorization requirements in 10 CFR 73.56(a)(4).

91. The licensee must evaluate CHRI pertaining to an individual applying for UA as required by 10 CFR 37.27. The CHRI check is used as an evaluative measure to help determine whether the individual has a record of criminal activity that may adversely affect their trustworthiness and reliability.

92. CHRI evaluations, including the decision-making basis for them, should be documented.

93. If a C/V discovers information that is different from that originally claimed by an individual applying for UA, the C/V should provide the investigation results to the licensee before or when UA is requested.

94. Licensees need not fingerprint official U.S. Government personnel who can be verified to have Q or L clearances or other active government-granted security clearances (e.g., Top Secret, Secret, or Confidential).

    a. Clearance confirmations should be received from the sponsoring agency (i.e., the NRC or the facility) and not hand-carried by the individual applying for UA.

    b. Verification of these active clearances may also be used in lieu of the FBI CHRI for reinvestigation.

95. If FBI CHRI results cannot be obtained because fingerprints are nonclassifiable, licensees should implement the process defined in appendix A.

96. An FBI CHRI evaluation need not be conducted for initial or updated authorizations, if completed within the past 365 days.

Reinvestigations

97. Only licensee employees assigned to process UA applications may access or review FBI CHRI. The licensee process should preclude other individuals from accessing, reviewing, and disseminating the FBI CHRI.

98. If applicable, submissions of fingerprints for reinvestigations should be handled separately from investigations for outage staffing (only if applicable), to preclude inadvertent outage staffing delays.

99. The guidance in this section applies to all individuals with UA. Individuals with UA who do not satisfy the reinvestigation requirements in 10 CFR 73.120 should have UA administratively withdrawn until the reinvestigation has been completed.

100. All personnel holding UA must have a reinvestigation completed at intervals not to exceed 10 years, pursuant to 10 CFR 73.120(c)(4).

101. A new consent form to screen and an authorization statement form should be completed before accomplishing a reinvestigation.

102. The reinvestigation conducted includes a review of CHRI obtained as provided in 10 CFR 37.27 or as the Commission may require. The licensee reviewing official should compare CHRI with the access authorization records of the person named in the record to ensure the person has complied with self-reporting requirements.

103. The start of the interval for the next reinvestigation should be the date when the licensee reviewing official completed a review of criminal history.

104. The licensee reviewing official should review the results of the criminal history update and supervisory review. If PDI is discovered during any reinvestigation review, the information should be evaluated by the licensee reviewing official and addressed according to licensee policy and procedures to determine the individual's trustworthiness and reliability for maintaining UA.

105. If the criminal history update and reevaluation have not been completed and the information evaluated by the licensee reviewing official within the required 10-year period, or within the time period specified in the licensee's physical security plan, the licensee should administratively withdraw the individual's UA until these requirements have been met.

106. If a licensee finds it challenging to fully implement the reinvestigation requirements because of difficulties in obtaining information from Federal, State, or local agencies that may be closed or have reduced or sequestered staff because of a public health emergency, the licensee may pursue alternatives for capturing fingerprints on a best effort basis. This only applies to individuals who are maintaining or updating UA, whose last fingerprint evaluation was within the past 365 days, whose true identity can be verified by the holding licensee, and for whom, if applicable, the licensee has dispositioned any reported legal actions in support of a positive finding to maintain UA.

Behavioral Observation

107. The licensee's or C/V's licensee-approved BO initiatives play a role in determining the continued trustworthiness and reliability of covered individuals.

a. Licensees must establish BO within their approved access authorization program for anyone granted or maintaining UA, in accordance with 10 CFR 73.120(c)(2).

b. Licensees should inform personnel who maintain UA of their roles and responsibilities in reporting behaviors or activities that may constitute an unreasonable risk to the safety and security of the facility. Personnel should do the following:

(1) Responsibly detect behaviors adverse to the safe operation and security of the facility, and report them either in the workplace, or to any individual whose duties and responsibilities permit them to take action by electronic means, either on site or remotely. This includes instances of behavior addressed in the licensee or C/V disciplinary process that would lead to unfavorable termination or resignation in lieu of termination. Personnel should report and evaluate legal

actions taken by a law enforcement authority or court of law to which the individual has been subject that could result in incarceration or a court order or that require a court appearance. Such actions include, but are not limited to, an arrest, an indictment, the filing of charges, or a conviction, but exclude minor traffic violations such as parking or speeding tickets.

(2) Provide all reports under the BO to the licensee reviewing official.

108. The following individuals are subject to BO:

a. any individual to whom a licensee intends to grant UA to a commercial nuclear plant protected area, vital area, or controlled access area where the radioactive material is used or stored;

b. any individual whose duties and responsibilities permit them to take actions by electronic means, either on site or remotely, that could adversely affect the licensee's operational safety, security, or emergency response capabilities;

c. any individual who has responsibilities for implementing a licensee's protective strategy, including, but not limited to, armed security force officers, alarm station operators, and tactical response team leaders, but not including Federal, State, or local law enforcement personnel;

d. the licensee access authorization program reviewing official or C/V access authorization program reviewers; and

e. other individuals, at the licensee's discretion, including C/V employees who are designated in access authorization program procedures or implement an access authorization program in accordance with this RG.

109. Personnel subject to a BO program are responsible for the following:

a. observing personnel for behavior traits and patterns that may reflect adversely on their trustworthiness or reliability;

b. demonstrating awareness of behaviors that might be adverse to the safe operation or security of the facility;

c. reporting observed behaviors of individuals that may adversely affect the safety or security of the facility, or that may constitute an unreasonable risk to public health and safety or to the common defense and security; and

d. reporting observations to appropriate licensee or C/V management in accordance with the licensee's or C/V's procedures.

110. Licensees, C/V management, and reviewing officials have the following responsibilities:

a. Personnel receiving BO reports or appropriate licensee or C/V management personnel should ensure that the licensee reviewing official is formally made aware of the observations.

b. The reviewing official should review the facts of the reported observation to determine whether or not to continue the UA.

c. If the reviewing official has a reason to question the reported individual's trustworthiness or reliability, the reviewing official should either administratively withdraw or terminate the individual's UA while completing a reevaluation or investigation.

d. Ensure personnel who maintain UA, are covered under the BO elements and are required to comply with the licensee's policies and procedures.

111. Under 10 CFR 73.120(c)(2)(ii), BO must include visual observation, in person or remotely by video, to detect and promptly report to plant supervision any concerns, including but not limited to questionable behavior patterns or activities.

a. Remote access can be used as an alternative to face-to-face interaction, maximizing flexibility when personnel are located off site or sequestered.

b. Video conferencing or other acceptable electronic means promoting face-to face interaction for individuals working remotely meets the intent of this regulation.

112. Integral to the licensee's BO elements for all employees is an annual management review of employee behavior, conducted by a reviewing official and the employee's supervisor. This review enables interaction between the reviewing official and their designee (i.e., the employee's immediate supervisor) and the employee, letting the supervisor become aware of any condition that may cause the employee to act or behave unconventionally. The review also lets the supervisor consider whether it may be necessary to refer the employee for additional medical or psychological assistance.

a. In addition to the requirements noted above, a review may incorporate information developed over the covered period (i.e., the previous year) about the employee's behavioral characteristics. This information would typically include deviations from the behavioral norm that have been reported to the reviewing official or supervisor through the implementation of BO, as well as deviations personally observed by the reviewing official or supervisor.

b. This review serves two purposes:

(1) It may identify potential issues that, left unattended or unaddressed, could lead to behaviors or activities that constitute an unreasonable risk to public health and safety or to the common defense and security.

(2) It may identify issues related to trustworthiness and reliability, other than those related to physical or mental impairment.

113. The licensee and, if appropriate, C/V should ensure that licensee and C/V personnel have sufficient awareness and sensitivity to detect degradation in their own performance that may adversely affect their ability to perform their duties safely and competently.

114. The licensee's BO elements should provide personnel with the awareness and abilities necessary to recognize behavior or activities that could constitute an unreasonable risk to public health and safety or to the safety and security of the facility.

115. Behaviors adverse to the safe operation and security of the facility include unusual interest in or predisposition towards security or operations activities outside the scope of one's normal work assignments, and frequent unexplained absence from work assignments.

Legal Action Reporting

116. Licensees must establish a legal action reporting program under 10 CFR 73.120(c)(3). The objective of the legal action reporting program is to report and evaluate legal actions taken by a law enforcement authority or court of law to which the individual has been subject that could result in incarceration or a court order or that requires a court appearance. Such actions include, but are not limited to, an arrest, an indictment, the filing of charges, or a conviction, but they exclude minor traffic violations such as parking or speeding tickets.

117. The legal action reporting program should do the following:

    a. Require individuals with UA to report any legal actions to which they have been subject.

    b. Notify individuals in writing of their responsibility to make this report and to whom.

    c. Provide sufficient guidance in the written notification so that an individual's reporting responsibility is clear, including a warning that failure to report could result in the denial or unfavorable termination of UA. Individuals are responsible for complying with the written notification.

118. The legal action reporting element should require an individual to report any legal actions that occur while they maintain UA at the commercial nuclear plant, for the period between the granting of UA and the 10-year reinvestigation.

    a. Legal actions reported by the individual should be documented and retained with the UA records on which the initial UA decision was based.

    b. The reviewing official should evaluate all legal action information received.

    c. The recipient of the legal action report, if other than the reviewing official, should promptly convey the report to the reviewing official.

    d. On the day that the report is received, the reviewing official should evaluate the circumstances related to the reported legal action(s) and redetermine the reported individual's UA status.

Reviewing Official Annual Review

119. Under 10 CFR 73.120(c)(4), UA determinations must be reviewed annually by the reviewing official. Reviewing official reviews should be conducted on a nominal annual basis for each individual granted UA for a period of at least 365 consecutive days.

120. Reviewing official annual reviews are not required for individuals whose UA has been terminated or administratively withdrawn before the end of the continuous 365-day period. Licensees are not required to provide the status of the reviewing official annual review to other licensees. The review should be based on interactions with the individual over the review period and need not involve immediate or face-to-face interaction.

121. The annual review should be conducted by the individual's immediate supervisor and provided to the reviewing official for determination, as defined in the licensee's or approved C/V's BO procedures. The review should be based on interactions with the individual over the review period. The review should include the following:

a. descriptions of any conditions that may have led the employee to act or behave unconventionally, including discipline and actions taken;

b. any circumstances that could indicate the need to refer the employee for additional medical or psychological review; and

c. any information developed over the review period on the employee's behavioral characteristics (typically including behavioral norm deviations that were either reported to the supervisor through implementation of BO or personally observed by the supervisor).

122. When PDI is identified, an access authorization program reviewing official should evaluate the reviewing official annual review to determine whether additional action is required to establish the individual's trustworthiness and reliability for maintaining UA.

123. The completed review should be included as part of the licensee's or C/V's access authorization files and retained in accordance with 10 CFR 73.120(c)(10) and the guidance in regulatory guidance positions C.203–C.210.

124. If a reviewing official annual review is not completed as required, UA should be administratively withdrawn until all requirements are satisfied. If a licensee or other entity cannot meet this requirement, the licensee should document the incident for inspection purposes. Personnel who cannot be assessed visually in person or through video conferencing should have their authorization removed until they can be so assessed.

125. If the reviewing official or the immediate supervisor does not have frequent interaction with the individual throughout the review period as needed to form an informed and reasonable opinion of their behavior, trustworthiness, and reliability, the review should be performed on a best effort basis and documented accordingly.

Unfavorable Employment Terminations

126. For any person granted UA, the licensee should have a process that requires the licensee reviewing official to review the facts involved in an unfavorable employment termination or resignation in lieu of termination.

127. The licensee's review policy and procedures should determine whether the behavior that an employer cites as the reason for unfavorable termination or resignation in lieu of termination may also make the individual untrustworthy or unreliable and therefore ineligible for continued UA.

128. If the individual's UA is denied or terminated unfavorably, the licensee should notify any other licensee with which the individual holds active UA.

Other Required Background Screening

129. BI screening of additional personnel, other than individuals applying for UA, may include the following:

a. BI screening company personnel, and
b. personnel assigned to process UA applications.

130. Licensees and C/Vs should verify the trustworthiness and reliability of any individual who collects, processes, or evaluates personal information for the purpose of processing UA applications; who has access to the files, records, and personal information associated with individuals who have applied for UA; or who is responsible for managing any databases that contain such files, records, and personal information. This determination should be made as follows:

a. The individual is subject to an access authorization program as defined in this document or to a comparable access authorization program under 10 CFR Part 37 or 10 CFR Part 73.

b. The individual may be subjected to either (1) a local criminal history check (for personnel not requiring UA to the commercial nuclear plant) or (2) the FBI criminal history check requirements under 10 CFR 37.27. A local criminal history check is based on information obtained from an appropriate State court or agency, or a court or agency of the county, borough, or parish in which the individual is a permanent resident.

Background Investigation Screeners

131. If a licensee or C/V uses persons not directly under its control to collect and process information that the reviewing official will use to make trustworthiness and reliability determinations, such persons should be known to be trustworthy and reliable. This includes persons responsible for data management for C/Vs and subcontractors.

132. The requirements should appear in the contract for the work and should include, at a minimum, the following:

a. consent,

b. verification of the individual's true identity,

c. an employment/unemployment history review and evaluation covering the past 3 years,

d. an evaluation of character and reputation through interviews of two developed references, and

e. a local criminal history review and evaluation, based on information obtained from an appropriate State court or agency, or a court or agency of the county, borough, or parish in which the individual is a permanent resident.

(1) If an FBI CHRI is conducted in accordance with the requirements under 10 CFR 37.27, a local criminal history check is not required.

(2) However, if the personnel will not hold UA or have access to safeguards information, an FBI criminal records check may not be conducted, and the local criminal records check should include the location of the individual's permanent residence.

133. If an individual covered by this section is determined to have left the employment of the BI screening company for a period of less than 365 days, then returned to these covered job duties, the BI screening company should ascertain the individual's activities and conduct an employment/unemployment check on a best effort basis for the period of interruption of employment, in order to ensure continued trustworthiness and reliability.

134. Individuals returning after a lapsed period greater than 365 days should be required to undergo screening for initial UA.

Personnel Processing Applications

135. An individual not already covered by the access authorization program who performs duties to process UA applications should meet the licensee's or C/V's standards for trustworthiness and reliability for the access authorization program. This includes individuals who—

a. evaluate personal information for the purpose of processing individuals for UA,
b. have unfettered access to the files and records of persons applying for or holding UA, or
c. are responsible for managing data upon which UA decisions may be based.

136. For individuals not covered by a licensee or approved C/V UA program, the employer should collect and adjudicate sufficient background information to provide reasonable assurance that the individual is trustworthy and reliable to perform duties related to proper handling of information, records, and databases entrusted to them. The program should include the following elements:

a. consent for the investigations,

b. evaluation of a completed PHQ (initial),

c. verification of true identity,

d. employment/unemployment history verification,

e. character and reputation evaluation, and

f. evaluation of a local criminal history check that includes the individual's permanent residence.

(1) If an FBI CHRI is conducted, a local criminal history check is not required.

(2) However, if the personnel will not hold UA or have access to safeguards information, an FBI criminal records check may not be conducted, and the local criminal records check should include the location of the individual's permanent residence.

137. If an individual covered by this section is determined to have left the employment of the licensee or approved C/V for a period of less than 365 days, then returned to these covered job duties, the

licensee or approved C/V should ascertain the individual's activities and complete the requirements of an employment/unemployment history verification for the period of interruption of employment, in order to ensure continued trustworthiness and reliability.

138. Individuals returning after a lapsed period greater than 365 days should be required to undergo initial screening for UA, covering the entire period since the individual left the company.

Licensee Shared Information

139. Key access authorization information should be accessible by other power reactor licensees, if applicable. However, this information could extend to other entities subject to 10 CFR 73.56 or 10 CFR 73.120 that have agreed to participate in the industry information-sharing program. This section defines the minimum elements that should be made available by licensees or other entities to meet requirements of an access authorization program. If a licensee or entity chooses to use an industry database to share access authorization determination, it may also request additional information to facilitate data management.

140. Licensees and C/Vs that have been authorized (by a licensee or through contractual agreements) to add or manipulate data in an information-sharing mechanism should ensure the retention in the information sharing mechanism of any data linked to the information specified in the licensee's access authorization program documents for individuals who have applied for UA.

141. If the shared information used for determining an individual's trustworthiness and reliability changes, or if new or additional information is developed about the individual, the licensees or C/Vs that acquire this information should correct or augment the data contained in the information-sharing mechanism.

142. If the changed, additional, or developed information may adversely affect an individual's trustworthiness or reliability, the licensee or C/V that discovered or obtained the new, additional, or changed information should, on the day of discovery, provide the updated information to the reviewing official of any licensee access authorization program under which the individual is maintaining their UA status.

143. The receiving reviewing official should evaluate the information and take appropriate actions, which may include denial or unfavorable termination of UA.

144. If the information-sharing mechanism is unavailable and a notification of changed or updated information is requested, licensees and C/Vs should take manual actions to ensure that the information is shared and should update the data in the information-sharing mechanism as soon as reasonably possible.

145. Records maintained in the database should be available for NRC review and inspection.

NOTE: Data pertaining to NRC employees is not required to be entered into the industry's information-sharing mechanism. Data pertaining to NRC contractors should be entered into the industry's information-sharing mechanism, because licensees are frequently requested to augment previously established data elements when making a UA current for the NRC contractor.

Request for Access Withdrawn

146. In some cases, a request for access is withdrawn before the BI is completed because the individual no longer needs UA. This may result from a variety of reasons, such as changes in work assignment or completion of the expected job, and should not be confused with a withdrawal of consent.

    a. If the individual no longer needs access, the BI does not need to be continued.

    b. No information is required to be shared if the request for access is withdrawn before any BI element was completed and no PDI is discovered.

147. The evaluation of specific PDI pertaining to persons who have not formally applied for UA is not permitted.

148. If the individual leaves the licensee's control before adjudication of PDI, an "Admin Data" entry and the company holding the "Admin Data" should be listed.

    CAUTION: If a licensee administratively withdraws an individual's UA status because of a delay in completing any portion of the BI, or for a licensee-initiated evaluation or reevaluation that is not under the individual's control, the licensee should record this administrative action to withdraw the individual's UA in the information-sharing mechanism.

    a. Licensees should not document this administrative withdrawal as denial or unfavorable termination, nor should they identify it as denial or unfavorable termination in response to an SI, a BI, or any other inquiry or investigation.

    b. Immediately upon favorable completion of the BI element that caused the administrative withdrawal, the licensee should ensure that any matter that could link the individual to the administrative action is eliminated from the individual's access authorization or personnel record and other records, except if a review of the information obtained or developed causes the reviewing official to unfavorably terminate or deny the individual's UA.

Individual Withdraws Consent

    NOTE: Licensees should document and maintain, within their own records, the reason for withdrawal of consent.

149. For an individual withdrawing consent, the only information to be shared is the following:

    a. the date when consent was withdrawn, and
    b. the name of the company holding the withdrawal request.

150. If an individual withdraws their consent, the licensee or C/V may not initiate any elements of the UA process specified in this document that were not in progress at the time when the individual withdrew their consent but should complete and document any elements that were in progress when consent was withdrawn.

151. The licensee or C/V should record the following:

a. the status of the individual's application for UA,

b. their withdrawal of consent, and the reason given for the withdrawal, if any, and

c. any pertinent information gathered from the elements that were completed (e.g., from the criminal history check or the SI).

152. The licensee to which the individual applied for UA should inform the individual of the following:

a. Withdrawal of consent will withdraw the individual's current application for UA under the licensee's access authorization program.

b. Other licensees and entities will have access to information documenting the withdrawal through the information sharing that is required under 10 CFR 73.120.

153. The licensee or approved C/V should inform, in writing, any individual who is applying for UA that the following actions are sufficient cause for denial or unfavorable termination of UA when consent is withdrawn or not reported by the individual:

a. refusal to provide written consent for the SI;

b. refusal to provide, or falsification of, any personal information required under 10 CFR 73.120, including, but not limited to, failure to report any previous denial or unfavorable termination of UA;

c. refusal to provide written consent for the sharing of personal information with other licensees or C/Vs that is required under 10 CFR 73.120; and

d. failure to report any legal actions.

Individual in a Denied Status

154. Access denial may occur as a result of the preaccess BI or when an individual's UA is terminated unfavorably. Access denial may also occur for an individual who is found not to be trustworthy and reliable, or who has violated a licensee or C/V policy while under BO used to maintain UA elements current.

155. In addition, the failure of a licensee to obtain consent before the denial of UA does not reduce the requirement to share the denial data with other licensees or C/Vs.

156. Information to be shared includes the following:

a. date UA denied, and

b. company holding the "additional information." "Additional information" is defined as the specific information that a previous licensee or utility may have or developed on an individual who last held UA at their facility. This information can only be transferred to another licensee or an agent of the licensee if a written consent is on file.

157. If an individual's access was restored at some later date, licensees should ensure that the current UA information is also listed. This information is needed to clearly establish which individuals currently have access-denied status.

Unescorted Access Denial Review Process

158. The licensee should describe the UA denial process to be used in the procedure that implements the requirement for a UA denial review process. The procedure must reflect that the determination from the denial review is final.

    a. Additionally, in accordance with 10 CFR 73.120(c)(7) and 10 CFR 37.23(f), procedures must include provisions for the review, at the request of the affected individual, of a denial or unfavorable termination of UA that may adversely affect employment.

    b. Licensees should not grant UA or permit the individual to maintain UA during the review process.

    c. All information pertaining to a denial or unfavorable termination of the individual's UA should be provided promptly, upon receipt of a written request by the subject individual or their designated representative (as designated in writing). The licensee may redact the information to be released to prevent the disclosure of personal privacy information pertaining to another individual, including the name of the source of the information.

    d. Licensee programs are not intended to modify, subjugate, or abrogate any review rights that currently exist for C/V employees with their respective employers. However, in all cases, whether to grant or deny UA to an individual at a licensee's facility is that licensee's decision to make, regardless of whether the individual satisfies some other C/V or licensee UA program requirements.

159. The licensee should have a review process that provides the following for any individual whose UA is denied:

    a. the basis for denial or revocation of UA,

    b. the opportunity to respond and provide any additional relevant information, and

    c. the opportunity to have the decision, and any additional information, objectively reviewed by a management-level employee of the licensee whom the licensee has designated to review UA denials, who holds position titles that are equivalent to or senior to those of the individual who made the initial decision to deny or unfavorably terminate UA, who is not a member of the access authorization program staff, and who will conduct an impartial and independent internal management review of the UA denial or termination decision

160. The UA decision of the licensee's initial reviewer or, if applicable, the decision from the licensee's internal management review process is final, should be the exclusive means by which UA decisions may be reviewed and may not be reviewed or overturned by any third party.

161. If the review finds in favor of the individual, the licensee should update the relevant records to reflect the outcome of the review and delete or correct all information the review found to be inaccurate.

162. When a C/V is administering an access authorization program on which licensees and other entities rely, and the C/V determines that its employee or subcontractor no longer meets the access authorization elements after a licensee company has granted UA, the C/V should notify the licensee granting UA and provide all relevant information to the licensee. The licensee that granted UA should review the information and, if a denial of UA is warranted, provide the individual with a review process.

Individuals Currently Denied Access

163. Except for personnel responding to emergency conditions (e.g., ambulance, fire, law enforcement response) and NRC employees, visitors should be checked against the industry's database or a comparable site access list to make sure that they are not currently denied access. The check for each visitor will be performed at least once daily (with a day defined as spanning 00:01–24:00 hours) before the individual's first daily entry into the protected area, vital area, or controlled access area.

164. Persons currently denied UA at a licensee facility should not be allowed in the protected area of any licensee facility, except under the following conditions:

    a. The denying licensee reviews its UA denial and determines after further review that UA authorization would now be appropriate.

    b. Another licensee reviews the conditions under which the denying licensee made the denial decision, and determines that the individual is now trustworthy and reliable and that UA authorization would be appropriate at the current licensee site.

    c. If an individual is identified as having access-denied status in the information-sharing mechanism or a comparable site access list, licensees should not permit the individual to enter any commercial nuclear plant protected area or vital area with or without escort of another licensee personnel who has been appropriately cleared through this RG. If the individual is identified as having an access authorization status other than favorably terminated (excluding a denial) as their most current industry status, licensees should limit the individual's UA until the licensee reviewing official evaluates the circumstances and determined that such access is warranted.

    d. If a licensee is aware of information about an individual that characterizes the individual as untrustworthy or unreliable for UA under its program, the licensee reviewing official should evaluate the information and determine whether to allow the individual escorted access.

Program Reliability

165. Licensees should ensure that any violation of an access authorization program element at one licensee or C/V is identifiable to all licensees, to the extent that, at the time of the discovery, persons holding UA who were the subject of, or included in, any program element violation at any licensee or C/V are identified by that licensee. This information should also be provided to any licensee where that person holds UA.

166. Licensees and C/Vs should ensure that only correct and complete information about individuals is retained and shared with other licensees and entities. If, for any reason, the shared information used for determining an individual's eligibility for UA changes or new information is developed

about the individual, licensees and other entities should correct or augment the shared information in the records. If the changed or developed information may adversely affect an individual's eligibility for UA, the licensee or C/V that discovered the incorrect information or developed the new information should provide the updated information to the reviewing official of any licensee under which the individual is maintaining UA, on the day of discovery. The reviewing official should evaluate the information and take appropriate actions, which may include denial or unfavorable termination of the individual's authorization.

167. If issues arise that affect the BI of an individual, or a group of individuals, the licensee should promptly take appropriate action to correct the deficiency, such as withdrawing UA or correcting the investigation element. The intent of this section is to ensure that when this is necessary, any other licensees relying on the shared information are informed so that they can take appropriate action. Correcting the shared information ensures that future UA decisions are based on valid information.

Backup or Manual Process for Sharing Information

168. In case of a failure of the industry electronic database, a backup process of manual information exchange is acceptable for short -term use. When the manual process is used, information should be entered into the database within a day after the database is restored.

169. The manual process can also be used to share information with, or obtain information from, facilities outside the scope of this document, such as decommissioned plants. Licensees using this process should ensure that any screening information received from these facilities meets regulatory requirements before entering the information into the industry database.

Audits

170. Each licensee should be responsible for the continuing effectiveness of its access authorization program, including access authorization program elements that are provided by C/Vs, and of the access authorization programs of any C/Vs that the licensee accepts.

171. Audits should be conducted by the licensee or the licensee's C/V's subcontractors. They should focus on the effectiveness of the access authorization program or program elements, as appropriate, and any corrective actions taken to correct nonconformances should be verified as being effective.

Audits performed by other licensees may be relied upon for acceptance of results and associated evaluation, provided the scope of the audit meets regulatory requirements.

Licensees relying on audit results should obtain and review a copy of the audit report, to include findings and corrective actions, and should retain these evaluation records for at least 3 years.

In addition, a licensee -approved C/V may rely on licensee -conducted audits of a background screener or subcontractor, provided the licensee agrees in advance to cover the scope of the C/V program.

172. Licensees may jointly conduct audits of C/Vs, or accept audits of C/Vs conducted by other licensees, if these audits address the scope of services obtained from the C/V. In addition, C/Vs may jointly conduct audits of subcontractors, or may accept audits of subcontractors that were

conducted by licensees or other C/Vs that are subject to this section, if these audits address the scope of services obtained from the subcontractor.

173. Audit results and any recommendations should be documented in the site corrective action program and reported to senior management having responsibility in the area audited and to management responsible for the access authorization program. Each audit report should identify any conditions adverse to the proper implementation of the access authorization program, the causes of such conditions, recommended corrective actions (when appropriate), and corrective actions taken. The licensee or C/V should review the audit findings and take any additional corrective actions, including re-auditing of the areas of deficiency where indicated, to preclude, within reason, repetition of the deficiency. The resolution of the audit findings and corrective actions should be documented.

174. Licensees and C/Vs should review audit records and reports to identify any areas that were not covered by the shared or accepted audit. If the shared audit did not address certain program elements or services upon which the licensee or C/V relies, additional measures should be taken to ensure that the elements or services are audited.

175. If a shared audit addresses the required scope, sharing licensees or C/Vs need not re-audit the same C/V or subcontractor for the same period of time.

176. Each sharing licensee and C/V should maintain a copy of the shared audit, including findings, recommendations, and corrective actions.

Licensee Program Audits of Unescorted Access Program

177. The initial audit of a licensee's UA program and its conformance to this document should be performed within 12 months of the effective date of implementation of this document or the access authorization program.

178. Follow-up audits are nominally conducted at an interval of every 24 months.

179. Licensees are responsible for determining the appropriate frequency, scope, and depth of additional auditing activities within the nominal 24-month period, based on the review of program performance indicators such as the frequency, nature, and severity of discovered problems; personnel or procedural changes; and previous audit findings.

180. The individuals performing the audit of the access authorization program or program element(s) should be independent both from the management of the subject access authorization program and from personnel who are directly responsible for implementing the access authorization program or program elements being audited. The audit should cover the full scope of the access authorization program.

181. The audit team should include a person who has experience in access authorization program administration.

182. The audit team should include a person knowledgeable and practiced in access authorization program administration. This person should be responsible for verifying that overall program performance is meeting the objective of screening individuals to provide high assurance that they are trustworthy and reliable to have or maintain UA.

183. The audit report should be provided to licensee management and should include any findings and corrective actions.

Licensee-Approved Contractor/Vendor Screening and Background Screening Company Programs

184. Licensee contracts with C/Vs should reserve the licensee's right to audit the C/V and the C/V's subcontractors providing access authorization program services at any time, including at unannounced times, and to review all information and documentation that is reasonably relevant to the performance of the program.

185. Licensee contracts with C/Vs and C/V contracts with subcontractors should also request that the licensee have access to and be permitted to take away copies of any documents or data that may be needed to verify that the C/V and its subcontractors are performing their functions properly and that staff and procedures meet applicable requirements.

186. The licensee or its designated representative should conduct audits of its approved C/V's UA programs, background screening companies, and other service providers that are off site or are not under the direct daily supervision or observation of the licensee's personnel, to ensure compliance with the criteria specified in this document. The audits should be conducted on a nominal 12-month frequency.

187. Licensees and C/Vs are responsible for determining the appropriate frequency, scope, and depth of additional auditing activities within the nominal 12-month period based on the review of program performance indicators, such as the frequency, nature, and severity of discovered problems; personnel or procedural changes; and previous audit findings.

188. A member of the audit team should be knowledgeable and practiced in access authorization and should be responsible for validating that overall program performance is meeting the objective of screening individuals to provide reasonable assurance that they are trustworthy and reliable to have or maintain UA.

Contractor/Vendor Internal Audit and Contractor/Vendor Audit of Subcontractors

189. Any access authorization program services that are provided to C/Vs by subcontractor personnel who are off site or are not under the direct daily supervision or observation of the C/V's personnel should be audited by the licensee or C/V on a nominal 12-month frequency.

190. C/V contracts with subcontractors providing access authorization program services should reserve the licensee's and C/V's right to audit the subcontractors at any time, including at unannounced times, and to review all information and documentation that is reasonably relevant to the performance of the program.

191. C/V contracts with subcontractors should request that the licensee or C/V be provided access to and be permitted to take away copies of any documents or data that may be needed to verify that the subcontractors are performing their functions properly and that staff and procedures meet applicable requirements.

192. Each licensee-approved C/V will conduct an audit of its own UA programs, including any subcontractors that conduct BIs, on a nominal 12-month frequency. The audit should focus on the effectiveness of the access authorization program or program element(s), as appropriate.

193. For a C/V's internal audits and audits of its subcontractors, no knowledgeable and practiced person is required.

Records and Protection of Information

194. Licensees and C/Vs should ensure that only correct and complete information about individuals is retained and shared with other licensees and entities. If, for any reason, the shared information used for determining an individual's eligibility for UA changes or new information is developed about the individual, licensees and other entities. should correct or augment the shared information in the records. If the changed or developed information may adversely affect an individual's eligibility for UA, the licensee or C/V that discovered the incorrect information or developed the new information should provide the updated information to the reviewing official of any licensee under which the individual is maintaining UA, on the day of discovery. The reviewing official should evaluate the information and take appropriate actions, which may include denial or unfavorable termination of the individual's authorization.

195. The records upon which UA is based or denied are not quality records (such as defined in American National Standards Institute (ANSI) N45.2.9-1979, "Requirements for Collection, Storage, and Maintenance of Quality Assurance Records for Nuclear Power Plants" (Ref. [18])), and therefore do not require the protection afforded quality records.

196. Licensees, C/Vs, and any individual or organization that collects and maintains personal information on behalf of a licensee or C/V should establish, use, and maintain a system of files and procedures for the protection of personal information, including personal information stored in electronic format, and for the secure storage and handling of the information collected.

197. This information should not be disclosed to unauthorized persons. Before disclosing any information collected and maintained for the purposes of granting UA, licensees and C/Vs should obtain signed consent from the subject individual that authorizes the disclosure of such information.

198. Records may be stored and archived electronically, provided that the method used to create the electronic records meets the following criteria:

    a. provides an accurate representation of the original records,

    b. prevents unauthorized access to the records,

    c. prevents the alteration of any archived information or data once it has been committed to storage, and

    d. permits easy retrieval and recreation of the original records.

199. For information stored or transmitted in electronic format, access to personal information will be controlled by the following:

    a. password protection to control access to personal data,
    b. limitation of data entry to each authorized individual's area of competency, and
    c. procedural controls.

200. When a record or electronic media meets the retention criteria and is determined to no longer be required, it should be disposed of in a way that prevents unauthorized disclosure of the information. Methods include, but are not limited to, shredding, burning, and pulverizing.

201. A contract with any individual or organization that collects and maintains personal information that is relevant to a UA determination should request that such records be held in confidence.

202. Upon termination of a contract between a C/V and a licensee, the C/V should provide the licensee with all records collected for the licensee.

Records Retention

203. Under 10 CFR 73.120(c)(10), licensees and C/Vs must maintain the records that are required by 10 CFR 73.120 for the period specified by the appropriate regulation. If a retention period is not otherwise specified, these records should be retained until the NRC terminates the facility's license, certificate, or other regulatory approval. Records should be retained for a designated period of time, as follows.

204. A licensee or C/V should retain the following documents, or their equivalents, for 3 years after favorable termination of UA by the licensee making the UA determination, or until the completion of all related legal proceedings, whichever is later:

a. Industry STD FORM, "Consent";

b. Industry STD FORM, "Personal History Questionnaires for Initial, Updated, Reinstated Authorizations and Reinvestigation Including Self-Disclosure Information";

c. BI records that record the conduct of the following:

(1) true identity verification;

(2) employment/unemployment history (including military service and education in lieu of employment), SI, or best effort (including verification of self-disclosure information);

(3) verification of character and reputation;

(4) FBI criminal history check; and

(5) reviewing official determination;

d. records pertaining to the determination of a violation of access policy and related management actions;

e. documentation of the granting, reinvestigation, and termination of UA; and

f. records of annual supervisory reviews.

205. After a denial or unfavorable termination of UA, the licensee making the denial or unfavorable termination of UA should retain all documents listed above, or their equivalents, for 3 years or until all related legal proceedings have been concluded.

206. After a 3-year or permanent denial of UA, the licensee making the denial or unfavorable termination of UA should retain all documents listed above, or their equivalents, for 40 years or until the NRC determines that the records are no longer needed.

207. The following records should be maintained for 3 years: records of audits, audit findings, and corrective actions taken under 10 CFR 73.120.

208. Written agreements with a provider of services should be retained for the life of agreement plus 3 years, or until completion of all proceedings related to a denial or unfavorable termination of UA that involved those services, whichever is later.

209. For access authorization program personnel, licensees and C/Vs should retain records of BIs, supervisory reviews, and BO-related actions for the length of the individual's employment by or contractual relationship with the licensee or C/V and for 3 years after the termination of employment, or until the completion of any proceedings related to the individual's actions, whichever is later.

210. Licensees and C/Vs that have been authorized to add or manipulate data that are shared with licensees subject to this RG through an information sharing mechanism should ensure that any data linked to the information specified in the licensee's access authorization program documents for individuals who have applied for UA are retained for the period specified in the licensee's procedures or for 3 years after termination of contractual services.

211.

D. IMPLEMENTATION

The NRC staff may use this regulatory guide as a reference in its regulatory processes, such as licensing, inspection, or enforcement. However, the NRC staff does not intend to use the guidance in this regulatory guide to support NRC staff actions in a manner that would constitute backfitting as that term is defined in 10 CFR 53.1590, "Backfitting," and as described in NRC Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests" (Ref. [19]), nor does the NRC staff intend to use the guidance to affect the issue finality of an approval under 10 CFR Part 53, Subpart H, "Licenses, Certifications, and Approvals." The staff also does not intend to use the guidance to support NRC staff actions in a manner that constitutes forward fitting as that term is defined and described in Management Directive 8.4. If a licensee believes that the NRC is using this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfitting or forward fitting appeal with the NRC in accordance with the process in Management Directive 8.4.

GLOSSARY

access-denied	The clearance condition where an individual is not considered trustworthy and reliable based upon the licensee reviewing official's evaluation of potentially disqualifying information (PDI).
additional information	Additional information is defined as the specific information that a previous licensee or utility may have or developed on an individual who last held unescorted access at their facility. This information can only be transferred to another licensee or an agent of the licensee if a written consent is on file.
administrative withdrawal of unescorted access (UA)	A process to temporarily withhold UA from an individual while action is taken to complete or update an element of the UA requirements**.**
annual	A 12-month cycle.
background investigation (BI)	Information from all BI elements to be collectively evaluated by the reviewing official pursuant to a determination of trustworthiness and reliability of an individual. Depending upon the BI period, the BI elements may include any or all of the following: verification of true identity, employment verification with suitable inquiry (SI) (includes education in lieu of employment and military service as employment), a credit check, and character and reputation determination.
behavioral observation (BO)	Observation of an individual's behavior in the workplace, to detect and report aberrant behavior or changes in behavior that might indicate a lack of trustworthiness or reliability. BO includes an annual supervisory review.
best effort	Documented actions taken by a licensee, a contractor/vendor (C/V), or their authorized agents to obtain sufficient employment or education information from an acceptable alternate or secondary source to make a trustworthiness and reliability determination.
business day	Normally, Monday through Friday, except Federal holidays; however, licensees may include Saturdays or Sundays for the purposes of sharing data when UA decisions are made on a Saturday or Sunday, and for making notifications whenever day of discovery requirements are initiated on a Saturday or Sunday.

contractor/vendor (C/V)

Any company or individual not employed by a licensee who is formally approved by a licensee to satisfy elements of the access authorization program, and who is providing work or services to a licensee by either contract, purchase order, oral agreement, or another arrangement to support requirements related to UA or access authorization.

critical group

Group consisting of the following personnel:

- Individuals who have extensive knowledge of defensive strategies and of the design or implementation of the plant's defense strategies. The positions include the following:

  a. site security supervisors
  b. site security managers
  c. security training instructors
  d. corporate security managers

- Individuals in a position to grant an applicant UA, including site access authorization managers.

- Individuals assigned the duty to search for contraband or other items that could be used to commit radiological sabotage (e.g., weapons, explosives, incendiary devices).

- Individuals who have access to, extensive knowledge of, or administrative control over plant digital computer and communication systems and networks as identified in 10 CFR 73.54, "Protection of digital computer and communication systems and networks," and plant network system administrators and information technology personnel who are responsible for securing plant networks.

- Individuals qualified for and assigned duties as armed security officers, armed responders, alarm station operators, response team leaders, and armorers as defined in the licensee's physical security plan; and reactor operators, senior reactor operators, and nonlicensed operators. Nonlicensed operators include those individuals responsible for the operation of plant systems and components,

	as directed by a reactor operator or senior reactor operator. Nonlicensed operators also include individuals who monitor plant instrumentation and equipment and principally perform their duties outside of the control room.
developed references	In the field of reference checking, there are two types of references. The first type is supplied by the candidate. The second type is "developed" by talking to the candidate's references and asking them who else would have known and worked with the candidate. In simple terms, developed references are references the candidate does not know are going to be called.
employment action	A change in job responsibilities or removal from a job; the employer-mandated implementation of a plan for substance abuse treatment in order to avoid a change in or removal from a job; or any military nonjudicial punishment because of an individual's use of drugs or alcohol.
employment/unemployment history verification	A verification of specified periods of employment, military service as employment, education in lieu of employment, and unemployment, on a best effort basis, from information provided or claimed by the individual on their personal history questionnaire.
formal action	The initiation of any UA element by a licensee at the licensee facility.
initial UA	An access category used to identify persons in the process of obtaining UA at a commercial nuclear plant for the first time, or after a lapsed clearance beyond the established 10-year cutoff, or after their last UA was terminated favorably.
knowledgeable and practiced (K&P)	Describes an individual audit team member who has current or previous access authorization program experience and who is responsible for validating that overall program performance is meeting the objective of screening individuals to provide high assurance that they are trustworthy and reliable to have or maintain UA.
legal action	A formal action taken by a law enforcement authority or court of law, through which an individual is held, detained, taken into custody, charged, arrested, indicted, fined, subject to bond forfeiture, cited, or convicted for a violation of

	any law, regulation, or ordinance. These include felony, misdemeanor, serious traffic offenses, serious civil charges, and military charges, but do not include minor misdemeanors such as parking tickets, minor civil actions such as zoning violations, or minor traffic violations such as moving violations when the individual was not physically taken into custody. Legal action includes the mandated implementation of a plan for treatment or mitigation in order to avoid a permanent record of an arrest or conviction due to the following activities: (1) the use, sale, or possession of illegal drugs (2) the abuse of legal drugs or alcohol (3) refusal to take a drug or alcohol test
need to know	Term referring to the requirement that, in order to gain access to personal information collected, an individual must need such access in order to perform their job and is authorized access to the information under the provisions of 10 CFR 73.56, 10 CFR 73.57, or 10 CFR 73.120. An individual's privacy rights under State and Federal law continue to be protected.
nominal	Permitting limited flexibility in meeting a scheduled due date for completing a recurrent required activity; an example is the nominal annual (12-month) frequency. Completing a recurrent activity at a certain nominal frequency means completing it within a period that is 25 percent longer or shorter than the period nominally required. The next scheduled due date would be no later than the current scheduled due date plus the nominal required frequency for completing the activity.
personal history questionnaire (PHQ)	A written statement by an individual applying for UA that provides the personal information required for processing UA elements.
personal information	All information unique to an individual that is collected or developed during the implementation of the UA program requirements.
potentially disqualifying information (PDI)	Any derogatory information (e.g., unfavorable information from an employer; developed or disclosed criminal history; credit history such as collection accounts, bankruptcies, tax liens, and judgments; unfavorable reference information; evidence of drug or alcohol abuse; discrepancies between information disclosed and developed)

	that is required to be evaluated against a licensee's or C/V's adjudication criteria. Fitness-for-duty PDI (10 CFR Part 26 uses the equivalent term "potentially disqualifying fitness-for-duty information") is a subset of PDI that includes information demonstrating that an individual has violated a licensee's or approved C/V's fitness-for-duty policy.
protected area/security zone	An area encompassed by physical barriers and to which access is controlled in accordance with 10 CFR Part 37 or 10 CFR Part 73.
reinvestigation	A periodic inquiry or assessment conducted to ensure that individuals continue to meet UA program suitability requirements.
reviewing official	Person designated by a licensee or C/V to be responsible for reviewing and evaluating data collected about an individual, including PDI, to determine whether the requesting individual may be certified UA by the licensee or C/V, or granted UA by the licensee.
self-disclosure	An individual applying for UA is required to report their past criminal history in a PHQ that is verified during the SI portion of the BI and evaluated in relation to the individual's trustworthiness and reliability. Also, while under BO, the individual is required to report all legal actions when they occur.
suitable inquiry (SI)	A check of self-disclosed information through an employment and education history verification that ascertains the following, on a best-effort basis: • the reason for termination • eligibility for rehire • other information that could reflect on the individual's trustworthiness and reliability to be granted UA, including information from previous employers and educational institutions about whether the individual has, in the past, done any of the following: a. violated a licensee or employer's fitness-for-duty policy b. been denied or terminated unfavorably at any commercial nuclear plant for any

reason, including fitness for duty

c. used, sold, or possessed illegal drugs

d. abused legal drugs or alcohol

e. refused to take a drug or alcohol test

f. subverted or attempted to subvert a drug or alcohol testing program

g. been subject to a plan (except self-referral) for treating substance abuse

h. been subject to an action by a law enforcement authority or court of law for any of the following:

(1) the use, sale, or possession of illegal drugs

(2) the abuse of legal drugs or alcohol

i. been subject to employment action taken for alcohol or drug abuse involving any of the following:

(1) a change in job responsibilities or removal from a job

(2) mandated implementation of a plan for substance abuse treatment in order to avoid a change in or removal from a job

unescorted access (UA) Granted to an individual who has satisfactorily completed all regulatory requirements for UA and is subjected to BO. The individual is provided the physical means to gain UA to the protected area, vital area, and controlled access areas.

REFERENCES[2]

[2]Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public website at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html. The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD. For problems with ADAMS, contact the PDR staff at 301-415-4737 or (800) 397-4209; fax (301) 415-3548; or email pdr.resource@nrc.gov.

Copies of the non-NRC documents included in these references may be obtained from the publishing organization.

Copies of International Atomic Energy Agency (IAEA) documents may be obtained through its website at WWW.IAEA.Org/ or by writing the International Atomic Energy Agency, P.O. Box 100, Wagramer Strasse 5, A-1400 Vienna, Austria; telephone (+431) 2600-0; fax (+431) 2600-7; or email at official.mail@IAEA.org.

Copies of American Society of Mechanical Engineers (ASME) standards may be purchased from ASME, Two Park Avenue, New York, NY 10016-5990; telephone (800) 843-2763. Purchase information is available through the ASME Web-based store at https://www.asme.org/publications-submissions/publishing-information.

APPENDIX A

SOLVING UNCLASSIFIABLE FINGERPRINTS

A-1 BACKGROUND INFORMATION

1. The regulations requiring fingerprints are found in Title 10 of the *Code of Federal Regulations* (10 CFR) 73.120, "Access authorization program for commercial nuclear plants," and in 10 CFR 37.27, "Requirements for criminal history records checks of individuals granted unescorted access to category 1 or category 2 quantities of radioactive material."

   Moreover, pursuant to 10 CFR 37.25(a)(2), licensees must verify the true identity of an individual who is applying for UA in order to ensure that the applicant is the person that they have claimed to be. To enable licensees to effectively meet the requirements, the U.S. Nuclear Regulatory Commission (NRC) has had to provide an alternate approach for fingerprints that are categorized by the Federal Bureau of Investigation (FBI) as "nonclassifiable" because of "occupational hands."

   Section 652 of the Energy Policy Act of 2005 amended section 149 of the Atomic Energy Act of 1954 to state the following:

   > The Commission shall require to be fingerprinted any individual who—
   > (i) is permitted unescorted access to—
   > (I) a utilization facility; or
   > (II) radioactive material or other property subject to regulation by the Commission that the Commission determines to be of such significance to the public health and safety or the common defense and security as to warrant fingerprinting and background checks; or
   > (ii) is permitted access to safeguards information under section 147.

2. The NRC staff identified a need for guidance on an alternative approach for processing nonclassifiable fingerprints on the basis of experience with reviewing electronically submitted fingerprint requests and answering questions from the nuclear power industry. The new electronic technology, except for one or two very high-end imaging systems, requires technicians processing fingerprints to apply fundamentally sound mechanical skills that closely match the mechanical skills required for rolling "inked cards." When a technician fails to apply these basic skills, the results are nonclassifiable fingerprints. The FBI defines nonclassifiable fingerprints as those resulting when the patterns of ridges and valleys that make up the fingerprint are worn down, so that the image does not provide sufficient data to accurately identify and locate the principal features of the fingerprint (i.e., too low for classification). Under the current regulations, if the FBI rejects an individual's fingerprints for being nonclassifiable, a licensee is burdened with submitting several electronic or hard copies of the fingerprints.

3. If a licensee receives nonclassifiable fingerprints, it can pursue an alternate approach for verifying the individual's identity.

   On March 23, 2018, the FBI Criminal Justice Information Services Division (FBI/CJIS) enhanced its Next Generation Identification (NGI) fingerprint management system. Previously, when fingerprints submitted by a recipient (i.e., licensee) for the required FBI criminal history records

check were rejected as nonclassifiable (based on the code L0008), the system response was as follows: “The quality of the characteristics is too low to be used.” The enhanced system now provides the following response when fingerprints are nonclassifiable but a possible biographic data match has been found: “The quality of the characteristics is too low to be used. Candidate(s) were found. Please resubmit a new set of fingerprints for comparison.”

As a result of the enhancements, the FBI/CJIS will only process the NGI reject response of L0008 as follows.

Example 1: “The quality of the characteristics is too low to be used. **Candidate(s) were found.** Please resubmit a new set of fingerprints for comparison.”

A licensee that receives the above response can request a name check only **after the second submission (L0008 code)**. The process is as follows:

a. The licensee can submit a name check request by email to the NRC Criminal History Team at CrimHist.Resource@nrc.gov.

b. The request must include the two rejected Transaction Control Numbers.

c. The FBI/CJIS staff will attempt a manual comparison and return an email response indicating ident, non-ident, or a reject.

d. If there is a positive identification, the Identity History Summary will be provided as an attachment to the email.

Example 2: “The quality of the characteristics is too low to be used. **No record based on descriptive data**.”

A licensee receiving this response **should not submit** a name check request to the FBI, as the FBI/CJIS staff will no longer process the name check based upon the NGI system upgrades.

In these cases, the licensee should **resubmit better-quality fingerprints** at its own expense.

BIBLIOGRAPHY

These additional references are provided for applicants and licensees to use to support the development of their access authorization programs.

NRC Documents

Title 10 of the *Code of Federal Regulations* (10 CFR) 50.5, "Deliberate misconduct."

U.S. Nuclear Regulatory Commission (NRC), Generic Letter 91-03, "Reporting of Safeguards Events," Washington, DC, March 6, 1991.

Industry Documents

Nuclear Energy Institute (NEI) 03-01, "Nuclear Power Plant Access Authorization Program," Washington, DC. May 2009

NEI 03-02, "Access Authorization and Fitness-for-Duty Audit Program," Washington, DC. January 2007

NEI 03-03, "PADS Health Physics Standards and Procedures," Washington, DC. January 2007

NEI 03-04, "PADS Guidelines for Plant Access Training," Washington, DC. January 2007

NEI 03-05, "PADS Operating Manual," Washington, DC. January 2007

NEI 03-06, "PADS Electronic System Technical Documentation," Washington, DC. January 2007

NEI 08-06, "Access Authorization Program Forms," Washington, DC. September 2008

Other Documents

American National Standards Institute (ANSI) N45.2.23-1978, "Qualification of Quality Assurance Program Audit Personnel for Nuclear Power Plants," New York, NY, 1978.

Fair Credit Reporting Act, 15 U.S.C. § 1681, complete as of July 30, 2004, as found at http://www.ftc.gov/os/statutes/fcra.htm.

American Nuclear Insurers, "Engineering Inspection Criteria for Nuclear Liability Insurance," Section 2.0, "General Employee Training," Glastonbury, CT. July 2010

[1] *U.S. Code of Federal Regulations* (CFR), "Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Plants," Part 53, Chapter I, Title 10, "Energy."

[2] CFR , "Physical Protection of Plants and Materials," Part 73, Chapter I, Title 10, "Energy"

[3] CFR, "Fitness for Duty Programs," Part 26, Chapter I, Title 10, "Energy."

[4] CFR, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material," Part 37, Chapter I, Title 10, "Energy."

[5] CFR, "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter I, Title 10, "Energy."

[6] CFR, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Chapter I, Title 10, "Energy."

[7] U.S. Nuclear Regulatory Commission (NRC), NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Section 13.6.4, "Access Authorization—Operational Program," Washington, DC.

[8] NRC, Regulatory Guide 5.66, "Access Authorization Program for Nuclear Power Plants," Washington, DC.

[9] NRC, "Nuclear Regulatory Commission International Policy Statement," *Federal Register*, Vol. 79, No. 132, July 10, 2014, pp. 39415–39418.

[10] NRC, Management Directive 6.6, "Regulatory Guides," Washington, DC.

[11] International Atomic Energy Agency (IAEA), Nuclear Security Series (NSS) No. 27-G, "Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5)," Vienna, 2018.

[12] IAEA, NSS No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," Vienna, 2011.

[13] U.S. Department of Homeland Security, "Nonimmigrant Classes of Admission," Washington, DC, last updated January 21, 2022, available at https://www.dhs.gov/immigration-statistics/nonimmigrant/NonimmigrantCOA.

[14] U.S. Department of State, "Directory of Visa Categories," Washington, DC, available at https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/all-visa-categories.html (last accessed May 27, 2022).

[15] U.S. Department of Defense, DD Form 214, "Certificate of Release or Discharge from Active Duty," Washington, DC.

[16] U.S. Department of Defense, Standard Form 180, "Request Pertaining to Military Records," Washington, DC.

[17] Federal Bureau of Investigation (FBI) Criminal Justice Information Services Division, "NRC Handling of Criminal History Record Information (CHRI) Obtained from the FBI," Clarksburg, West Virginia, October 24, 1997. (ADAMS Accession No. ML12110A327)

[18] American Society of Mechanical Engineers, ANSI N45.2.9-1979, "Requirements for Collection, Storage, and Maintenance of Quality Assurance Records for Nuclear Power Plants," New York, NY, 1979.

[19] NRC, Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests," Washington, DC.