



Security
Fleet Procedure

FP-S-AA-01

Revision: 6

Corporate Office Quality Procedures

Title: Access Authorization Program

Approval:
(Signed copy on file)

Brian Linde

Director, Security

Effective Date: 3/10/2004

Site Adoption by: 5/9/2004

Submit comments

Note: This procedure is issued and controlled by Nuclear Oversight in Hudson. Site Specific procedure review and approval processes shall be used at each NMC plant to implement this procedure.

Table of Contents

1.0	PURPOSE.....	2
2.0	APPLICABILITY.....	2
3.0	RESPONSIBILITIES.....	3
4.0	DEFINITIONS.....	6
5.0	REQUIREMENTS.....	8
5.1	UNESCORTED ACCESS (UA) PROCESSING.....	8
5.2	UNESCORTED ACCESS AUTHORIZATION (UAA) PROCESSING.....	14
5.3	INITIAL UAA ELEMENTS.....	18
5.4	REINVESTIGATIONS.....	31
5.5	UPDATED UAA.....	34
5.6	REINSTATEMENT OF UAA.....	34
5.7	ENHANCED OVERSIGHT.....	44
5.8	CRIMINAL HISTORY CHECKS.....	45

CC-31

5.9	PSYCHOLOGICAL EVALUATIONS	50
5.10	INVESTIGATING DEROGATORY INFORMATION.....	54
5.11	EVALUATION FOR UAA.....	57
5.12	REVIEWING UAA DENIALS	67
5.13	BEHAVIORAL OBSERVATION PROGRAM (BOP).....	69
5.14	APPROVED CONTRACTOR UAA PROGRAMS	71
5.15	AUDITS.....	75
5.16	REPORTING OF UAA SAFEGUARDS EVENTS.....	75
6.0	REQUIRED RECORDS	79
7.0	REFERENCES.....	82
8.0	ATTACHMENTS.....	83
9.0	REVISION SUMMARY.....	83

1.0 PURPOSE

This program defines the requirements for granting escorted and unescorted access to Nuclear Management Company nuclear plant protected areas. Included in this program are elements to assure personnel granted unescorted access to NMC plant protected areas are trustworthy and reliable, and do not constitute an unreasonable risk to health and safety of the public, including a potential to commit radiological sabotage.

2.0 APPLICABILITY

- 2.1 This procedure applies to all personnel granted unescorted access to NMC nuclear plant protected areas and Independent Spent Fuel Storage Installations (ISFSIs). ISFSIs shall be considered protected areas as referenced in this procedure.
- 2.2 Exceptions: This program does not apply to employees of the Nuclear Regulatory Commission (NRC), contractors of the NRC when certified by same as suitable for unescorted access, or law enforcement, medical or fire personnel responding to emergencies.

As defined herein NMC departments and approved contractor/vendors are required to comply with the requirements of this procedure and any subsequent revisions. If additional information regarding this procedure is necessary, the respective NMC Site Access Authorization Lead (SAAL) should be contacted.

3.0 RESPONSIBILITIES

The following positions have responsibility

3.1 The Director Nuclear Oversight, NMC shall be responsible for:

3.1.1 The auditing of NMC approved contractor access authorization (AA) programs.

3.1.2 Maintaining records of contractor (AA) program audits.

3.2 The Manager IT Application Services, NMC shall be responsible for:

3.2.1 The control of the NMC Industry Shared Database computer and its associated programs, journals and data back-ups.

3.3 Site Managers Nuclear Training shall be responsible for:

3.3.1 The control of the site training data files used for access processing.

3.3.2 Providing General Access Training (GAT)/Plant Access Training (PAT).

3.3.3 Providing radiation protection and respirator training.

3.3.4 Providing Fitness for Duty (FFD) training.

3.4 Site Vice Presidents (VPs) shall be responsible for:

3.4.1 Approving the denial or suspension of access for personnel currently granted (UA).

3.4.2 Deciding access review requests.

3.5 The Access Manager, NMC shall be responsible for:

3.5.1 Developing and administering the AA and FFD Programs.

3.5.2 Managing plant access processing.

- 3.5.3 Overall management of the PADS program as implemented at NMC sites.
- 3.6 Site Access Authorization Leads (SAAL) shall be responsible for onsite implementation of:
 - 3.6.1 AA and FFD Programs.
 - 3.6.2 Access Processing.
 - 3.6.3 The process providing Site Managers/Supervisors AA rosters to verify access level needs at NMC sites.
 - 3.6.4 Site Access Coordinator and Specialist training.
 - 3.6.5 Site AA/FFD self-assessment program.
 - 3.6.6 Reviewing official duties as defined herein.
 - 3.6.7 In the SAAL's absence, the SAS may perform SAAL reviewing official responsibilities as defined herein.
- 3.7 Site Access Specialists (SAS) shall be responsible for onsite implementation of:
 - 3.7.1 AA and FFD Program elements.
 - 3.7.2 Access processing.
 - 3.7.3 Reviewing official duties as defined herein.
 - 3.7.4 SAAL reviewing official duties during peak workload (e.g. outage in-processing) or in SAAL's absence.
 - 3.7.5 Site Access Coordinator (SAC) duties in SAC's absence.
- 3.8 Site Access Coordinators (SAC) shall be responsible for:
 - 3.8.1 Processing site access requests.
 - 3.8.2 Coordinating completion of AA, FFD, radiation protection and training in-processing requirements.
 - 3.8.3 Verifying completion of in-processing elements and issuing badges for unescorted access.

**Access Authorization Program
FP-S-AA-01, Revision 6**

- 3.8.4 Issuing to Site Managers/Supervisors AA rosters to verify access level needs at NMC sites.
- 3.8.5 Updating changes in site access status.
- 3.8.6 Notifying workers of requirements for maintaining unescorted access.
- 3.8.7 Reviewing official duties as defined herein.
- 3.9 The Site Supervisor Medical Services or NMC Access Manager shall be responsible for providing services supporting implementation of 10CFR26 drug and alcohol testing requirements.
- 3.10 NMC Supervision shall be responsible for:
 - 3.10.1 Initiating access processing of employees and non-employees, including contractors or consultants, performing work at the nuclear plant under a purchase order.
 - 3.10.2 Submitting site access requests identifying personnel requiring unescorted access and defining areas to the plant to which access should be granted.
 - 3.10.3 Submitting site access termination requests.
 - 3.10.4 Ensuring access to NMC sites is only requested for those individuals, packages, or vehicles necessary for maintenance, operation, or security.
 - 3.10.5 Reviewing access authorization rosters and informing the Site Access Coordinators of changes in access status.
 - 3.10.6 Implementing the CBOP requirements as defined in Section 5.13.
 - 3.10.7 Industry Shared Database data entry and validation if their department is involved with access processing data entry.
- 3.11 Approved UAA Contractors shall be responsible for adhering to Section 5.14 requirements.
- 3.12 Contractor management shall notify the Site Security Manager or SAAL immediately if an employee is:
 - 3.12.1 Terminated unfavorably.
 - 3.12.2 Displaying aberrant behavior.

3.12.3 Unfit for duty.

3.12.4 Arrested, charged, or convicted for violation of law.

4.0 DEFINITIONS

- 4.1 **ACCESS DENIED:** The UAA condition where an individual is not considered trustworthy and reliable based upon the reviewing official's: 1) evaluation of information developed through background investigation or the behavior observation program information, or 2) conclusion that the individual has violated an access authorization or fitness-for-duty policy or been terminated unfavorably but has not completed required actions (such as drug abuse rehabilitation) for UAA restoration consideration.
- 4.2 **APPROVED CONTRACTOR UAA PROGRAM:** A contractor unescorted access authorization (UAA) program approved by NMC to perform elements of NMC's Access Authorization Program.
- 4.3 **BACKGROUND INVESTIGATION:** Background investigation involves the collection of information regarding an individual's history that may be indicative of suitability for UAA.
- 4.4 **BEST EFFORT:** Documented actions taken to obtain the required information pertaining to an individual's UAA determination, when the primary source refuses or indicates an inability or unwillingness to provide the information within three business days and a secondary source is used to complete the requirement.
- 4.5 **BEHAVIORAL OBSERVATION PROGRAM:** An awareness program that meets requirements of both the access authorization and fitness-for-duty programs. Personnel are trained in techniques related to recognition of behaviors adverse to the safe operation and security of the facility in observing the behavior of others in the workplace and to detect and report aberrant behavior or changes in behavior that might reflect negatively on an individual's trustworthiness or reliability. Integral to the program is the management oversight of employee behavior and the individual's reporting of arrests.
- 4.6 **CONTRACT WORKER:** Contractor employee, supervisor, agent, representative and/or subcontractor employee, supervisor, agent or representative (i.e., any worker not employed by NMC or an NMC asset owner).
- 4.7 **ESSENTIAL ACTIVITIES:** Those activities directly related to plant or ISFSI maintenance or operation.

Access Authorization Program
FP-S-AA-01, Revision 6

- 4.8 **GRANDFATHERED UAA:** A UAA in effect during the 180-day period prior to and on April 25, 1991.
- 4.9 **INITIAL UAA:** An access category used to identify persons in the process of obtaining unescorted access at a nuclear power plant for the first time or after a lapsed clearance beyond the applicable cutoff period established herein.
- 4.10 **NOMINAL:** Period of time plus or minus 25%.
- 4.11 **OVERSIGHT:** Oversight means monitoring, by a person with a full clearance, of the activities within a vital area performed by a worker(s) with temporary clearance. The oversight should consist of frequent and regular contact sufficient to ensure that the worker is not engaging in unauthorized activities.
- 4.12 **PIPS:** A central data base contains personnel, security, training and fitness for duty information on individuals granted access at NMC sites.
- 4.13 **REINSTATED UAA:** An unescorted access authorization or unescorted access that has been reestablished within 365 days consistent with requirements defined herein.
- 4.14 **RECEIVING LICENSEE:** Any utility authorized to operate a nuclear power reactor pursuant to 10 CFR 50.21(b) or 10 CFR 50.22 that requests a transfer of UAA.
- 4.15 **REVIEWING OFFICIAL:** The licensee or, if applicable, C/V persons assigned by their company to make access determinations relative to an access applicant's trustworthiness, reliability and fitness for duty based upon all collected information. Reviewing Official duties for the SAC/SAS/SAAL are defined in Section 5.11.
- 4.16 **TERMINATED FAVORABLY:** Basis for removal of UAA **does not** adversely reflect on trustworthiness, reliability, or fitness for duty (e.g., completed job, retired, left company for another job).
- 4.17 **TERMINATED UNFAVORABLY:** Basis for removal of UAA does adversely reflect on trustworthiness, reliability, or fitness for duty (e.g., terminated for-cause; violated code of conduct, fitness for duty policy).
- 4.18 **TRANSFERRING LICENSEE:** any utility authorized to operate a nuclear power reactor pursuant to 10 CFR 50.21(b) or 10 CFR 50.22 that transfers AA related data upon request from another utility.
- 4.19 **UNESCORTED ACCESS (UA):** Authorization for unescorted access; granted after satisfactorily completing all regulatory requirements for UAA after which the individual is provided plant access training, is covered by

behavioral observation and random drug and alcohol testing programs, and is provided the physical means to gain unescorted access to the protected area.

- 4.20 **UNESCORTED ACCESS AUTHORIZATION (UAA):** Status in an individual's access authorization process after his or her satisfactory completion of all required elements, which are then evaluated by a reviewing official who makes an access determination relative to the individual's trustworthiness, reliability and fitness for duty. These required elements for unescorted access authorization are: verified identity of individual, employment history with suitable inquiry (includes education in lieu of employment and military service as employment), a credit check, character and reputation determination, a psychological evaluation, FBI criminal history check, preaccess drug and alcohol testing results and appropriate training.
- 4.21 **UPDATED UAA:** An UAA that has been restored after access was terminated under favorable conditions during a period greater than 365 days but less than 3 years as applicable herein prior to restoration.
- 4.22 **VISITOR:** A person issued a visitor badge by site security and granted escorted access to an NMC nuclear plant protected area.

5.0 REQUIREMENTS

5.1 UNESCORTED ACCESS (UA) PROCESSING

5.1.1 Prior to Worker's Arrival

1. The responsible NMC Manager/Supervisor shall:
 - a. Determine the individual's need for unescorted access.
 - b. Assure the worker has contacted NMC's SAC to obtain the necessary NMC forms for completion and submittal or been provided with a complete list of information and documents needed to complete the necessary NMC records.
 - 1) Anticipated processing time is one to two weeks from the date the properly completed NMC forms are received by NMC Security.
 - 2) A summary of information needed to complete the necessary NMC forms to initiate access authorization is presented in NMC Security Attachment 3, *Personal Information and Identification Needed for Initial Unescorted Access Processing*.

- c. Communicate to the SAC the need for contract worker unescorted access by completing site's access request process as identified in Table QF-0382, *Initiating UA Requests at NMC Sites*.

NOTE: Only individuals holding UA may submit requests for UA and perform monthly access levels reviews in accordance with Section 5.1.5.

- d. Assure the worker has contacted NMC's SAC to schedule required in-processing and training.
- e. For workers requiring vital area access, indicate whether the work involves essential activities.

5.1.2 In-processing Coordination

- 1. NMC Security/SAC shall:
 - a. Provide personnel to:
 - 1) Obtain and submit fingerprints to the NRC as required for UAA and safeguards access,
 - 2) Proctor psychological testing,
 - 3) Review UAA required forms for completeness.
 - b. Review NMC Security Table QF-0376, *NMC Badging Matrix*, to determine UAA processing requirements, including applicable forms.
 - c. Coordinate completion of in-processing elements required for UA, including:
 - 1) Required UA training,
 - 2) Badge photo,
 - 3) Hand geometry (as applicable),
 - 4) UAA forms,
 - 5) Proctor psychological testing,
 - 6) Fingerprinting

**Access Authorization Program
FP-S-AA-01, Revision 6**

- 7) Drug and alcohol testing.
 - 8) Other plant specific processing requirements
 - d. Control access to the nuclear plant using a badging and/or hand geometry system in accordance with the plant's security plan.
 - e. Ensure the requirements of Section 5.1.1 (1) are transmitted to Department Managers and others who have employees or contract workers requiring unescorted access authorization.
2. Site Training shall provide as appropriate:
 - a. General Access Training (GAT)/Plant Access Training (PAT) clean area training
 - b. GAT/Radiological Worker Training (RWT) controlled area training
 - c. Fitness For Duty training (minimally worker/escort duty/manager/supervisor level).
 - d. Respirator training
 - e. Communicate training results to the SAC.
4. The Site Supervisor Medical Services (unless provided by NMC Access Manager) shall:
 - a. Provide registered nurses, medical laboratory technicians or other qualified personnel for collecting urine and breath specimens for drug and alcohol testing in accordance with 10 CFR 26 Appendix A.
 - b. Communicate the results of drug and alcohol testing to NMC Security.
5. Each person being granted access shall be required to complete those portions of access processing necessary for his/her function at the plant.
6. The access processing data files should be updated in a timely manner (e.g., daily) after the completion of each applicable portion of the processing.

7. Requirements for behavioral observation are provided in Section 5.13.

5.1.3 Granting Unescorted Access

1. The SAC shall process the requests for UA after checking that the appropriate unescorted access processing requirements are satisfied. This includes:

- a. Unescorted access authorization.

NOTE: PIPS Access Tab fields UA Granted and UA From Date shall be the same date.

- b. Applicable PAT/RWT/FFD training status and updates.
- c. Plant specific unescorted access processing requirements.
- d. Positive identification of the person and a check of the Social Security Number.

2. Upon satisfactory completion of the elements in Section 5.1.3 (1), the SAC shall:

- a. Grant site access corresponding to type requested on applicable site access level form (see NMC Security Table QF-0382).
- b. As applicable, update site databases to reflect changes in access status, including:
 - 1) PIPS, including UA From and To dates.
 - 2) Site databases supporting random testing and UAA tracking.
- c. Issue the badge.

5.1.4 Terminating Unescorted Access

1. For workers **unfavorably terminated**, management shall immediately notify Site Security (see Table QF-0384, *NMC Security AA/FFD Points of Contact*) and submit to the SAC site's access termination form (see Table QF-0383).

**Access Authorization Program
FP-S-AA-01, Revision 6**

- a. Site Security Representative shall:
 - 1) Immediately notify the Site Security Manager and SAAL. Site Security Manager and SAAL shall confer with other appropriate management personnel regarding worker's access to and knowledge of plant security systems,
 - 2) Terminate worker's unescorted access prior to or simultaneously with notice of termination.
 - b. SAC shall:
 - 1) Terminate worker's access in PIPS,
 - 2) Update site databases to reflect unfavorable termination status.
 - c. As identified in 10 CFR 73.55 (d)(8), a subsequent denial of UA in accordance with Section 5.11, shall be considered a revocation of access.
2. For workers favorably terminated, management should submit a completed site access termination form, on or before the date UA is to be terminated, but no later than 5-days following the date access is no longer needed, to the SAC.
- a. SAC shall:
 - 1) Terminate worker's site access and update PIPS,
 - 2) Update site databases to reflect favorable termination status.
 - 3) Maintain notice of terminations for five (5) years from the date access is terminated.

5.1.5 Monthly Access Level Reviews

- 1. For workers granted protected area and ISFSI access, each month the SAC shall:
 - a. Send the worker's supervisor, or designated access reviewer, a report:
 - 1) Identifying current access levels.

- 2) Requiring written approval of current access levels or changes needed to perform assigned duties.
 - b. Send reports identified in Section 5.1.5.1.a to supervisors or designated access reviewers by the seventh (7th) day of each month.
 - c. For access review reports **not** returned within twenty-one (21) days following the distribution date, inform the responsible supervisor or designated access reviewer that access will be suspended for assigned workers if the access review report is not returned by the date thirty-one days following the access review report distribution date.
 - d. Maintain a copy of reports identified in Section 5.1.5.1.a.
 - e. For access review reports not returned within the 31st day following distribution, immediately inform the SAAL.
- 2) The SAAL shall place workers identified in accordance within Section 5.1.5.1.e on administrative hold in accordance with Section 5.1.6.

5.1.6 Administrative Holds

1. Supervision/management may request suspension of unescorted access to the protected area by placing a worker's access on administrative hold. Situations warranting an administrative hold include, but are not limited to:
 - a. A badge is found to be inactive or expired.
 - b. Failure to pass required General Access Training (GAT).
 - c. Behavior observation and/or FFD concerns that warrant removal from duty pending assessment/investigation.
2. All requests to place a badge on administrative hold shall be directed through the Central Alarm Station (CAS)/Secondary Alarm Station (SAS) or designee. CAS/SAS operators or designee shall:
 - a. Complete Form QF-0389, *Administrative Hold Checklist*.
 - b. Obtain approval for a badge being placed on administrative hold from:

- 1) Security Manager
- 2) SAAL

Note: approval is not required to place badges on Administrative hold because of expired or failed GAT training.

3. SAALs shall approve the removal of an administrative hold.
4. A visitor badge may be issued to personnel on administrative hold only if approved by NMC security management.
5. SAS shall change the BFA in PIPS to "ADMIN DATA" for individuals placed on administrative hold.

5.2 UNESCORTED ACCESS AUTHORIZATION (UAA) PROCESSING

5.2.1 Initiating UAA Processing

1. UAA processing should not be initiated unless a responsible site supervisor requests unescorted access processing via site access request process identified in NMC Security Table QF-0382.
2. Upon receipt of a request for UA, the SAC shall review the individual's UAA history and NMC Security Table QF-0376 to determine UAA processing requirements.
3. An individual's UAA history may be determined by reviewing site UAA records, PIPS, NRC certification lists, approved vendor UAA records, or other appropriate sources as determined by the SAAL.
4. The SAC shall coordinate scheduling and completion of UAA in-processing elements.
5. Designated UAA processing personnel shall ensure that applicable forms are properly completed.
6. No element of UAA processing shall be initiated without the written consent of the individual requesting UAA.
7. Consent to UAA processing may be withdrawn at any time. Withdrawal should be in writing and is effective immediately

Access Authorization Program
FP-S-AA-01, Revision 6

upon receipt by the SAAL. Processing activities shall not be initiated.

5.2.2 Use and Disclosure of Information

1. Information obtained through the AA Program shall be used solely for the purpose of determining suitability for UAA.
2. A file containing developed information, forms and reports used to process and disposition requests for UA/UAA shall be established for each individual.
3. Information contained in the files for UA/UAA shall be considered confidential and protected.
4. The SAAL is responsible for establishing and maintaining a system for the protection of confidential records.
5. The contents of UA/UAA files may be released or transferred only to individuals with a need to know as determined by the SAAL.
6. By July 7, 2003, all transaction and decision date values required to support an unescorted access decision for all persons holding unescorted access authorization on or after January 7, 2003 shall be recorded in the Industry Shared Database. As applicable to the Industry Shared Database basis for action, the following data shall be recorded:
 - a. UA From date.
 - b. Citizenship.
 - c. Date psychological evaluation completed.
 - d. Date CHRI received.
 - e. Date of drug/alcohol test.
 - f. Date background investigation and suitable inquiry completed.
 - g. NMC site providing the information.
 - h. Company holding the supporting records, if not an NMC site.
7. Effective July 7, 2003, for individuals granted UAA/UA or formally applying for the same, the following demographic and Plant Access Training data shall be entered in the Industry Shared Database:
 - a. Current address.
 - b. Height.
 - c. Weight.
 - d. Eye color.

**Access Authorization Program
FP-S-AA-01, Revision 6**

- e. Hair color.
 - f. Gender.
 - g. Place of birth (city, state (if US), and country).
 - h. Date PAT Training is completed.
8. By July 7, 2003, all individuals denied UAA/UA since January 1, 1997, and related pertinent information, shall be recorded in the Industry Shared Database, to minimally include:
- a. Date UA denied.
 - b. Company holding the "additional information".
9. By July 7, 2003, all individuals currently granted UAA/UA at NMC sites subject to a follow-up drug/alcohol testing program shall be identified in the Industry Shared Database, to minimally include follow-up:
- a. Begin date.
 - b. Estimated end date.
 - c. Frequency.
 - d. Number of tests.
 - e. Completed date.
10. On or after July 7, 2003, any violation of a 10 CFR 26 program element at an NMC site, to the extent that, at the time of discovery, individuals holding UA who were the subject of or included in, any program element violation at an NMC site, are identified by NMC, to any licensee where persons hold UA, in the Industry Shared Database:
- a. Where such violations are identified, the respective NMC SAAL shall notify via phone effected NMC sites and other licensees.
 - b. SAS shall change the BFA in PIPS to "ADMIN DATA" for individuals placed on administrative hold.
11. If a suitable inquiry record (i.e., "yes" response to item identified in QF-0350, Section 9, or comparable) is developed, the Suitable Inquiry Info Developed block on the PIPS Access Tab shall be checked. A PADS synopsis report shall be run to verify the additional information is indicated on PADS SEC5 for the site of origin.

5.2.3 Determining UAA Elements

1. The SAC or designated in-processing personnel shall review the individual's UA/JAA history and NMC Security Table QF-0376 to determine in-processing UAA requirements.

5.2.4 Maintaining UAA

1. Once UAA is granted in accordance with applicable Sections 5.3 through 5.6, UAA is maintained provided the individual remains under a licensee-approved behavioral observation program (BOP), including training on their responsibilities for remaining trustworthy and reliable, for both the access authorization program including arrest reporting requirements, and the fitness-for-duty program. If a period of interruption of greater than 30 days occurs, UAA shall be withheld until requirements for UAA are made current.
2. Once authorized UAA and while under an approved BOP, the individual may be maintained in a UAA-authorized status ready to be granted UA.

5.2.5 NRC and its Contractors

1. The NRC provides letters/lists indicating those persons authorized to be granted unescorted access. The letters/lists should be retained by the SAAL, until the letters/lists are updated.
2. SAC/SAS shall complete Form QF-1702, NRC UAA Checklist, prior to granting NRC personnel UA to NMC sites.

5.2.6 APPROVED UAA CONTRACTORS

1. Approved UAA contractors shall submit NMC Security Attachment 2 (or comparable) to initiate requests for UA.

5.2.7 Background Screener/Personnel Processing PHQ Requirements

1. Contracts with companies performing background investigation elements as defined herein shall require the companies to perform the following background investigation on any individuals collecting and processing information by July 7, 2003:
 - a. Verification of identity.
 - b. A local criminal history check at the location of the individual's permanent residence.
 - c. A credit check.

- d. An employment check for the past three years.
 - e. Interview two developed references.
2. Individuals evaluating personal information for the purpose of processing individuals for UAA/UA, or who have unfettered access to the files and records of persons applying for or holding UA, or who are responsible for data management upon which UA decisions may be based, shall be granted and maintain UAA in accordance with this procedure.

5.3 INITIAL UAA ELEMENTS

5.3.1 General

- 1. Initial UAA in accordance with Section 5.3.4 may be granted prior to April 6, 2003 and shall be granted on or after April 7, 2003 for individuals not granted UAA within the prior 3 years or where last access was terminated unfavorably.
- 2. A best effort attempt shall be made to complete UAA elements prior to granting UAA.
- 3. Additional initial UAA elements are contained in Attachment 5 to this procedure.

5.3.2 Initial Background Investigation Scope

- 1. The scope of the background investigation (BI) shall be:
 - a. Up to five (5) years as identified in Section 5.3.3 respectively or back to the individual's 18th birthday. (provided the last UAA was favorably terminated), whichever is less.

5.3.3 Initial UAA Elements

- 1. Employment/Unemployment Activity
 - a. Employment/unemployment history for the three (3) year period prior to the application for UAA to an NMC facility shall be verified as follows:
 - 1) Prior to the date the individual completes the PHQ, for all claimed employment within the first year and the longest claimed employment in each calendar month for the second and third years, verify the

Access Authorization Program
FP-S-AA-01, Revision 6

length and nature of employment on a best effort basis as defined in Section 5.3.3.1.a.3 through contacts with previous employers. Investigate the following aspects of the employment relationship:

- a) Dates of employment periods;
 - b) Reason for termination and eligibility for rehire;
 - c) Any disciplinary history or other information that could impact the trustworthiness/reliability decision for unescorted access; and
 - d) Fitness for duty history as defined in 10 CFR Part 26 suitable inquiry requirements:
 - 1) Has worker ever used alcohol that resulted in on duty impairment or tested positive for drugs?
 - 2) Has worker been subject to a plan for treating substance abuse (except for self-referral)?
 - 3) Has worker been removed from or made ineligible for activities in accordance with a fitness for duty policy?
 - 4) Has worker been denied unescorted access at any nuclear power station for any reason or been denied other employment in accordance with a fitness for duty policy?
- 2) Periods of self-employment shall be verified through one or more of the following:
- a) Self-employment tax records
 - b) Bookkeeper or accountant
 - c) Client(s)
 - d) Employee(s)
 - e) Reference(s)
 - f) Co-worker(s)
 - g) Relative(s) may be used after the other methods, a) through f) above, have been unsuccessful in providing the information needed to verify the self-employment claim.

The specifics of the effort shall have been documented, prior to using relatives.

- 3) For each employer, employment best effort is satisfied under the following conditions:
 - a) On day one (1) of the investigation:
 - 1) If the employer's policy is to respond only on days beyond the 3-day period following initiation of the background investigation (and this policy has been verified as current within the last 6 months), fax or mail a request to the employer and go to a secondary source as defined in Section 5.3.3.1.a.4.
 - 2) If the employer refuses to provide dates of employment, go to a secondary source.
 - 3) If the employer indicates an unwillingness to respond within the 3-day period following initiation of the background investigation, fax or mail a request to the employer and go to a secondary source.
 - 4) If the employer's policy is to not provide dates of employment (and this policy has been verified as current within the last 6 months), fax or mail a request to the employer and go to a secondary source.
 - 5) If the employer indicates a willingness to respond within 3 days by phone or fax, go to Section 5.3.3.1.a.3.b.
 - 6) If the employer does not respond to a phone or fax request, go to Section 5.3.3.1.a.3.b.
 - b) On day two (2) of the investigation:

Access Authorization Program
FP-S-AA-01, Revision 6

- 1) If the employer indicates a willingness to respond within 2 days by phone or fax, go to Section 5.3.3.1.a.3.c.
- 2) If the employer does not respond to a phone or fax request, go to Section 5.3.3.1.a.3.c.
- c) On day three (3) of the investigation:
 - 1) If the employer indicates an unwillingness to respond within 1 day by phone or fax, go to a secondary source.
 - 2) If the employer does not respond to a phone or fax request, go to a secondary source.
- 4) As identified in Section 5.3.3.1.a.3, one or more of the following secondary sources shall be used to verify employment information:
 - a) Pay stubs, W2 form, wage and benefit statement, or business records confirming periods of employment.
 - b) Union contribution records used in determination of employee retirement benefits.
 - c) Reference(s). Shall not use as a secondary source a developed reference developed in accordance with Section 5.3.3.2 during the current investigation.
- 5) Unemployment periods of 30 days or more shall be verified through contact with relatives, references, unemployment compensation or union records.
- 6) For periods of military service as employment within the last 3 years or since the last UAA:
 - a) Contact the most recent duty station to verify the period and character of service by

investigating the following aspects of military service:

- 1) Dates of enlistment period and character of service;
 - 2) Reason for separation and eligibility for re-enlistment;
 - 3) Any disciplinary history or other information that could impact the trustworthiness/reliability decision for unescorted access; and
 - 4) Fitness for duty history as defined in 10 CFR Part 26 suitable inquiry requirements:
 - i. Has individual ever used alcohol that resulted in on duty impairment or tested positive for drugs?
 - ii. Has individual been subject to a plan for treating substance abuse (except for self-referral)?
 - iii. Has individual been removed from or made ineligible for activities in accordance with a fitness for duty policy?
 - iv. Has individual been denied unescorted access at any nuclear power station or branch of the military service for any reason or been denied other employment in accordance with a fitness for duty policy?
- b) If the veteran's last duty station cannot provide the information requested in Section 5.3.3.1.a.6.a.(1-4), a hand carried copy of the DD 214 (or equivalent for foreign military service) presented by the veteran may be accepted, which on its face appears legitimate.

Access Authorization Program
FP-S-AA-01, Revision 6

- 1) If hand-carried copy of the DD 214 or equivalent appears altered in any way, unescorted access shall be withheld until a certified copy of the veteran's DD 214 or equivalent, is obtained from a custodian of military records.
- c) Where (a) and (b) immediately above cannot be satisfied, a copy of the veteran's DD 214 or equivalent, obtained from a custodian or military records, shall be necessary to satisfy the requirement for verification of military service.
- b. Education history for any claimed enrollment in lieu of employment during the past five-year period or since the last UAA shall be verified.
 - 1) Verify the length and nature of claimed education on a best effort basis as defined in Section 5.3.3.1.b.2 through contacts with educational institutions to investigate the following aspects of education:
 - a) Dates of enrollment;
 - b) Reason for leaving school and eligibility to re-enroll;
 - c) Any disciplinary history or other information that could impact the trustworthiness/reliability decision for unescorted access; and
 - d) Fitness for duty history as defined in 10 CFR Part 26 suitable inquiry requirements:
 - 1) Has student ever used alcohol that resulted in on-duty impairment or tested positive for drugs?
 - 2) Has student been subject to a plan for treating substance abuse (except for self-referral)?
 - 3) Has student been removed from or made ineligible for activities in accordance with a fitness for duty policy?

- 4) Has student been denied unescorted access at other nuclear power station or other education or employment in accordance with a fitness for duty policy?
- 2) If the educational institution will not release the requested information, an alternate source as identified in Section 5.3.3.1.a.4 may be used to verify the information identified in Section 5.3.3.1.b.1 (a-d).
- c. Records of employment checks include dates of employment (or periods in lieu of) and shall include:
 - 1) Name of employer,
 - 3) Name, business address and phone number of the contact,
 - 4) Name of the investigator,
 - 5) Date of contact,
 - 6) Cross verification of identity,
 - 7) Responses to required questions.

2. Reference Checks

- a. Interviews of at least two developed references shall be conducted to examine the individual's character and reputation for emotional stability, trustworthiness and reliability.
- b. Developed references may be identified using references listed on the personal history statement, past or present employers (unless previously used for employment check), schools, neighborhoods, co-workers, clubs, churches, etc.
 - 1) A reference listed on the PHQ may not be used as a developed reference.
- c. It is not necessary that references (individual or collective) associated with or having knowledge of the applicant cover the entire three (3) year retrospective period.
- d. References cannot be close relatives (i.e., wife, husband, mother, father, brother, sister, or child) of the subject.

Access Authorization Program
FP-S-AA-01, Revision 6

- e. A developed reference cannot live in the same permanent household as the applicant, a listed reference or another developed reference.
- f. A developed reference shall have known the subject within the scope of the investigation.
- g. Individuals used as a character reference may not be used to verify employment or unemployment.
- h. A developed reference's (individual or collective) association with the applicant should be substantive enough to be able to provide meaningful information. At a minimum, the reference will have known the applicant for not less than six months, and had at least one contact with the applicant in the last six months.
- i. Emphasis shall be placed on the following:
 - 1) behavior/psychological problems.
 - 2) Unlawful/criminal activities.
 - 3) Illegal use, sale or possession of a controlled substance.
 - 4) Abuse of alcohol, prescription or over-the-counter drugs.
 - 5) Susceptibility to bribery or coercion.
 - 6) Any other conduct relating to an assessment of potential untrustworthiness and/or unreliability.
- j. Records of reference checks are to include the name and address of the reference, period and frequency of association (e.g., known since), adverse or discrepant information,
 - 1) Full name, address, phone number of the reference,
 - 2) Type of association, (e.g., co-worker, friend, neighbor, etc.) and duration/frequency of contact,
 - 3) Adverse or discrepant information regarding areas investigated in Section 5.3.4.2.i,
 - 4) Date of the verification and name of the investigator,
 - 5) Name and phone number of source used to develop the reference.

3. Credit Check

**Access Authorization Program
FP-S-AA-01, Revision 6**

- a. Subject's credit history shall be developed through checks of any national credit database. If unable to develop credit history through national databases, local credit bureaus may be used.
 - b. For subjects who do not have established credit history with credit bureau(s), a statement of responsibility concerning the individual's financial record shall be obtained from an entity within the country the individual resides (personal credit sources such as landlords, banks, utilities, schools, etc).
 - c. Each credit check shall, where available, include an inquiry to detect potential fraud or misuse of social security numbers or other financial identifiers.
4. Criminal History Check
- a. A criminal history record check of the individual shall be completed as described in 10 CFR 73.57 and Section 5.8 herein.
 - b. State and local checks may be conducted in addition to the FBI check as directed by the SAAL.
 - c. Completion of criminal history checks shall be documented by receipt of returned FBI criminal history checks from the NRC or a best effort to complete such as defined in Section 5.8.
5. Psychological Evaluation
- a. A psychological evaluation conducted in accordance with Section 5.9 shall be conducted to evaluate the possible impact of any noted psychological characteristics that may have a bearing on trustworthiness and reliability.
 - b. Successful completion of a psychological evaluation shall be documented by receipt of a letter from a licensed psychologist recommending the individual for UAA.
6. Verification of Identity
- a. Individuals requesting access to NMC facilities shall be positively identified.

Access Authorization Program
FP-S-AA-01, Revision 6

- b. Individual's official government issued photo ID (e.g., driver's license, passport, government or military ID) shall be compared to his/her physical characteristics to verify identity.
 - c. Cross verification of ID (name, date of birth, SSN) shall be completed during the background investigation. Sources used for such verification shall be included in the background investigation report.
 - d. Additional identity verification requirements are contained in Attachment 5.
7. If individual has not passed a drug and alcohol test in accordance with a licensee or NMC approved contractor program within the 30-day period prior to granting UAA/UA, drug and alcohol testing successfully completed in accordance with applicable site FFD procedure within the 30-day period prior to granting UAA/UA.
8. Form QF-0350 or QF-0351 or QF-0353 (for approved contractors) reviewed within the 30-day period prior to granting UAA.
9. Previous file reviewed (if derogatory information is developed).
10. Request for access submitted in accordance with site access request process identified in NMC Security Table QF-0382, and, if approved contractor, on *NEI's Contractor Access Request Form* or comparable.
11. Verify individual is not on *NMC Access Review List*, Table QF-0381 or identified within the Industry Shared Database as denied or requiring resolution of an access issue.
12. PIPS data entry requirements corresponding to Initial UAA elements are as follows:
- a. For each item, SAC/SAS shall complete the following fields using the PHQ and/or background investigation as the source unless otherwise specified:
 - 1) At main PIPS data entry screen, enter Social Security Number or Industry Shared Database formatted identification number in accordance with PADS 03-05 manual.

Access Authorization Program
FP-S-AA-01, Revision 6

- 2) At PIPS InProcess – New ID Number screen complete following fields:
 - a) If formatted identification number, check Non-SSN box.
 - b) Name (last, first, middle initial).
 - c) Birthdate.
 - d) Access Needed (date worker is expected to arrive for inprocessing as identified on site access request form).
 - e) Plant (enter NMC plant access is being requested for as indicated on applicable site access request form).

- 3) On Process Tab:
 - a) Requested date is the date the authorized supervisor completes the site access request form.
 - b) If no derogatory information is identified on the PHQ, Industry Shared Database Consent (date applicable NMC PHQ is completed).
 - c) Arrival date is the date site verifies individual identity in personal data section of applicable PHQ.
 - d) Supervisor is the individual requesting access as identified on site access request form.
 - e) FFD Pool (contractor or licensee as identified on site access request form).

- 4) On Employee Tab:
 - a) General Information (citizenship, applicable Industry Shared Database employer code, gender).
 - b) Current Address (street, city, state, zip code, country, phone number as identified in personal data section of PHQ).
 - c) Positive ID (height, weight, eye and hair color).
 - d) Birth Information (city, state and country).

- 5) On Access Tab:
 - a) Basis for Action is "INITIAL".

Access Authorization Program
FP-S-AA-01, Revision 6

- b) Basis date is the date you select basis for action.
- c) Utility/Approved CV is the parent company or, if approved C/V per Section 5.14, contractor submitting access request.
- d) BI Type is- "Initial".
- e) BI Submit date is the date background investigation submitted.
- f) If no derogatory information is identified in background investigation report, BI Completed date is the date 5-year background investigation is completed.
- g) Screening Company is the Industry Shared Database code for company performing background investigation.
- h) Holding Company is the entity maintaining the records supporting UAA (parent-company or, if approved C/V per Section 5.14, contractor submitting access request).
- i) Military Submitted date is the date request for military history is initiated.
- j) If no derogatory information is received, Military Received date is the date military history is received.
- k) Fingerprint Data is: dates submitted/received, results "Yes" or "No".
- l) Psychological Data is: Test Date is date of test, Interview Date is date of interview (if required), Screening Company is code for entity performing psychological services, if interview is required, check Interview Box, if interview recommends against the granting of access, check Interview Failed Box, Holding Company is the parent-company for the site access is being requested or, if approved C/V per Section 5.14, contractor submitting access request).
- m) Chemical Test Performed is the date of collection, Type of Test is the 10CFR26 test type, Results are P-Alc, fail or pass, Screening Company is the laboratory performing the urine analysis, Holding Company is the parent-company for site access is being requested or, if approved C/V per Section 5.14, contractor submitting access request, Utility/Approved CV is NMC

Access Authorization Program
FP-S-AA-01, Revision 6

- or other licensee or approved CV performing test.
 - n) If no derogatory information is received, Suitable Inquiry Completed (date suitable inquiry completed by background firm.
- 6) On Schedule Tab:
- a) Add "INPROCESSING" task, check the Needed, Start and Completed boxes and enter date and time inprocessing was initiated using the time and date recorded on the applicable PHQ and the date and time UAA is granted as the Completed date and time.
- b. For each item, SAS/SAAL shall complete the following fields using the PHQ and/or background investigation as the source unless otherwise specified:
- 1) On Process Tab:
 - a) If derogatory information is identified on the PHQ, enter date Industry Shared Database Consent form is completed (date applicable NMC PHQ Form is completed).
 - 2) On Access Tab:
 - a) If derogatory information is identified in background investigation report, Background Investigation Completed date is the (date 5-year background investigation completed.
 - b) If derogatory military information is received, Military History Received is the date requested military history verification is received.
 - c) If derogatory Fingerprint Data is received, enter "Yes" in Results field.
 - d) If derogatory suitable inquiry information is received, Suitable Inquiry Completed date is the date suitable inquiry information is received from the background investigation company. If a suitable inquiry record is established regarding an incident subsequent to the individual's last unescorted access, check Suitable Inquiry

Information Developed Box and enter parent company in Where field.

- 3) On Derogatory Tab:
 - a) If derogatory information is identified in the background investigation, military history verification, or criminal history check, enter corresponding incident date(s), description and notes (optional).

5.4 REINVESTIGATIONS

5.4.1 General

1. A reinvestigation as defined in Section 5.4.2 shall be conducted of all individuals maintaining UA, where the period since the last investigation is greater than five years.
 - a. The last investigation date is the:
 - 1) Reinvestigation date in PADS, or
 - 2) Date UA was granted corresponding to the last update or full investigation.
2. Periodic reinvestigations as defined in Section 5.4.2 shall be conducted of all individuals maintaining UA at periods not to exceed five years.
3. Reinvestigations for individuals holding UA on January 7, 2004, where the period since the last investigation is greater than five years, shall be completed no later than January 6, 2004.
4. Data developed in the conduct of the reinvestigation shall be:
 - a. Compared to the access authorization records of the person named in the developed records to ensure the person has complied with self-reporting requirements, including verification with the licensee(s) where reporting should have occurred, and
 - b. Evaluated in accordance with Section 5.11 to determine impact of developed information on access authorization.

5. Submissions of fingerprints for review of criminal history should be processed separately from investigations for outage staffing, to preclude inadvertent outage staffing delays.

5.4.2 Reinvestigation Elements

1. Credit check completed as defined in Section 5.3.3.
2. FBI criminal history check completed as defined in Section 5.3.4.
3. Verification of identity completed in accordance with Section 5.3.3.6 and documented on NMC Form QF-0319, Reinvestigation PHQ.
4. Form QF-0319 completed prior to initiating reinvestigation.
5. Previous file reviewed (if derogatory information is developed).
6. PIPS data entry requirements corresponding to Reinvestigation elements are as follows:
 - a. For each item, SAC/SAS shall complete the following fields using the PHQ and/or background investigation as the source, unless otherwise specified:
 - 1) At main PIPS data entry screen, enter Social Security Number or formatted identification number in accordance with Industry Shared Database 03-05 manual.
 - 2) On Process Tab:
 - a) PADS Consent Date is the date NMC Form QF-0319 is completed.
 - 3) On Access Tab:
 - a) BI Type is "REINVESTIGATION".
 - b) BI Submitted Date is the date reinvestigation background investigation initiated.
 - c) If no derogatory information is developed, the BI Completed Date is the date the information is evaluated in accordance with Section 5.11, provided the criminal record

Access Authorization Program
FP-S-AA-01, Revision 6

- check results and credit check received dates are within the previous 30-days, or, enter the least recent date the credit or criminal check results are received.
 - d) Credit Date Received is the date credit report is received).
 - e) Holding Company (parent-company for site where access is being requested or, if approved C/V per Section 5.14, contractor submitting access request).
 - f) Screening Company is the Industry Shared Database code for company performing background investigation.
 - g) Fingerprint Data: dates submitted/received, results "Yes" or "No".
 - 4) On Schedule Tab:
 - a) Add "REINVESTIGATION" task, check the Needed, Start and Completed boxes and enter date and time inprocessing was initiated using the time and date recorded on Form QF-0319 and the date and time reinvestigation is completed as the Completed date and time.
- b. For each item, SAS/SAAL shall complete the following fields using the PHQ and/or background investigation as the source unless otherwise specified:
- 1) On Access Tab:
 - a) BI Completed Date is: If derogatory information is identified in reinvestigation, enter the date the information is evaluated in accordance with Section 5.11, provided the criminal record check results and credit check received dates are within the previous 30-days, or enter the least recent date the credit or criminal check results are received.
 - 2) On Derogatory Tab:
 - a) If derogatory information is identified in the background investigation, enter corresponding incident date(s), description and notes (optional).

5.5 UPDATED UAA

5.5.1 General

1. An updated UAA may be granted where the last UAA at an NMC or licensee site was favorably terminated greater than 365 days but less than 3 years prior to the date UAA at an NMC site is granted.
2. Updated UAA elements shall be completed as identified in Section 5.3, Initial UAA Elements, covering the period of time since last unescorted access was favorably terminated.

5.6 REINSTATEMENT OF UAA

5.6.1 General

1. Individuals may be eligible for a reinstatement of UAA provided their last UA under a licensee UAA program is current or was favorably terminated within the previous 365 days.

5.6.2 Determining UAA Reinstatement Elements

1. For individuals with last UA favorably terminated under a licensee UAA program within the 30 days prior to granting UAA, proceed to Section 5.6.4.
2. For individuals with last UA favorably terminated under a licensee UAA program greater than 30 but less than or equal to 365 days prior to granting UAA, proceed to Section 5.6.3.
3. For individuals with UA current under a licensee UAA program, proceed to Section 5.6.5.

5.6.3 Reinstatement Elements – Last UA Favorably terminated > 30 & < or = to 365 Days Prior to Date UAA is Granted at an NMC Site

1. The following elements shall be completed prior to evaluating an individual for NMC UAA:
 - a. Verification of identity completed in accordance with Section 5.3.3.6 and documented on applicable NMC Security Form QF-0352, or QF-1704.

Access Authorization Program
FP-S-AA-01, Revision 6

- b. If individual has not been continuously subject to a licensee random drug and alcohol testing program since UA was terminated or has not had a negative drug and alcohol test within the last 30 days in accordance with a licensee or NMC approved contractor program, collection of a urine specimen for drug testing and receipt of negative alcohol test results completed in accordance with applicable site procedure within the 30-day period prior to granting UAA/UA.
 - c. NMC Security Form QF-0352/QF-1704 or QF-0353/QF-1705 (if approved contractor) is completed by individual and reviewed by SAS within the 30-day period prior to granting UAA.
 - d. Previous file reviewed (as applicable).
 - e. Site access request process completed (see NMC Security Table QF-0382), and if approved contractor, *NEI's Approved Contractor Access Request Form*, or comparable, completed.
 - f. Verify worker is not on *NMC Access Review List*, Table QF-0381 or identified within the Industry Shared Database as denied or requiring resolution of an access issue.
 - g. Verify last UAA is not a temporary UAA.
2. Following the reinstatement of UAA/UA, the following elements shall be completed:
- a. Unless subject to a behavior observation program since last UA, within the following time frames and authorization, for the period of time since the individual last held UAA/UA to the date the individual completes the PHQ, verify the length and nature of employment and unemployment as defined in Section 5.3.3.1.a for the longest claimed employment in each calendar month and any unemployment greater than 30 days:
 - 1) Within five (5) business days following the granting of UA, or
 - 2) If the investigation in 5.6.3.2.a is not completed within Five (5) business days following the

**Access Authorization Program
FP-S-AA-01, Revision 6**

granting of UA, UA may be extended for up to 10 business days following the granting of UA provided:

- a) No potentially disqualifying information (i.e., derogatory information as defined in Section 5.11.2) is identified within the previous five-year period (in Industry Shared Database or individual's NMC access authorization file), and;
 - b) SAAL has authorized the five-day extension by signing next to the UA Granted block on the respective hard copy PIPS file checklist.
- 3) If the investigation in 5.6.3.2.a is not completed within Ten (10) business days following the granting of UA, UA shall be administratively suspended pending completion of required elements.
- b. As required in accordance with Section 5.6.3.1.b, receipt of negative drug test results within five (5) business days of collection. If results are not received within the five (5) business days following the collection, UA shall be administratively suspended pending receipt of negative drug test results.
3. PIPS data entry requirements corresponding to reinstatement or transfer of UA > 30 & < or = to 365 days prior to date UAA is Granted at an NMC site are as follows:
- a. Prior to granting UAA, for each item, SAC/SAS shall complete the following fields using the PHQ and/or background investigation as the source unless otherwise specified:
 - 1) At main PIPS data entry screen, enter Social Security Number or formatted identification number in accordance with Industry Shared Database manual.
 - 2) At PIPS InProcess – New ID Number screen complete following fields:
 - a) If formatted identification number, check Non-SSN box.

Access Authorization Program
FP-S-AA-01, Revision 6

- b) Name (last, first, middle initial).
 - c) Birthdate.
 - d) Access Needed (date worker is expected to arrive for inprocessing as identified on site access request form).
 - e) Plant (enter NMC plant access is being requested for as indicated on applicable site access request form).
- 3) On Process Tab:
- a) Requested date is the date the authorized supervisor completes the site access request form.
 - b) If no derogatory information is identified on the PHQ, Industry Shared Database Consent date is the date applicable NMC PHQ is completed.
 - c) Arrival date is the date site verifies individual identity in personal data section of applicable PHQ.
 - d) Supervisor is the individual requesting access as identified on site access request form.
 - e) FFD Pool (contractor or licensee as identified on site access request form).
- 4) On Employee Tab:
- a) General Information (citizenship, applicable Industry Shared Database employer code, gender).
 - b) Current Address (street, city, state, zip code, country, phone number as identified in personal data section of PHQ).
 - c) Positive ID (height, weight, eye and hair color).
 - d) Birth Information (city, state and country).
- 5) On Access Tab:
- a) Basis for Action – “REINSTATEMENT 31 TO 365 DAYS” or equivalent.
 - b) Basis date is the date you select basis for action.
 - c) Utility/Approved CV is the parent company for site where access is being requested or,

Access Authorization Program
FP-S-AA-01, Revision 6

- a) If derogatory information is identified on the PHQ, enter date Industry Shared Database Consent form is completed (date applicable NMC PHQ is completed).
- 2) On Derogatory Tab:
 - a) If derogatory information is identified on the PHQ, enter corresponding incident date(s), description and notes (optional).
- c) Subsequent to granting UAA,, for each item, SAC/SAS shall complete the following fields using the PHQ and/or background investigation as the source, unless otherwise specified:
 - 1) On Access Tab:
 - a) If no derogatory information is identified in the background investigation report, Background Completed Date is the date employment/suitable inquiry background investigation is completed.
 - b) Holding Company is the entity maintaining the records supporting UAA (parent-company or, if approved C/V per Section 5.14, contractor submitting access request).
 - c) Chemical Test (Results are as applicable "P-Alc, fail or pass" .
 - d) If no derogatory information is identified in the suitable inquiry background investigation report, Suitable Inquiry Completed date is the date the employment/suitable inquiry background investigation report is completed.
- d) Subsequent to granting UAA,, for each item, SAS/SAAL shall complete the following fields using the PHQ and/or background investigation as the source unless otherwise specified:
 - 1) On Access Tab:
 - a) If derogatory information is identified in the background investigation report, Background Investigation Completed and Suitable Inquiry

Completed dates is the date employment/suitable inquiry background investigation is completed. If a suitable inquiry record is established regarding an incident subsequent to the individual's last unescorted access, check Suitable Inquiry Information Developed Box and enter parent company as site Where Developed.

- b) Holding Company is the entity maintaining the records supporting UAA (parent-company or, if approved C/V per Section 5.14, contractor submitting access request).

2) On Derogatory Tab:

- a) If derogatory information is identified in the background investigation, enter corresponding incident date(s), description and notes (optional).

5.6.4 Reinstatement Elements – UA Favorably Terminated under a Licensee UAA program within the 30 Days Prior to Granting UAA at an NMC Site

1. The following elements shall be completed prior to evaluating a worker for NMC UAA:
 - a. Verification of identity completed in accordance with Section 5.3.3.6 and documented on NMC Security Form QF-0353/QF-1705.
 - b. Previous file reviewed (if derogatory information is developed).
 - c. Site access request process completed (see NMC Security Table QF-0382), and if approved contractor, *NEI's Approved Contractor Access Request Form*, or comparable, completed.
 - d. Verify worker is not on *NMC Access Review List*, Table QF-0381 or identified within the Industry Shared Database as denied or requiring resolution of an access issue.
 - e. Verify last UAA is not a temporary UAA.

Access Authorization Program
FP-S-AA-01, Revision 6

2. PIPS data entry requirements corresponding to reinstatement or transfer of UA/UAA < or equal to 30 days prior to date UAA is Granted at an NMC site are as follows:
 - a) Prior to granting UAA, for each item, SAC/SAS shall complete the following fields using the PHQ and/or background investigation as the source unless otherwise specified:
 - 1) At main PIPS data entry screen, enter Social Security Number or Industry Shared Database formatted identification number in accordance with Industry Shared Database manual.
 - 2) At PIPS InProcess – New ID Number screen complete following fields:
 - a) If Industry Shared database formatted identification number, check Non-SSN box.
 - b) Name (last, first, middle initial).
 - c) Birthdate.
 - d) Access Needed (date worker is expected to arrive for inprocessing as identified on site access request form).
 - e) Plant (enter NMC plant access is being requested for as indicated on applicable site access request form).
 - 3) On Process Tab:
 - a) Requested date is the date the authorized supervisor completes the site access request form.
 - b) If no derogatory information is identified on the PHQ, Industry Shared Database Consent (date applicable NMC PHQ is completed).
 - c) Arrival date is the date site verifies individual identity in personal data section of applicable PHQ.
 - d) Supervisor is the individual requesting access as identified on site access request form.
 - e) FFD Pool (contractor or licensee as identified on site access request form).
 - 4) On Employee Tab:

Access Authorization Program
FP-S-AA-01, Revision 6

- a) General Information (citizenship, applicable Industry Shared Database employer code, gender).
 - b) Current Address (street, city, state, zip code, country, phone number as identified in personal data section of PHQ).
 - c) Positive ID (height, weight, eye and hair color).
 - d) Birth Information (city, state and country).
- 5) On Access Tab:
- a) Basis for Action is "REINSTATEMENT 30 DAYS OR LESS" or equivalent.
 - b) Basis date (date you select basis for action).
 - c) Utility/Approved CV (parent-company for site where access is being requested or, if approved CV per Section 5.14, contractor submitting access request).
 - d) BI Type Reinstatement 30 Days or Less
 - e) BI Submit date is the date the PHQ is completed.
 - f) BI Completed date is the date PHQ is completed.
 - g) BI Screening Company is the parent company.
 - h) BI Holding Company is the parent company.
 - i) Suitable inquiry date the date the PHQ is completed.
- 6) On Badge Tab:
- a) Last Access – enter date individual last held UAA in accordance with a licensee UAA program.
- 7) On Schedule Tab:
- a) Add "INPROCESSING" task, check the Needed, Start and Completed boxes and enter date and time inprocessing was initiated using the time and date recorded on the applicable PHQ and the date and time UAA is granted as the Completed date and time.

**Access Authorization Program
FP-S-AA-01, Revision 6**

- b. Prior to granting UAA, for each item, SAS/SAAL shall complete the following fields using the PHQ and/or background investigation as the source unless otherwise specified:
 - 1) On Process Tab:
 - a) If derogatory information is identified on the PHQ, enter the date the Industry Shared Database Consent form is completed (date applicable NMC PHQ is completed).

5.6.5 Reinstatement Elements – UA current under a Licensee UA Program

- 1. If the individual's UA is **current under a non-NMC licensee UA Program**, the following elements shall be completed prior to evaluating an individual UAA:
 - a. Verification of identity completed in accordance with Section 5.3.3.6 and documented on NMC Security Form QF-0353.
 - b. Previous file reviewed (if derogatory information is developed).
 - c. Site access request process completed (see NMC Security Table QF-0382), and if approved contractor, *NEI's Approved Contractor Access Request Form*, or comparable, completed.
 - d. Verify worker is not on *NMC Access Review List*, Table QF-0381 or identified within the Industry Shared Database as denied or requiring resolution of an access issue.
- 2. If the individual's UA is **current at an NMC site**, the following elements shall be completed prior to evaluating an individual UAA:
 - a) Verification of identity completed in accordance with Section 5.3.4.6 and documented on NMC Security Form QF-0354 or QF-0365.

b) Previous file reviewed (if derogatory information is developed).

) Site access request process completed (see NMC Security Table QF-0382), and if approved contractor, NEI's Approved Contractor Access Request Form, or comparable, completed.

5.6.6 Incomplete UAA Reinstatement Elements

1. If any of the required elements for an UAA determination cannot be completed due to the individual leaving the site, the SAS shall consult with the SAAL.
2. If the SAAL concurs the element is required for determination for UAA, the SAS shall document the reason on the Derogatory Tab.
3. The SAAL shall enter into PIPS:
 - a. If the individual leaves the site prior to the granting of UAA, a basis for action of "Admin Data" on the Access Tab.

5.7 ENHANCED OVERSIGHT

5.7.1 General

1. Workers granted access to vital or ISFSI areas as identified in Attachment 5, Section B shall:
 - a. Perform essential work.
 - b. Be subject to oversight by a worker with an access authorization type as designated in Attachment 5, Section B.

5.7.2 Responsibilities

1. Prior to granting workers vital or ISFSI area access as designated in Attachment 5, Section B, Security shall:
 - a. Verify workers meet the requirements of Section 5.7.1.1.
 - b. Communicate to badge sponsors the identity of workers granted vital or ISFSI Attachment 5, Section B, area access.

- c. Verify the badge sponsor has an access authorization type as designated in Attachment 5, Section B and has completed Form QF-0391.
- 2. Badge sponsors shall:
 - a. Ensure workers with Attachment 5, Section B UAA only enter vital or ISFSI areas to perform essential activities and that oversight is provided as identified in section 5.7.3.
 - b. Complete Form QF-0391 to acknowledge understanding of oversight responsibilities for workers performing essential activities in the vital or ISFSI areas with Attachment 5, Section B UAA.

5.7.3 Oversight of Workers with Attachment 5, Section B UAA in Vital or ISFSI Areas

- 1. Workers with Attachment 5, Section B UAA performing essential activities in the vital or ISFSI areas shall be subject to oversight. Workers providing oversight of activities in vital or ISFSI areas:
 - a. Shall have unescorted access to the vital or ISFSI area.
 - b. Shall have an access authorization type as designated in Attachment 5, Section B.
 - c. Shall monitor activities on a frequency sufficient to ensure workers are not engaging in unauthorized activities.
 - d. May monitor more than one worker at a time.
 - e. Are not required to maintain constant visual contacts of workers being monitored.
 - f. If unable to provide oversight, shall ensure another worker is designated to assume oversight responsibilities.

5.8 CRIMINAL HISTORY CHECKS

5.8.1 Responsibilities

- 1. The SAAL shall be responsible for:

**Access Authorization Program
FP-S-AA-01, Revision 6**

- a. Ensuring a sufficient number of individuals are trained for the taking of fingerprints.
 - b. Approving best efforts for criminal history checks in accordance with NMC Security Form QF-0361, *Best Effort Documentation for Criminal History Check*.
2. The SAC shall be responsible for:
- a. Ensuring individuals are positively identified by photo identification prior to being fingerprinted.
 - b. Ensuring only satisfactory quality fingerprints are submitted to the NRC.
3. Personnel assigned responsibilities for fingerprinting shall:
- a. Ensure individuals are positively identified by a photo identification prior to being fingerprinted.
 - b. Ensure only satisfactory quality fingerprints are submitted to SAC.
4. In the SAAL's absence, the SAS shall assume the responsibilities for the SAAL as defined in Section 5.8.

5.8.2 General

1. The following individuals shall have criminal history checks performed:
 - a. Individuals seeking unescorted access to NMC nuclear sites requiring criminal history checks as defined herein.
 - b. Individuals seeking access to safeguards information as defined by 10 CFR 73.21.
2. To obtain a criminal history check, individuals shall be fingerprinted.
3. Fingerprints shall be submitted through the Nuclear Regulatory Commission, to the Federal Bureau of Investigation (FBI).
4. All information obtained through the criminal history records check shall be used solely for the purpose of determining an individual's suitability for Access Authorization or access to safeguards information.

5.8.3 Exemptions

1. Individuals exempt from the aforementioned requirements are:
 - a. NRC employees and NRC contractors on official agency business.
 - b. Individuals responding to a site emergency in accordance with 10 CFR 73.55(a).
 - c. Representatives of the International Atomic Energy Agency engaged in activities associated with the US/IAEA Safeguards Agreement.
 - d. Law enforcement personnel acting in an official capacity.
 - e. State or local government employees who have equivalent reviews of FBI Criminal history data.
 - f. Individuals employed at a facility possessing Federal (Q) or (L) clearances, or other government security clearances such as Top Secret, Secret or Confidential.

5.8.4 Prohibitions

1. A final determination to deny an individual access authorization shall not be based solely upon the information received from the FBI involving:
 - a. An arrest of more than one (1) year old for which there is no information of disposition.
 - b. An arrest that resulted in dismissal of the charge or an acquittal.
2. Information received from the Criminal History shall not be used in any manner that would:
 - a. Infringe upon the rights of the individual under the First Amendment to the Constitution of the United States.
 - b. Discriminate among individuals on the basis of race, religion, sex, age, or national origin.

5.8.5 Criminal History Self-Disclosure

1. Upon determination that an individual requires fingerprinting in accordance with Section 5.8.2, the individual responsible for fingerprinting shall:
 - a. Verify the individual's identity through a cross comparison of the individual's physical characteristics to a photo identification.
 - b. Document the type of identification verified on NMC Security Form QF-0350 or QF-0351, Section I.
 - c. Instruct the individual to complete NMC Security Form QF-0350 or QF-0351, Section X.

5.8.6 Fingerprinting the Individual

1. The individual responsible for fingerprinting shall:
 - a. Roll fingers onto fingerprint card or device using the site fingerprinting system.
 - b. Take fingerprints according to finger printing system instructions.
 - c. Closely inspect the fingerprints to ensure adequate quality.
2. While there are many methods/styles for fingerprinting, the individual conducting the process is encouraged to develop a comfortable and reliable style. The following depicts several unique situations associated with fingerprinting and if applicable, corrective actions:
 - a. **Dirty or Greasy Hands**

Because excess oil or dirt on the individual's hands can result in rejectable prints, individuals should be instructed to wash their hands before being printed.
 - b. **Sweaty Hands**

Often times caused from the anxiety associated with fingerprinting; individuals should first towel their hands and if necessary apply a light coating of talcum powder. This will help raise the definition of the fingerprint and reduce the likelihood of rejection.

**Access Authorization Program
FP-S-AA-01, Revision 6**

c. **Amputated Fingers**

Missing or scarred fingers should be clearly identified by description on the fingerprint card.

3. **The individual responsible for fingerprinting shall:**

- a. Type or write the information from NMC Security Form QF-0350 or QF-0351 onto the Fingerprint Card.
- b. Instruct the individual to sign the fingerprint card certifying the prints are authentic (signature not required if using Electronic Fingerprinting System, EFS).
- c. Sign and date the fingerprint card (not required if using EFS).
- d. Submit the completed fingerprint cards with NMC Security QF-0350 or QF-0351 to NMC Security.

5.8.7 Fingerprint Card or EFS Submittal

1. Upon receipt of completed fingerprint cards or EFS images, the assigned SAS shall:
 - a. Inspect the fingerprints for adequate quality.
 - b. Reprint individuals if fingerprints are of unsatisfactory quality.
 - c. Ensure the fingerprint card or EFS is completely filled out.
 - d. Submit acceptable fingerprint cards or EFS requests with correct processing fee to:

U.S. Nuclear Regulatory Commission
Division of Facilities and Security/CHP
11545 Rockville Pike
Mail Stop T-6 E46
Rockville, MD 20852

5.8.8 Handling Rejected & Unclassifiable Fingerprints

1. See Attachment 5 to this procedure.

5.8.9 Receipt of Criminal History Records

1. Upon receipt of criminal history records or Fingerprint cards or EFS results indicating "No Arrest Record on File" from the NRC, the assigned Personnel Security Section member shall update applicable site electronic databases.
2. Criminal history records returned by the NRC containing criminal history shall be immediately forwarded to the SAAL for review in accordance Sections 5.10, Investigating Derogatory Information and 5.11, Evaluation for Unescorted Access Authorization and Attachment 5 to this procedure.

5.9 PSYCHOLOGICAL EVALUATIONS

5.9.1 Responsibilities

1. SASs shall be responsible for:
 - a. Controlling testing materials.
 - b. Scheduling testing and clinical interviews.
 - c. Providing relevant background information to psychologists performing clinical interviews.
 - d. Proctoring tests.
 - e. Scoring tests as required to expedite processing.
2. NMC approved licensed psychologists shall be responsible for:
 - a. Scoring and interpreting tests.
 - b. Performing clinical interviews.
 - c. Based upon results of the evaluation process, recommending to NMC Security whether individuals meet psychological requirements for nuclear access authorization.

5.9.2 General

1. Individuals requiring psychological evaluations shall complete the Minnesota Multiphasic Personality Inventory-2 (MMPI-2).

Access Authorization Program
FP-S-AA-01, Revision 6

2. Psychological tests, clinical interviews and relevant background information (as requested by psychologist) shall be interpreted and conducted respectively by licensed psychologists.
3. As requested by an NMC approved psychologist, an individual may be required to complete additional tests (e.g. California Personality Inventory).
4. Psychological evaluations shall not be initiated without individual consent as indicated by completion of NMC Security Form QF-0350 or QF-0351, Section VII, *Authorization for Release of Information to the Nuclear Management Company*.
5. Delivery of psychological tests and results as required herein shall be by means of hand-delivery, secure fax, or mail in a sealed envelope marked confidential.

5.9.3 Proctoring Tests

1. Individuals shall be given a copy of NMC Security Forms QF-0362, *Psychological Test Information*.
2. Individuals may (as determined by NMC psychologists) be required to complete NMC Security Form QF-0363, *Psychological Release* (or comparable), prior to completing psychological tests.
3. All individuals requiring psychological evaluations shall complete the Minnesota Multiphasic Personality Inventory-2 (MMPI-2).
4. Personnel responsible for proctoring shall complete proctor training recommended by psychologist.
5. Completion of tests shall be proctored as follows:
 - a. Testing of more than one individual shall be observed by a proctor.
 - b. Testing of one individual may be done unobserved if done in an unoccupied private space to which access is controlled by the individual proctoring the test. The individual proctoring the test shall periodically, and on an unannounced basis, observe the individual being tested.
 - c. Individuals shall not be permitted to talk to others during testing.

- d. Tests shall be examined to ensure completeness. All questions should be answered. More than 10-questions left unanswered shall invalidate the test and require to be retaken.
- e. Individual identification shall be verified through a cross comparison of the individual's physical characteristics to photo identification.
- f. Completed tests shall be placed in a sealed envelope, marked confidential and sent to the SAC or SAS.

5.9.4 Scoring and Interpreting Tests

- 1. Tests and corresponding questionnaire(s) (as requested by psychologist) shall be confidentially delivered to the psychologist assigned to interpret the tests.
- 2. Psychologist shall use predetermined cutoff values for each scale on test to determine if a clinical interview is needed.
- 2. If the psychologist's test interpretation indicates individual meets psychological criteria for unescorted access, the psychologist shall prepare documentation referenced in Section 5.9.6 (1) indicating worker is acceptable for unescorted access.
- 3. If psychologist's test interpretation indicates a clinical interview is needed, psychologist shall confidentially communicate to the site the need for a clinical interview.

5.9.5 Clinical Interviews

- 1. SAC/SASs shall schedule clinical interviews.
- 2. As requested by the interviewing psychologist, SAC/SAS shall provide relevant background information in an individual's security dossier.
- 3. Prior to conducting clinical interviews, psychologists shall verify identity. Identity may be verified using photo identification (e.g. Driver's license, Military ID or Passport).
- 4. Psychological evaluation results following interview shall be communicated to NMC Security in accordance with Section 5.9.6.

5.9.6 Documenting Evaluation Results

1. Based upon the results of test and applicable interview interpretation, psychologists shall make written recommendations to NMC Security on whether individuals meet psychological criteria for unescorted access which minimally contain:
 - a. Individual's name and SSN.
 - b. The basis of the recommendation; written test results, test results and interview data, or test results and interview data and background information.
 - c. Name, signature and license number with expiration date of the licensed psychologist that interpreted the written tests and/or conducted the clinical interview.

5.9.7 Controlling Psychological Testing Materials

1. Testing materials consist of MMPI-2 answer sheets and test booklets.
2. Testing materials shall be placed in a secured area when , unattended.
3. Access to testing materials shall be to individuals with a need to perform responsibilities defined herein.

5.9.8 Audits

1. NMC shall audit providers of psychological services once every 24 months to evaluate conformance to NMC and regulatory requirements.
2. Audits shall minimally verify that:
 - a. Adequate procedural controls are in place to ensure compliance with NMC's specification for nuclear psychological services.
 - b. Licensed psychologists make recommendations.
 - c. Subject identity is properly verified.
 - d. Psychologist files contain the following:

- 1) MMPI test sheets and results.
- 2) Recommendations consistent with recommendations on file at NMC.

5.10 INVESTIGATING DEROGATORY INFORMATION

5.10.1 General

1. Information obtained through the PHQ, conduct of the background investigation, suitable inquiry, behavior observation program and psychological evaluation shall be reviewed in accordance with Section 5.11, Evaluation for UAA, for the identification of derogatory information.
2. Derogatory information previously disclosed and resolved that is subsequently received or developed by NMC Security need not be re-investigated.
3. If during an informational interview, the individual discloses derogatory information not previously disclosed, the SAS shall stop the interview and arrange for a non-accusatory, issue related interview in accordance with Section 5.10.3.

5.10.2 Investigation

1. Once derogatory information has been identified in accordance with Section 5.11, the assigned SAS shall review the derogatory information with the SAAL.
2. The SAAL shall determine if the derogatory information needs further investigation. This determination should be based upon the severity, relevancy, and age of the information.
3. If the SAAL determines further investigation is required, the SAS shall conduct a non-accusatory, issue-related interview with the individual in accordance with Section 5.10.3.
4. If the individual cannot be located for the interview, the SAS shall:
 - a. Consult with the SAAL.
 - b. Suspend UA as applicable and evaluate the information in accordance with Section 5.11.
 - c. Document the reason on the PIPS Derogatory Tab.

5. If the derogatory information involves criminal charges, arrests, and/or convictions (with no disposition) meeting Attachment 5 criteria, the local criminal history records should be obtained from the applicable county, state, or local law enforcement.

NOTE: If the individual discloses derogatory information on the PHQ meeting Attachment 5 criteria, obtaining local criminal history records is not required.

5.10.3 Interview Guidelines

1. If the interview involves clarification of derogatory information discovered during a criminal history check, the NMC Security Section member shall also perform the items stated in Section 5.10.5.
2. The SAS shall:
 - a. Verify identity by comparing a valid government issued photo identification to the individual's physical characteristics.
 - b. Inform the individual that the interview is a non-custodial interview and that the person is free to leave or terminate the interview at any time.
 - c. Allow the individual to have representation (e.g., union or legal) during the interview. However, the role of this representation is simply to document and observe the proceedings.
3. Interview results shall be documented on the PIPS Derogatory Tab.
4. If the individual refuses to participate in the interview, the SAS shall document refusal on the PIPS Derogatory Tab.

5.10.4 Substantiating Derogatory Information

1. Based upon the evaluation results of the background investigation and/or interview the SAAL may expand the initial scope of the access authorization process to substantiate unresolved allegations or derogatory information.

2. If, after evaluating information obtained during the background investigation and/or the interview process, the SAS was unable to prove or disprove the derogatory information, the SAAL may request the SAS to conduct further investigative efforts. This may include:
 - a. Requiring the NMC approved investigative agency to re-verify information from prior sources.
 - b. Contacting additional sources to corroborate the individual's case.
 - c. Obtaining additional criminal history records.
3. The SAS shall ensure their efforts to prove or disprove derogatory information are properly documented and recorded in the individual's security dossier.

5.10.5 Derogatory Information from Criminal History

1. When interviewing individuals concerning derogatory information obtained through a criminal history check in accordance with Section 5.8, Criminal History Checks, the SAS shall:
 - a. Review the criminal history record with the individual.
 - b. Provide the individual with a copy of the criminal history record and 10CFR73.57, if the individual believes the information is incorrect or incomplete in any respect, and wishes to initiate challenge procedures.

5.10.6 Case Finalization

1. Subsequent to the interview process the SAS shall document the results of the interview on NMC Security Form QF-0365 or the PIPS Derogatory Tab, including:
 - a. Pertinent administrative items, i.e., location, date and time of interview, who was present and any special requests made by the individual during the interview.
 - b. Acknowledgement and identification of all advisement provided to the individual.

- c. A detailed, narrative of interview results to include: admissions, and/or confessions regarding the information being investigated.
2. Once completed, NMC Security Form QF-0365 or the PIPS Derogatory Tab shall be evaluated in accordance with Section 5.11.
3. Notes, memorandums or miscellaneous correspondence collected during the investigation shall be maintained in original form, in the screening file.

5.11 EVALUATION FOR UAA

5.11.1 General

1. Information obtained through the PHQ, conduct of the background investigation, suitable inquiry, psychological evaluation and behavior observation program shall be used to determine the potential to adversely affect the individual's reliability, trustworthiness and emotional stability.
2. True identity shall be evaluated by comparing individual provided identification and PHQ data to pertinent information from the background investigation, credit report and other sources (e.g., SSN, date of birth verified through an employer).
3. To ensure impartiality, NMC Security Section members shall remove themselves from an evaluation and recommendation process regarding a relative or close personal friend.
4. Recommendations for denial of UAA based upon criminal history records obtained in accordance with Section 5.8, Criminal History Checks, shall not be processed, if the individual is challenging the information, until receipt of the FBI's confirmation or correction of the record.
5. For individuals requesting access and prior to granting UAA, NMC security Section members shall review:
 - a. NMC Security Table QF-0381, *NMC Access Review List* (ARL), to determine whether approval in accordance with Section 5.11.1 (6) is needed.
 - b. PADS/PIPS to determine whether follow-up is needed for information received subsequent to an individual's termination of access.

Access Authorization Program
FP-S-AA-01, Revision 6

6. Prior to processing an individual for UAA who is currently on the ARL, the following authorization shall be documented on a memo to file or the PIPS Derogatory Tab:
 - a. For workers denied UAA, Site VP recommendation to reconsider access.
 - b. For workers requiring completion of pending UAA elements, SAAL verification of favorable resolution of pending element(s).
 - c. For workers with outstanding management return to work requirements, manager indication of favorable completion/resolution of return to work requirements.
 - d. For workers unfavorably terminated, NMC Site Human Resources recommendation to reconsider access.
7. The SAAL may require applicant interviews with a licensed Psychologist to aid in determining an individual's trustworthiness and reliability. This interview shall be conducted regardless of the results of the written psychological test.
8. Willful or intentional acts of omission or untruthfulness are grounds for denial of UAA/UA.
9. Requirements for maintaining UAA developed in accordance with site FFD programs, the behavior observation program or in accordance with applicable UAA elements shall be tracked on Form QF-0334, Nuclear UAA Active Case Log to ensure individuals are meeting UAA/FFD commitments for continued UAA. The SAAL shall assign a Section member the primary responsibility for tracking outstanding requirements to ensure timely completion. A second Section member shall be assigned to perform monthly audits of Form QF-0334 verifying timely completion of requirements. If an individual fails to meet a UAA commitment, access shall be suspended pending an investigation to determine the impact on trustworthiness and reliability and fitness for duty.

5.11.2 Derogatory Information

1. The following are definitions of derogatory information developed through the access authorization program elements (e.g., PHQ, background investigation, psychological evaluation, behavior observation program):

**Access Authorization Program
FP-S-AA-01, Revision 6**

- a. Negative information provided by a present or previous employer.
- b. Information received from the educational institution not consistent with the individual's PHQ.
- c. Criminal history, including:
 - 1) Arrests, charges, or convictions of law as disclosed on the NMC Personal History Questionnaire, developed during the background investigation, or disclosed by the worker.
 - 2) Criminal history received from NRC from FBI Criminal History Check.

NOTE: Arrests or charges that were dismissed, or resulted in an acquittal, as stated on the criminal history record received from the FBI, are not considered derogatory.
- d. Military service indicating:
 - 1) Individual received discharge that was other than honorable, as stated on his NMC PHQ or DD-214.
 - 2) Negative information on DD-214.
- e. Substantiated negative information provided by reference.
- f. Inconsistencies between information disclosed by the individual on the PHQ or otherwise and information developed through UAA program elements as defined herein.
- g. No credit history or a credit history indicating past or present bankruptcies, collection accounts, judgments or tax liens.
- h. Letter from psychologist stating individual is not recommended for unescorted access to a nuclear plant.
- i. Negative information disclosed by the worker on the NMC PHQ.

**Access Authorization Program
FP-S-AA-01, Revision 6**

- j. Willful omission or falsification of material information.
- k. Derogatory FFD information as defined in site FFD procedures.
- l. Other information that would adversely reflect upon the reliability and trustworthiness of the individual relating to granting unescorted access.
- m. NMC Security Section members shall investigate derogatory information in accordance with Section 5.10, Investigating Derogatory Information.

5.11.3 Individuals with Current Unescorted Access

- 1. Approved contractor/vendors and background investigation companies shall immediately notify the SAAL when derogatory information is developed subsequent to the granting of UAA or submittal of a background report to NMC.
- 2. Upon receipt of derogatory information not previously disclosed to NMC, the SAC/SAS shall:
 - a. Immediately inform the SAAL.
 - b. Investigate in accordance with Section 5.10.
 - c. If substantiated, evaluate the information in accordance with Section 5.11.4 (4).
- 3. The SAAL shall recommend to the Site Manager and VP suspending the individual's UAA depending on severity and previous disclosure of the derogatory information pending further investigation. If access is suspended pending additional investigation, SAAL shall:
 - a. Complete Form QF-0388.
 - b. On the PIPS Access Tab:
 - 1) Add a new screening for the applicable NMC site. Enter "ADMIN DATA" for the BFA and enter the appropriate date the BFA is applied as the Basis Date. Enter that same date in the UA Granted field. Enter the most recent consent form date in the Consent field on the Process Tab.

**Access Authorization Program
FP-S-AA-01, Revision 6**

- 2) The "ADMIN DATA" screening shall be deleted in PIPS and PADS (and verified by running a PADS synopsis report) provided the derogatory information is favorably adjudicated and the individual meets maintenance requirements as defined herein.
4. After the SAAL makes an initial request to the sites(s) to suspend unescorted access, the SAAL shall verify within one-half hour the suspension of access through the applicable site electronic database or the senior on-shift site Security Officer.

5.11.4 Individuals Requesting UAA

1. For individuals requesting UAA, SAC/SAS/SAAL(s) shall review and document completion of required UAA elements as defined in Sections 5.3-5.6 (and NMC Security Table QF-0376) in PIPS by:
 - a. Running the applicable (to BFA or investigation type) PIPS status report to ensure background elements meet defined scope requirements.
 - b. Documenting completion of actions identified on applicable PIPS status report (e.g., identity verification, review of ARL).

NOTE: Forms comparable to NMC forms shall be accepted from Contractor UAA programs approved in accordance with Section 5.14.

2. SAC/SAS(s) shall review all elements applicable to the screening type for derogatory information, as defined in Section 5.11.2.
3. If no derogatory information is identified, the SAC/SAS shall:
 - a. If PIPS status report indicates the individual meets requirement in accordance with FP-S-AA-01, sign the PIPS status report on the same day the audit report is run.
 - b. Enter current date in UA Granted Date on PIPS Access Tab (must be the same date the PIPS status report is run).
4. If derogatory information is identified, the SAAL shall:

**Access Authorization Program
FP-S-AA-01, Revision 6**

- a. Investigate the derogatory information in accordance with Section 5.10.
- b. If substantiated:
 - 1) Record the derogatory information in PIPS.
 - 2) Evaluate the information in accordance with the review criteria identified in Attachment 5 to this procedure.
 - 3) Determine whether inconsistencies are intentional, innocent, or an oversight.
 - 4) Document the evaluation of derogatory information and the decision making basis for determining trustworthiness and reliability on Form QF-0358.
 - 5) If the individual is determined not to be trustworthy and reliable, proceed to Section 5.11.5. If the Section member determines the individual is trustworthy and reliable, proceed to Section 5.11.6.
5. If the individual is unable to complete UAA elements necessary to adjudicate information in accordance with Attachment 5, on the PIPS Access Tab, change the BFA to "ADMIN DATA" and enter the corresponding date the BFA is applied as the Basis Date. Enter the same date in the UA Granted field.
 - a. If the partial elements are subsequently completed and favorably adjudicated, delete the UA Granted date, change the BFA to "PARTIAL ELEMENTS" and enter the corresponding adjudication/completion date as the BASIS DATE. A PADS synopsis report should be run to verify change in PADS.
6. For initial and update screening types as defined in Sections 5.3 and 5.5, the review required in Sections 5.11.4 (1-3) shall be performed and documented on the applicable PIPS status report by two NMC Security Section members.

5.11.5UAA Denial Process

1. SAS/SAAL(s) shall:

Access Authorization Program
FP-S-AA-01, Revision 6

- a. Document the basis for the denial by completing Section I of NMC Security Form QF-0367, *Request for Review of UAA Denial based on Background Investigation*, or NMC Security Form QF-0371, *Access Authorization Denial Based on Psychological Evaluation*.
 - b. Discuss recommendations with the SAAL.
2. The SAAL shall:
- a. Review the derogatory information to ensure proper investigation and adjudication.
 - b. If the individual's UAA was suspended in accordance with Section 5.11.3, obtain Site Director (or equivalent as determined by Site VP) approval to deny UAA and record such approval on the PIPS Derogatory Tab.
 - c. Record the UAA status recommendation in PIPS:
 - 1) For individuals requesting access, on the Process Tab, enter the date access is denied in the Deny Access Date and corresponding Reason Code from Attachment 5.
 - 2) For individuals with an open UA To Date and an "ADMIN DATA" hold:
 - a) Delete the "ADMIN DATA" screening..
 - b) On the open UA TO record change the Basis Date to the prior "ADMIN DATA" Basis Date.
 - c) Enter the "ADMIN DATA" BFA Basis Date as the UA To Date
 - d) Enter the corresponding Attachment 5, Section C, denial code as Term Reason and indicate the Term Favorable as "No".
 - e) Run a PADS synopsis report to verify the "ADMIN DATA" has been removed and "Additional Information" is indicated on SEC1.

- 3) For individuals with an open UA To Date with no BFA of "ADMIN DATA", on the Access Tab, enter the corresponding Attachment 5, Section C, reason code as Term Reason and indicate the Term Favorable as "No".
- 4) For individuals denied subsequent to a favorable termination of UA:
 - a) If an "ADMIN DATA" hold was in place, delete the "ADMIN DATA" screening.
 - b) On the Access Tab, change the Term Reason to the corresponding Attachment 5, Section C, denial code and indicate the Term Favorable as "No".
 - c) Run a PADS synopsis report to verify the "ADMIN DATA" has been removed and "Additional Information" is indicated on SEC1.
 - d) If the affected worker has been granted access at subsequent licensee site(s), immediately notify the respective site access manager(s) via phone of the access denial at NMC sites.
3. Upon approval of UAA denial, the assigned SAS shall complete notifications in accordance with Section 5.11.7.
4. Notify the individual in writing in accordance with Section 5.12.

5.11.6 Granting UAA for Individuals with Derogatory Information

1. The SAAL shall:
 - a. Review the derogatory information to ensure:
 - 1) Proper investigation and adjudication.
 - 2) The individual meets applicable FFD requirements.
 - 3) If PIPS status report indicates the individual meets requirement in accordance with FP-S-AA-01, sign

the PIPS status report on the same day the status report is run.

2. For initial and update screening types as defined in Sections 5.3 and 5.5, the review required in Sections 5.11.6.1.a (1-3), shall be performed by a second Section member at a SAS or SAAL level and documented on the applicable PIPS status report.
3. The SAC/SAS shall record the UAA status determination in PIPS.
4. Upon approval of the UAA status, the SAS shall complete the necessary notifications in accordance with Section 5.11.7.

5.11.7 UAA Status Notifications

1. The SAS shall notify the respective Site Access Coordinator after:
 - a. Granting a full UAA.
 - b. Denying an UAA.
 - c. Changing of UAA status results in suspension of unescorted access.
2. The SAS shall notify the NMC Supervisor when a change in UAA status results in suspension of unescorted access.
3. For changes in UAA status resulting in suspension of unescorted access, the SAAL shall notify:
 - a. The Site Security Manager or senior security officer.
 - b. Site NMC Department Manager.
 - c. Parent-Company Labor Relations Director for Parent-Company bargaining unit employees.
4. Notifications shall be documented on Form QF-0388, *AA Status Change Actions/Notifications*.
5. For Contractors denied UAA, notify the contractor using QF-0320, Contractor Access Denial Notification Form.

5.11.8 Access Review List Additions

**Access Authorization Program
FP-S-AA-01, Revision 6**

1. Workers shall be added to the Access Review List if:
 - a. Denied UAA.
 - b. Unfavorably terminated.
 - c. Management submits written request to SAAL to add worker. SAAL shall record basis for addition to ARL on PIPS Derogatory Tab.
 - d. Outstanding UAA/FFD requirements shall be completed prior to returning to site.
2. The ARL shall list all workers identified in Section 5.11.8.1 at NMC operated sites.
3. The designated SAAL shall be responsible for maintaining and distributing to each SAAL updates to the ARL.
 - a. Upon receipt of a name for addition to the ARL, the designated SAAL shall add the name to the ARL and distribute a copy of the updated ARL to each SAAL by the close of the next business day.
4. Upon identifying a worker to be added to the ARL, each site SAAL shall:
 - a. Manually (pen and ink with initials & date) add the worker's name to the current ARL at the site access point(s).
 - b. Provide the designated SAAL the name of the worker.
 - c. Review Industry Shared Database/PIPS to determine whether the worker has access at another licensee/NMC site and notify as appropriate.
5. SAAL shall ensure updated ARL(s) are provided to site access control points.

5.11.9 Reconsideration of Denied UAA

1. Individuals denied access authorization shall not be granted access until a substantive change in the precluding condition can be established as defined in NMC Security Table QF-0378, *Denied UAA Reconsideration Elements*.

5.12 REVIEWING UAA DENIALS

5.12.1 Responsibilities

1. The Site VP shall be responsible for deciding the disposition of requests for review of UAA denials based on background investigations.
2. The NMC Site Access Authorization Lead shall be responsible for:
 - a. Briefing the Site VP on review requests received and coordinating disposition.
 - b. Notifying individuals of review dispositions.
3. NMC Site Access Specialists shall be responsible for:
 - a. Preparing individual notification of denial letters and right to review applications.

5.12.2 General

1. To ensure impartiality, NMC Security members shall remove themselves from any review process regarding a relative, co-worker or close personal friend.
2. Pending final disposition of review request, access authorization shall remain suspended or denied.
3. Individuals for whom access authorization is reversed shall become immediately eligible to reapply for access authorization.
4. Actions taken in response to the review requests shall be documented on NMC Security Form QF-0367, *Request for Review of UAA Denial Based on Background Investigation*, for background investigation based denials or in a letter from an NMC psychologist for denials of UAA based upon psychological evaluations.
5. Reviews of UAA denials based on psychological evaluations shall be conducted by an NMC approved psychologist other than the NMC psychologist recommending the denial and limited to the following scope:
 - a. Was the psychological test properly administered and scored.

- b. Whether the psychologist recommendation to NMC is reflected in the psychologist's case file.

5.12.3UAA Denial Notification

1. As applicable, SAALs or the ACL are responsible for notifying all individuals denied access authorization in accordance with Section 5.11 of their right to request a review. This notification should be made in-person during in-processing where practical or by letter via certified mail within 10 days following the access authorization denial.
2. Individuals denied based on a background investigation shall be notified of:
 - a. Their right to request a review with NMC Security Form QF-0368, *Notice of UAA Denial Based on Background Information*, and NMC Security Form QF-0367, *Request for Review of UAA Denial Based on Background Investigation*.
 - b. Review request dispositions with NMC Security Form QF-0369 or QF-0370, *Request for Review of UAA Denial Based on Background Investigation Disposition*.
3. Individuals denied based on a psychological evaluation shall be notified of:
 - a. Their right to request a review with NMC Security Form QF-0371, *Notice of UAA Denial Based on Psychological Evaluation*.
 - b. Review request dispositions with NMC Security Form QF-0372 or QF-0373, *Request for Review of UAA Denial Based on Psychological Evaluation Disposition*.

5.12.4NMC Site VP Review

1. The NMC Site Access Authorization Lead shall brief the responsible Site VP on all review requests of denials based on background information, presenting the basis for denial and information supporting review requests.
2. NMC Site VP disposition of the review request shall be documented on NMC Security form QF-0367.

5.13 BEHAVIORAL OBSERVATION PROGRAM (BOP)

5.13.1 Responsibilities

1. Site Nuclear Training shall be responsible for performing BOP training as defined herein.
2. SACs shall be responsible for tracking contractor protected area access.

5.13.2 Training

1. Site Nuclear Training shall provide training to all workers granted UA:
 - a. On the detection of illegal drug use, alcohol/legal drug abuse, and other behavior that may constitute an unreasonable risk to the health and safety of the public, including a potential threat to commit radiological sabotage.
 - b. Providing reasonable awareness and sensitivity to detect degradation in performance which may be the result of being under the influence of any substance, legal or illegal, physical or mental impairment which in any way may adversely affect their ability to safely and competently perform their duties, with an expectation of promptly reporting noticeable changes in behavior to NMC management for appropriate evaluation and action.
 - c. On techniques for recognizing behaviors adverse to the safe operation and security of the facility.
 - d. On the responsibility to report arrests, charges, or convictions.
 - e. On manager/supervisor responsibilities for acting on behavior that may reflect adversely on trustworthiness, reliability or safe operation and security of the facility.
2. Individuals granted unescorted access authorization shall have an NMC supervisor trained in accordance with Section 5.13.2 (1).
 - a. This training shall be completed on a frequency as defined by fleet/site training procedures.

**Access Authorization Program
FP-S-AA-01, Revision 6**

- b. For offsite personnel supervising off-site licensee employees with unescorted access to NMC's nuclear plants:
 - 1) The SAC/SAS shall conduct a monthly audit to ensure training is completed at frequencies defined in site implementing procedures.
 - 2) For supervisors not granted UA, the SAC/SAS obtain monthly verification of behavior observation program coverage through distribution and receipt of NMC Form QF-1707, *Cognizant Supervisor BOP Review*.
 - 3) The SAAL shall quarterly review the monthly audit to assure personnel are trained at frequencies defined in Section 5.13.2 (2) (a).

- c. For supervisors whose training has expired, the SAAL shall:
 - 1) Suspend the access of workers reporting to the affected supervisor, or
 - 2) Reassign the workers reporting to affected supervisor to a supervisor whose training is current.

- d. Supervisors are responsible for designation of an appropriately trained replacement (FFD supervisory trained) when unable to fulfill behavior observation program responsibilities due to temporary assignment or leave of absence of greater than 30 days.

5.13.3 Contractor Protected Area Access

- 1. SACs shall:
 - a. Suspend UA for all contractors not accessing the protected area and outside a behavior observation program for periods greater than 30 days.

5.13.4 Licensee Employee Protected Area Access

- 1. NMC supervisors shall notify the SAC when it is anticipated that a licensee employee, badged for nuclear plant access, is expected to be outside the CBOP for greater than 30 days.

2. SACs shall:
 - a. Suspend UA.

5.13.5 Criminal History Reporting

1. Workers badged for unescorted access authorization shall provide written report to their NMC Supervisor any arrest, charge or conviction on Form QF-1703, Report of Arrest, Charge or Conviction. This includes all arrests, charges or convictions related to operation of motor vehicles with the exception of minor traffic violations such as speeding or parking tickets. Reports should be made as soon as possible but no later than prior to a worker's next work period.
2. Workers granted UAA shall be informed in writing of the requirement to report arrests, charges or convictions in Plant Access Training and when completing an NMC personal history questionnaire (Forms QF-0350-0353).
3. Supervisors shall forward Form QF-1703 to the SAAL.
4. SAAL shall complete the applicable Sections of Form QF-1703 and provide a copy to the individual making the report, obtaining written verification of receipt.
5. The SAAL shall consult with the MRO to determine whether a mandatory EAP assessment is required for any arrest, charge, or conviction related to drugs, alcohol, theft or violence. As recommended by the MRO, SAAL shall coordinate through the responsible NMC supervisor, a mandatory EAP assessment.

5.14 APPROVED CONTRACTOR UAA PROGRAMS

5.14.1 Responsibilities

1. NMC Security shall be responsible for reviewing contractor requests for UAA certification.
2. The Fleet AA/FFD Approved Contractor Lead (ACL) shall be responsible for:
 - a. Evaluating contractor UAA programs for initial program approval status.

**Access Authorization Program
FP-S-AA-01, Revision 6**

- b. Evaluating NMC Supplier Q.A./NEI audit reports of contractor UAA Programs, to include findings, recommendations and corrective actions, for effective implementation and compliance with regulatory requirements.
 - c. Reviewing audit reports for reportability.
 - d. Evaluating changes to FP-S-AA-01 to determine whether changes to approved contractor programs are required. If changes are required, prior to implementation of FP-S-AA-01 changes, review approved contractor programs to determine whether their program is eligible for continued approval status and update letter of agreement (if revised).
3. Site SAALs may perform the responsibilities of the ACL in the ACL's absence.

5.14.2 General

- 1. Approved contractor UAA programs for each site shall be identified on NMC Security Table QF-0379, *NMC Approved Contractor UAA Programs*.

5.14.3 Review Process

- 1. The ACL shall evaluate the contractor's UAA Program to ensure compliance with applicable 10 CFR 73.56, NRC Regulatory Guide 5.66, and NRC Access Authorization Order (dated 7 January 2003) requirements. This evaluation shall minimally include a review of:
 - a. Contractor policies and procedures.
 - b. Most recent licensee or NEI audit (if completed within the last 5 years).
 - c. Interview program administration personnel and review of collection facilities (unless other licensee or NEI audit within the last year is available).
- 2. The ACL shall communicate UAA program evaluation results to contractors.

**Access Authorization Program
FP-S-AA-01, Revision 6**

- a. If the evaluation results are satisfactory, proceed to Section 5.14.5.
- b. If the evaluation results indicate deficient areas, proceed to Section 5.14.4.

5.14.4 Program Deficiencies

1. The ACL shall draft and send a letter to the contractor:
 - a. Identifying UAA program deficiencies.
 - b. Requiring the contractor to submit revised procedures addressing the programmatic deficiencies to NMC Security
2. The revised procedures shall be evaluated in accordance with Sections 5.14.3 (1-2).

5.14.5 Program Approval

1. Contractors shall be notified of their UAA Program approval status through execution of NMC Security Form QF-0359, *Contractor UAA Program Approval Notice*.
2. The ACL shall notify NMC Supplier Quality Assurance of the Contractor FFD Program approval with NMC Security Form QF-0316, *Approved AA/FFD Program; Audit Review Checklist*.
3. Approved contractors shall provide the ACL a letter identifying by full printed name and signature the personnel authorized to submit contractor UAA Request Forms.

5.14.6 UAA Certification Elements

1. Contractors shall provide:
 - a. Documented completion of applicable 10 CFR Part 73.56, Regulatory Guide 5.66 and NRC Access Authorization Order (dated 7 January 2003) requirements on *NEI's Contractor Access Request Form* or comparable (see NMC Attachment 2).
 - b. Any derogatory information disclosed by the individual or developed during the background investigation subsequent to last licensee unescorted access.

2. Prior to granting UAA, NMC Security shall review the Contractor Access Request Form to verify the individual minimally meets NMC requirements for granting UAA as defined in Sections 5.3 through 5.6.

5.14.7 Audits

1. Approved contractors shall be required to conduct audits on a nominal annual basis of their programs to assure compliance with applicable 10 CFR Parts 26 and 73.56, Regulatory Guide 5.66 and NRC Access Authorization Order (dated 7 January 2003) requirements.
2. NMC shall conduct audits on a nominal annual basis of approved contractor programs to assure compliance with applicable 10 CFR 26, 73.56 and NRC Access Authorization Order (dated 7 January 2003) requirements.
 - a. Supplier Quality Assurance or NEI audits of contractor UAA programs shall be used to satisfy the licensee nominal annual NRC contractor audit requirement.
 - b. A member of the audit team should be a person knowledgeable and practiced in access authorization to validate that overall program performance is meeting the objective of screening individuals to provide to provide reasonable assurance that there are no security deficiencies that might allow other than trustworthy and reliable people into the plant.
3. The ACL shall:
 - a. Review audits reports, to include findings, recommendations, and corrective actions, to determine whether contractors are effectively implementing and complying with regulatory requirements. This review shall be documented on NMC Security Form QF-0316.
 - b. Forward to NMC Supplier Quality Assurance completed NMC Security Form QF-0316.
 - c. If the audit of a contractor UAA program contains findings or other significant deficiencies, the ACL shall review the information to determine reporting requirements in accordance with Section 5.16.

- d. If the review indicates the findings shall be reported or logged, the ACL shall:
 - 1) Immediately notify the SAAL for the respective nuclear site. If the finding or concern involves an individual and the individual currently has unescorted access, the unescorted access shall be suspended pending resolution of the finding.
 - 2) Change the individual's Access Authorization status to "Incomplete" until the findings are resolved.

NOTE: This is also required for individuals who do not currently have unescorted access.

- 3) Complete the applicable site event reporting form.

5.15 AUDITS

5.15.1 Responsibilities

- 1. The NMC Nuclear Oversight shall conduct an independent audit of UAA requirements defined herein and their conformance to applicable Regulatory Guide 5.66, 10 CFR 73.56 and NRC Access Authorization Order (dated 7 January 2003), within 12-months (not to exceed 365 days) of the implementation date of Revision 3 to this procedure and at least once every 24 months thereafter on a nominal biennial basis.
 - a. A member of the audit team shall meet the requirements of Section 5.14.7.2.b.
- 2. Agencies contracted to provide UAA services (e.g., background investigations, psychological evaluations) shall be required to retain records for five-year record retention audits. UAA agencies not previously used in the nuclear industry shall require a pre-award audit.
- 3. Duly-authorized NMC and/or NRC representatives may inspect, copy, or take away copies of any NMC or contractor/vendor audit records.

5.16 REPORTING OF UAA SAFEGUARDS EVENTS

5.16.1 Responsibilities

1. The SAAL shall be responsible for evaluating access authorization events for reportability.
2. NMC Security Section members shall be responsible for reviewing access authorization events with the SAAL.
3. In the SAAL's absence, the SAS shall assume the responsibilities for the SAAL as defined herein.

5.16.2 General

1. 10 CFR 26.27 Suitable Inquiry requirements referenced herein shall be considered elements reportable in accordance with this procedure.
2. Appropriate compensatory measures following identification of an event requiring reporting herein shall include the timely change of access authorization and removal of unescorted access.

5.16.3 Loggable Event

1. The following events shall be logged within 24 hours from discovery:
 - a. Incomplete access authorization records, as defined in Section 5.16.5.
 - b. Subsequent access authorization denials based on personal deception (e.g., individuals gaining unescorted access by deliberately falsifying their own background screening information).
 - c. Inadequate administration, control or evaluation of psychological tests.

5.16.4 Reportable Events

1. The following events shall be reported to the NRC within 1 hour from discovery:
 - a. Subsequent denial of access authorization following completion of incomplete access authorization record.
 - b. Subsequent denial of a properly authorized access authorization for which proper compensatory measures were not taken.

- c. Subsequent denial of access authorization based on personal deception and evidence that the individual performed acts in an attempt to commit or cause events identified in 10 CFR Part 73, Appendix G (l)(a)&(d).

5.16.5 Incomplete Access Authorization Records

1. UAA records shall be considered incomplete if the intent of any required element, as defined in the applicable access authorization procedure, has not been met (including falsification by personnel performing background investigations).
2. Incomplete access authorization records may be discovered through:
 - a. Audits/surveillance of NMC's Access Authorization Program.
 - b. Audits/surveillance of NMC approved Contractor Access Authorization Programs.
 - c. Internal NMC Security Section review of access authorization records.
3. Upon discovery of incomplete access authorization records for individuals with current unescorted access:
 - a. NMC Security Section members shall:
 - 1) Inform the SAAL.
 - 2) Document the discovery on Form QF-0365, *Memo to File*.
 - b. The SAAL/designee shall:
 - 1) Change the individual's BFA in PIPS to ADMIN DATA".
 - 2) Contact the respective Security Manager to suspend the individual's unescorted access.
 - 3) Document and communicate the Loggable event in accordance with Section 5.16.6.

**Access Authorization Program
FP-S-AA-01, Revision 6**

- c. NMC Security Section members shall complete and/or investigate the incomplete element in accordance with the applicable Sections herein.
- 4. Upon discovery of incomplete access authorization records for individuals that currently do not hold unescorted access:
 - a. NMC Security Section members shall:
 - 1) Inform the SAAL.
 - 2) Document the discovery on Form QF-0365, *Memo to File*.
 - 3) Change the individual's BFA in PIPS to "ADMIN DATA".
 - b. The SAAL/designee shall document and communicate the Loggable event in accordance with Section 5.16.6.
 - c. NMC Security Section members shall complete and/or investigate the incomplete element, in accordance with the applicable Sections herein.
- 5. If upon completion of the incomplete element the individual is denied access authorization, the SAAL/Designee shall immediately document and communicate the reportable event in accordance with Section 5.16.6.

5.16.6 Documenting and Communicating UAA Safeguards Events

- 1. UAA events shall be documented and communicated in accordance with applicable site procedures and recorded on NMC Table QF-0380, *Access Authorization Event Log*.
- 2. The UAA Event Log shall minimally include:
 - a. Event date
 - b. Log/Report number
 - c. Plant
 - d. Responsible access authorization group
 - e. Findings (program requirements not met)

- f. Date Event Closeout
 - g. Final disposition
3. The Industry Shared Database system shall be updated for any access authorization events associated with individuals on the Industry Shared Database system in accordance with the Industry Shared Database Standards and Procedures Manual.

6.0 REQUIRED RECORDS

6.1 RECORD PROTECTION & RETENTION

6.1.1 Responsibilities

- 1. SAALs *shall* be responsible for approving requests for the release of personal information.
- 2. NMC Security Section members shall be responsible for:
 - a. The protection of personal and confidential information collected in support of the access authorization process.
 - b. Retaining records as required by this procedure.

6.1.2 General

- 1. Information obtained through background investigations, suitable inquiries, and psychological evaluations shall be protected and maintained in a confidential manner. This information shall not be released without written consent from the individual, except as identified in 6.1.3.1.

6.1.3 Protection of Information

- 1. Personal information collected during the access authorization process shall not be disclosed to persons other than:
 - a. The subject individual or their official representative who has been identified in writing..
 - b. NMC Quality Oversight personnel or contractors working under contract with NMC for the purpose of program audits and/or surveillance.
 - c. NMC personnel having a need to know in performing assigned duties related to NMC AA Program.

- d. Individuals deciding matters on review or appeal.
 - e. Other licensees, contractors, or vendors legitimately seeking the information for the determination of access authorization.
 - f. NRC representatives.
 - g. Law Enforcement officials under court order.
 - h. NMC Medical Review Officers.
 - i. Other persons pursuant to court order.
2. SAALs shall approve all additions to the list of individuals granted access to the UAA records storage areas.
 3. Access to PIPS and Industry Shared Database stored information shall be controlled by:
 - a. Password protection.
 - b. Data entry limited to authorized individual's area of competency.
 - c. Access to PIPS shall be approved by the SAAL on NMC Form QF-1706, *PIPS Access Approval Form*.
 - d. Quarterly review by SAAL to verify continued user need to know.

6.1.4 Release of Personal Information

1. Requests for release of personal information from individuals defined in Section 6.1.3 (1) (a & e) shall be processed by NMC Security Section members as follows:
 - a. Requests received telephonically:
 - 1) Inform the caller that the information can only be released with a signed, written release from the individual, and
 - 2) The release shall be specific and address which areas or information is required, and its intended use.
 - b. Requests received via mail or fax:

**Access Authorization Program
FP-S-AA-01, Revision 6**

- 1) Verify the personal identification data contained in the release form with identification data in the individual's security dossier.
 - 2) Process the request in accordance with Form QF-0318, *Request for Release of Personal Information*.
- c. Requests made in person:
- 1) Verify the personal identification data contained in the release form with identification data in the security dossier.
 - 2) Verify the identity of the requestor through photo identification.
 - 3) Process the request in accordance with Form QF-0318.
2. If during the verification process it is determined that the request is questionable or not legitimate, NMC Security shall advise the SAAL.

6.1.5 Physical Protection of Information

1. All documents in the security dossier shall be secured to the folder with metal fasteners to preclude loss of individual pages.
2. Security dossiers and documents related to the access authorization program shall, when not under the direct control of NMC Security, be secured in the department's record storage area.
3. During the workday, NMC Security may lock security dossiers and confidential information in their desks, while at lunch or during breaks.

6.1.6 Record Retention Requirements

1. Notes, memorandums, and miscellaneous correspondence collected during the investigative process shall be maintained in its original form, and filed in the security dossier as specified in Section 6.1.5 (1).
2. Security dossiers and miscellaneous documents used to support access authorization for an individual shall be

maintained for a period of five years from the date in which the individual's unescorted access is terminated.

3. Security dossiers and documents used to support denial of an individual's access authorization shall be maintained for five years from the date of final denial action.
4. In addition to the aforementioned retention requirements, security dossiers and documents for an individual on the Industry Shared Database system shall be maintained for a period of five years inactivity on Industry Shared database.

7.0 REFERENCES

- 7.1 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage"
- 7.2 10 CFR 73.56, "Access Authorization Program for Nuclear Power Plants"
- 7.3 Regulatory Guide 5.66, "Access Authorization Program for Nuclear Power Plants"
- 7.4 NEI 94-02, Standardized Industry Audit Process for Licensee - Approved Contractor/Vendor Access Authorization and Fitness For Duty Programs
- 7.5 NEI 95-03, Personnel Access Data System Health Physics Standards and Procedures
- 7.6 NEI 95-04, Guideline for General Access Training
- 7.7 NEI 95-05, Industry Shared Database Operating Manual
- 7.8 10 CFR 73.57, "Requirements for Criminal History Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility or Access to Safeguards Information by Power Reactor Licensees"
- 7.9 10 CFR 26, "Fitness For Duty Program"
- 7.10 NUMARC 89-01, "Industry Guidelines for Nuclear Power Plant Access Authorization Programs"
- 7.11 NUMARC 91-03, "Nuclear Power Plant Personnel Access Authorization Data Exchange Guidelines"
- 7.12 NEI 95-06, Electronic System Technical Information Manual
- 7.13 NRC Generic Letter 91-03, Reporting of Safeguards Events

- 7.14 NRC Regulatory Guide 5.62, Reporting of Safeguards Events
- 7.15 NEI-03-01, Nuclear Power Plant Access Authorization Program
- 7.16 NRC Order for Compensatory Measures Related to Access Authorization dated January 7, 2003
- 7.17 Point Beach significant finding detailed in CAP 028386 requires maintenance of language in Section 5.1.5 to prevent finding recurrence.

8.0 ATTACHMENTS

- 8.1 Attachment 1 NMC AA Forms and Tables
- 8.2 Attachment 2 NEI's Contractor Access Request Form
- 8.3 Attachment 3 Personal Information and I.D. Needed for Initial UA...
- 8.4 Attachment 4 SF180, Request Pertaining to Military Records
- 8.5 Attachment 5 Safeguards Provisions

9.0 REVISION SUMMARY

Section	Change
5.1.1.1.c.	Added requirement that access reviewer must hold UA.
5.2.2.11.	Added specific guidance on how to indicate in PIPS additional information on PADS SEC5.
5.11.5.2.b.	Changed requirement for denial approval to Site Director (or equivalent as designated by Site VP).
5.11.5.2.c.	(Items 2 & 4) Clarified the means for effecting an additional information designation in PADS.
5.13.2.2.b.	Added requirements for monthly review of offsite supervisors, not granted UA; to verify behavior observation program coverage.
6.1.3.3.	Added SAAL requirements to complete Form QF-1706 prior to granting PIPS access and quarterly review PIPS and PADS users to verify continued need to know.

**Access Authorization Program
FP-S-AA-01, Revision 6**

**Attachment 1
NMC AA Forms and Tables**

Type	#	Title
Form	<u>QF-0316</u>	<i>Approved AA/FFD Program; Audit Review Checklist</i>
Form	<u>QF-0318</u>	<i>Request for Release of Personal Information</i>
Form	<u>QF-0319</u>	<i>Reinvestigation PHQ</i>
Form	<u>QF-0320</u>	<i>Contractor Access Denial Notification Form</i>
Form	<u>QF-0334</u>	<i>NMC UAA Active Case Log</i>
Form	<u>QF-0350</u>	<i>NMC Initial Personal History Questionnaire (PHQ)</i>
Form	<u>QF-0351</u>	<i>NMC Update PHQ</i>
Form	<u>QF-0352</u>	<i>NMC Reinstatement PHQ – 31-365</i>
Form	<u>QF-0353</u>	<i>NMC Reinstatement PHQ < 30</i>
Form	<u>QF-0354</u>	<i>Authorization for Release of Information to NMC</i>
Form	<u>QF-0355</u>	<i>NMC Contractor Access Authorization Procedure</i>
Form	QF-0356	<i>Deleted</i>
Form	QF-0357	<i>Deleted</i>
Form	<u>QF-0358</u>	<i>Access Authorization Adjudication Checklist</i>
Form	<u>QF-0359</u>	<i>Contractor UAA Program Approval Notice</i>
Form	<u>QF-0360</u>	<i>Approved Contractor Authorized Signature List</i>
Form	QF-0361	<i>Deleted</i>
Form	<u>QF-0362</u>	<i>Psychological Test Information</i>
Form	<u>QF-0363</u>	<i>Psychological Release</i>
Form	<u>QF-0364</u>	<i>NMC Approved Contractor UAA BOP Requirements</i>
Form	<u>QF-0365</u>	<i>Memo to File</i>
Form	QF-0366	<i>Deleted</i>
Form	<u>QF-0367</u>	<i>Request for Review of UAA Denial Based on Background Investigation</i>
Form	<u>QF-0368</u>	<i>Notice of UAA Denial Based on Background Investigation</i>
Form	<u>QF-0369</u>	<i>Request for Review of UAA Denial Based on Background Investigation Disposition- Upheld</i>

**Access Authorization Program
FP-S-AA-01, Revision 6**

Type	#	Title
Form	<u>QF-0370</u>	<i>Request for Review of UAA Denial Based on Background Investigation Disposition- Reversed</i>
Form	<u>QF-0371</u>	<i>Access Authorization Denial Based Upon Psychological Evaluation</i>
Form	<u>QF-0372</u>	<i>Request for Review of UAA Denial Based on Psychological Evaluation Disposition- Upheld</i>
Form	<u>QF-0373</u>	<i>Request for Review of UAA Denial Based on Psychological Evaluation Disposition - Reversed</i>
Form	QF-0374	<i>Deleted</i>
Form	<u>QF-0375</u>	<i>Palisades Access Termination Form.</i>
Table	<u>QF-0376</u>	<i>NMC Badging Matrix</i>
Table	QF-0377	<i>Deleted</i>
Table	<u>QF-0378</u>	<i>Denied UAA Reconsideration</i>
Table	<u>QF-0379</u>	<i>NMC Approved Contractor UAA Programs</i>
Table	<u>QF-0380</u>	<i>Access Authorization Event Log</i>
Table	<u>QF-0381</u>	<i>NMC Access Review List</i>
Table	<u>QF-0382</u>	<i>Initiating UA Requests at NMC Sites</i>
Table	<u>QF-0383</u>	<i>Site Access Termination Forms</i>
Table	<u>QF-0384</u>	<i>Site Security AA/FFD Points of Contact</i>
Table	QF-0385	<i>Deleted</i>
Form	<u>QF-0388</u>	<i>UA Status Change Actions/Notifications</i>
Form	<u>QF-0389</u>	<i>Administrative Hold Checklist</i>
Form	<u>QF-0390</u>	<i>Alternative Means for Verifying Military History</i>
Form	<u>QF-0391</u>	<i>Enhanced Oversight Instruction</i>
Form	QF-1702	<i>NRC Unescorted Access Authorization Checklist</i>
Form	QF-1703	<i>Report of Arrest, Charge or Conviction</i>
Form	QF-1704	<i>NMC Reinstatement/Reinvestigation Questionnaire - >30 & < 365 Days</i>
Form	QF-1705	<i>NMC Reinstatement/Reinvestigation Questionnaire - <30 Days</i>
Form	QF-1706	<i>PIPS Access Approval Form</i>
Form	QF-1707	<i>Cognizant Supervisor BOP Review</i>

**Access Authorization Program
FP-S-AA-01, Revision 6**

**Attachment 2
NEI's Contractor Access Request Form
NEI Unescorted Access Authorization Request Form**

TO: (Company Name) (Utility Site Name) Arrival Date:
(Address) Site Where Access is Requested:
(FAX Number) (E-mail address)

REQUESTING COMPANY: Address:

It is requested that the individual named below be granted unescorted access. The individual named herein has been screened in accordance with the requirements of 10CFR73.56 and NRC Regulatory Guide 5.66; and has been determined to meet the suitability requirements for trustworthiness and reliability.

IDENTIFICATION & EMPLOYMENT STATUS

Name: (Last, First, Middle)		SSAN or Identification Number:	Date of Birth:
<input checked="" type="checkbox"/>	Mark Either 1 or 2 as appropriate		
<input type="checkbox"/>	1. Current Employee of Requesting Company	Hire Date: (Only for Requesting Company)	
<input type="checkbox"/>	2. Employee of Company other than Requesting Company	Company Name:	Assignment Date to Requesting Company:

TYPE OF SCREENING (Mark One Selection, As Applicable)

TYPE	<input checked="" type="checkbox"/>	Instructions	TYPE	<input checked="" type="checkbox"/>	Instructions
Temporary	<input type="checkbox"/>	Complete Sections 1,2, and 3	Reinstatement/Transfer	<input type="checkbox"/>	Complete Sections 2 and 3
Full	<input type="checkbox"/>	Complete Sections 1,2, and 3	Update	<input type="checkbox"/>	Complete Sections 1,2, and 3

Section 1: BI Investigation, Evaluation Summary and Company Holding Records:

Element	Completion Date	Element	Completion Date
Background Investigation		Identity Verification	
Psychological Evaluation		FFD Test:	
NPRC Verification on File ?	YES N/A NO	If NO, Request Last Submitted:	Date:
If Company Holding Source Records Is Different Than Approved Contractor/Vendor, please specify:		Name:	Address:

Section 2: Fitness for Duty Program

Drug/Alcohol Test Date:	Conducted By: (Approved Contractor Vendor or Utility)
Suitable Inquiry	Date:
<input checked="" type="checkbox"/>	Mark Appropriate Certification
<input type="checkbox"/>	I certify that the individual has NOT been away from a licensee or approved contractor/vendor behavioral observation program for more than 30 consecutive days.
<input type="checkbox"/>	I certify that the continual behavior observation has been interrupted for a period exceeding 30 consecutive days. The individual's activities during the interruption have been evaluated and they do NOT affect the individual's trustworthiness and reliability.
<input type="checkbox"/>	I certify that the continual behavior observation has been interrupted for a period exceeding 30 consecutive days. The individual's activities during the interruption have NOT been evaluated.

Section 3: Access Authorization History

Utility Where Unescorted Access Last Held:					
Access Terminated Favorably?	YES	NO	UNK	Access Terminated:	Date:
Information Requiring Adjudication? IF YES, Please attach To This Form	YES	NO	PADS Transfer Consent Form Signed: Yes NO If Yes, Please attach to this form		

I understand that our company's must notify you when unescorted access is no longer required for this worker.

Printed Name:	Signature:
Title:	Date:

**Attachment 3
Personal Information and I.D. Needed for Initial Unescorted Access Authorization**

Unescorted Access Authorization Information

1. Employment for the past three years.
2. Military service dates and DD 214 showing type of discharge if in the service during the past three years.
3. Education in lieu of employment within the last five years (name, address and phone number of the school).
4. Residences (street, city, county and state) for the last five years.
5. Arrests/convictions (charges, disposition, dates, and location) for entire adult life.
6. Names, addresses, and daytime telephone numbers for four personal character references.

Drug Screening

1. All prescription drugs, non-prescription drugs, over-the-counter medications, or any other chemical substances taken within the last 30 days.
2. For prescribed drugs: prescribing physician, telephone number, and address.
3. Mailing address at which the person wants his drug and alcohol test results sent to him.
4. Work telephone number and home telephone number.

Identification

1. Driver's license or other valid picture identification.
2. Social Security number.

**Access Authorization Program
FP-S-AA-01, Revision 6**

**Attachment 4
SF180, Request Pertaining to Military Records**

Standard Form 180 (Rev. 3-99)
Prescribed by NARA (26 CFR 1228.142(g))

Authorized for local reproduction
Previous editions obsolete

OMB No. 3025-0022 Expires 7/31/2007

**REQUEST PERTAINING
TO MILITARY RECORDS**

To ensure the best possible service, please thoroughly review the instructions at the bottom before filling out this form. Please print clearly or type. If you need more space, use plain paper.

SECTION I - INFORMATION NEEDED TO LOCATE RECORDS (Furnish as much as possible.)

1. NAME USED DURING SERVICE (Last, first, middle)		2. SOCIAL SECURITY NO.		3. DATE OF BIRTH		4. PLACE OF BIRTH	
5. SERVICE, PAST AND PRESENT (For an effective records search, it is important that ALL service be shown below.)							
	BRANCH OF SERVICE	DATES OF SERVICE		CHECK ONE		SERVICE NUMBER DURING THIS PERIOD (If unknown, please write unknown)	
		DATE ENTERED	DATE RELEASED	OFFICER	ENLISTED		
a.	ACTIVE SERVICE						
b.	RESERVE SERVICE						
c.	NATIONAL GUARD						
6. IS THIS PERSON DECEASED? If "YES" enter the date of death. <input type="checkbox"/> NO <input type="checkbox"/> YES _____				7. IS (WAS) THIS PERSON RETIRED FROM MILITARY SERVICE? <input type="checkbox"/> YES <input type="checkbox"/> NO			

SECTION II - INFORMATION AND/OR DOCUMENTS REQUESTED

1. **REPORT OF SEPARATION** (DD Form 214 or equivalent) This contains information normally needed to verify military service. A copy may be sent to the veteran, the deceased veteran's next of kin, or other persons or organizations if authorized in Section III, below. NOTE: If more than one period of service was performed, even in the same branch, there may be more than one Report of Separation. Be sure to show EACH year that a Report of Separation was issued, for which you need a copy.

An UNDELETED Report of Separation is requested for the year(s) _____

This normally will be a copy of the full separation document including such sensitive items as the character of separation, authority for separation, reason for separation, reenlistment eligibility code, separation (SPD/SPN) code, and dates of time lost. An undeleted version is ordinarily required to determine eligibility for benefits.

A DELETED Report of Separation is requested for the year(s) _____

The following information will be deleted from the copy sent: authority for separation, reason for separation, reenlistment eligibility code, separation (SPD/SPN) code, and for separations after June 30, 1979, character of separation and dates of time lost.

2. **OTHER INFORMATION AND/OR DOCUMENTS REQUESTED** _____

3. **PURPOSE (OPTIONAL)**—An explanation of the purpose of the request is strictly voluntary. Such information may help the agency answering this request to provide the best possible response and will in no way be used to make a decision to deny the request.) _____

SECTION III - RETURN ADDRESS AND SIGNATURE

1. **REQUESTER IS**

Military service member or veteran identified in Section I, above

Legal guardian (must submit copy of court appointment)

Next of kin of deceased veteran. _____
(relation)

Other (specify) _____

2. **SEND INFORMATION/DOCUMENTS TO**
(Please print or type. See instruction J, below.)

3. **AUTHORIZATION SIGNATURE REQUIRED** (See instruction 2, below.)
I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the information in this Section III is true and correct.

Name _____
Street _____
City _____

Signature of requester (Please do not print) _____
Date of this request _____ Daytime phone () _____
E-mail address _____

Attachment 5

**THIS ATTACHMENT IS CLASSIFIED AS
SAFEGUARDS INFORMATION AND IS
STORED SEPARATE FROM THIS PROCEDURE**