

§ 25.13

to grant an exemption. If this condition is relied on exclusively for satisfying paragraph (b) of this section, the exemption may not be granted until the Executive Director for Operations has consulted with the Commission.

[64 FR 15647, Apr. 1, 1999]

§ 25.13 Maintenance of records.

(a) Each licensee or organization employing individuals approved for personnel security access authorization under this part, shall maintain records as prescribed within the part. These records are subject to review and inspection by CSA representatives during security reviews.

(b) Each record required by this part must be legible throughout the retention period specified by each Commission regulation. The record may be the original or a reproduced copy or a microform provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period. The record may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period. Records such as letters, drawings, specifications, must include all pertinent information such as stamps, initials, and signatures. The licensee shall maintain adequate safeguards against tampering with and loss of records.

[45 FR 14481, Mar. 5, 1980, as amended at 53 FR 19245, May 27, 1988; 62 FR 17687, Apr. 11, 1997]

ACCESS AUTHORIZATIONS

§ 25.15 Access permitted under “Q” or “L” access authorization.

(a) A “Q” access authorization permits an individual access on a need-to-know basis to (1) Secret and Confidential Restricted Data and (2) Secret and Confidential National Security Information including intelligence information, CRYPTO (i.e., cryptographic information) or other classified communications security (COMSEC) information.

(b) An “L” access authorization permits an individual access on a need-to-know basis to Confidential Restricted

10 CFR Ch. I (1–1–06 Edition)

Data and Secret and Confidential National Security Information other than the categories specifically included in paragraph (a) of this section. In addition, access to certain Confidential COMSEC information is permitted as authorized by a National Communications Security Committee waiver dated February 14, 1985.

(c) Each employee of the Commission is processed for one of the two levels of access authorization. Licensees and other persons will furnish National Security Information and/or Restricted Data to a Commission employee on official business when the employee has the appropriate level of NRC access authorization and need-to-know. Some individuals are permitted to begin NRC employment without an access authorization. However, no NRC employee shall be permitted access to any classified information until the appropriate level of access authorization has been granted to that employee by NRC.

[45 FR 14481, Mar. 5, 1980, as amended at 47 FR 9195, Mar. 4, 1982; 50 FR 36984, Sept. 11, 1985]

§ 25.17 Approval for processing applicants for access authorization.

(a) Access authorizations must be requested for licensee employees or other persons (e.g., 10 CFR part 2, subpart I) who need access to classified information in connection with activities under 10 CFR parts 50, 52, 54, 60, 63, 70, 72, or 76.

(b) The request must be submitted to the facility CSA. If the NRC is the CSA, the procedures in § 25.17 (c) and (d) will be followed. If the NRC is not the CSA, the request will be submitted to the CSA in accordance with procedures established by the CSA. The NRC will be notified of the request by a letter that includes the name, Social Security number and level of access authorization.

(c) The request must include a completed personnel security packet (see § 25.17(d)) and request form (NRC Form 237) signed by a licensee, licensee contractor official, or other authorized person.

(d)(1) Each personnel security packet submitted must include the following completed forms:

Nuclear Regulatory Commission

§ 25.21

(i) Questionnaire for National Security Positions (SF-86, Parts 1 and 2) (Part 2 is to be completed by the applicant and placed in a sealed envelope which is to be forwarded to NRC unopened. No licensee, licensee contractor official, or other person at a facility is permitted to review Part 2 information);

(ii) Two standard fingerprint cards (FD-258);

(iii) Security Acknowledgment (NRC Form 176); and

(iv) Other related forms where specified in accompanying instructions (NRC Form 254).

(2) Only a Security Acknowledgment (NRC Form 176) need be completed by any person possessing an active access authorization, or who is being processed for an access authorization, by another Federal agency. The active or pending access authorization must be at an equivalent level to that required by the NRC and be based on an adequate investigation of not more than five years old.

(e) To avoid delays in processing requests for access authorizations, each security packet should be reviewed for completeness and correctness (including legibility of response on the forms) before submittal.

(f)(1) The Office of Personnel Management (OPM) bills NRC for the cost of each background investigation conducted in support of an application for access authorization. The combined cost of the OPM investigation and NRC's application processing overhead are recovered from the licensee through an authorization fee calculated with reference to current OPM personnel investigation billing rates {OPM rate + [(OPM rate × 11.6%), rounded to the nearest dollar] = NRC access authorization fee}. Updated OPM billing rates are published periodically in a Federal Investigations Notice (FIN) issued by OPM's Investigations Service. Copies of the current OPM billing schedule can be obtained by phoning the NRC's Security Branch, Division of Facilities and Security, Office of Administration at 1-800-368-5642. Any change in the NRC's access authorization fees will be applicable to each access authorization request received on or after the effective date of

OPM's most recently published investigations billing schedule.

(2) Applications for access authorization or access authorization renewal processing that are submitted to the NRC for processing must be accompanied by a check or money order, payable to the United States Nuclear Regulatory Commission, representing the current cost for the processing of each "Q" and "L" access authorization, or renewal request. Applicants shall calculate the access authorization fee according to the stated formula {OPM rate + [(OPM rate × 11.6%), rounded to the nearest dollar] = NRC access authorization fee} and with reference to the table in Appendix A to this part.

(3) Certain applications from individuals having current Federal access authorizations may be processed more expeditiously and at less cost, since the Commission, at its discretion, may decide to accept the certification of access authorization and investigative data from other Federal Government agencies that grant personnel access authorizations.

[62 FR 17687, Apr. 11, 1997, as amended at 68 FR 62512, Nov. 5, 2003; 70 FR 32227, June 2, 2005]

§ 25.19 Processing applications.

Each application for an access authorization or access authorization renewal must be submitted to the CSA. If the NRC is the CSA, the application and its accompanying fee must be submitted to the NRC Division of Facilities and Security. If necessary, the NRC Division of Facilities and Security may obtain approval from the appropriate Commission office exercising licensing or regulatory authority before processing the access authorization or access authorization renewal request. If the applicant is disapproved for processing, the NRC Division of Facilities and Security shall notify the submitter in writing and return the original application (security packet) and its accompanying fee.

[64 FR 15648, Apr. 1, 1999]

§ 25.21 Determination of initial and continued eligibility for access authorization.

(a) Following receipt by the CSA of the reports of the personnel security

§ 25.23

10 CFR Ch. I (1–1–06 Edition)

investigations, the record will be reviewed to determine that granting an access authorization or renewal of access authorization will not endanger the common defense and security and is clearly consistent with the national interest. If this determination is made, access authorization will be granted or renewed. If the NRC is the CSA, questions as to initial or continued eligibility will be determined in accordance with part 10 of chapter I. If another agency is the CSA, that agency will, under the requirements of the NISPOM, have established procedures at the facility to resolve questions as to initial or continued eligibility for access authorization. These questions will be determined in accordance with established CSA procedures already in effect for the facility.

(b) The CSA must be promptly notified of developments that bear on continued eligibility for access authorization throughout the period for which the authorization is active (e.g., persons who marry subsequent to the completion of a personnel security packet must report this change by submitting a completed NRC Form 354, "Data Report on Spouse" or equivalent CSA form).

(c)(1) Except as provided in paragraph (c)(2) of this section, an NRC "Q" access authorization must be renewed every five years from the date of issuance. Except as provided in paragraph (c)(2) of this section, an NRC "L" access authorization must be renewed every ten years from the date of issuance. An application for renewal must be submitted at least 120 days before the expiration of the five-year period for a "Q" access authorization and the ten-year period for an "L" access authorization, and must include:

(i) A statement by the licensee or other person that the individual continues to require access to classified National Security Information or Restricted Data; and

(ii) A personnel security packet as described in § 25.17(d).

(2) Renewal applications and the required paperwork are not required for individuals who have a current and active access authorization from another Federal agency and who are subject to a reinvestigation program by that

agency that is determined by the NRC to meet the NRC's requirements. (The DOE Reinvestigation Program has been determined to meet the NRC's requirements.) For these individuals, the submission of the SF-86 by the licensee or other person to the other Government agency pursuant to their reinvestigation requirements will satisfy the NRC's renewal submission and paperwork requirements, even if less than five years have passed since the date of issuance or renewal of the NRC "Q" access authorization, or if less than 10 years have passed since the date of issuance or renewal of the NRC "L" access authorization. Any NRC access authorization continued in response to the provisions of this paragraph will, thereafter, not be due for renewal until the date set by the other Government agency for the next reinvestigation of the individual pursuant to the other agency's reinvestigation program. However, the period of time for the initial and each subsequent NRC "Q" renewal application to the NRC may not exceed seven years or, in the case of an NRC "L" renewal application, twelve years. Any individual who is subject to the reinvestigation program requirements of another Federal agency but, for administrative or other reasons, does not submit reinvestigation forms to that agency within seven years for a "Q" renewal or twelve years for an "L" renewal of the previous submission, shall submit a renewal application to the NRC using the forms prescribed in § 25.17(d) before the expiration of the seven-year period for a "Q" renewal or twelve-year period for an "L" renewal.

(3) If the NRC is not the CSA, reinvestigation program procedures and requirements will be set by the CSA.

[62 FR 17688, Apr. 11, 1997, as amended at 64 FR 15648, Apr. 1, 1999]

§ 25.23 Notification of grant of access authorization.

The determination to grant or renew access authorization will be furnished in writing to the licensee or organization that initiated the request. Upon receipt of the notification of original grant of access authorization, the licensee or organization shall obtain, as

a condition for grant of access authorization and access to classified information, an executed "Classified Information Nondisclosure Agreement" (SF-312) from the affected individual. The SF-312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial access authorization shall execute a SF-312 before being granted access to classified information. The licensee or other organization shall forward the executed SF-312 to the CSA for retention. If the employee refuses to execute the SF-312, the licensee or other organization shall deny the employee access to classified information and submit a report to the CSA. The SF-312 must be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date. The individual shall also be given a security orientation briefing in accordance with §95.33 of this chapter. Records of access authorization grant and renewal notification must be maintained by the licensee or other organization for three years after the access authorization has been terminated by the CSA. This information may also be furnished to other representatives of the Commission, to licensees, contractors, or other Federal agencies. Notifications of access authorization will not be given in writing to the affected individual except:

(a) In those cases when the determination was made as a result of a Personnel Security Hearing or by a Personnel Security Review Panel ; or

(b) When the individual also is the official designated by the licensee or other organization to whom written NRC notifications are forwarded.

[62 FR 17688, Apr. 11, 1997, as amended at 64 FR 15648, Apr. 1, 1999]

§ 25.25 Cancellation of requests for access authorization.

When a request for an individual's access authorization or renewal of an access authorization is withdrawn or canceled, the requestor shall notify the CSA immediately by telephone so that the single scope background investigation, national agency check with law and credit investigation, or other personnel security action may be discon-

tinued. The requestor shall identify the full name and date of birth of the individual, the date of request, and the type of access authorization or access authorization renewal requested. The requestor shall confirm each telephone notification promptly in writing.

[64 FR 15648, Apr. 1, 1999]

§ 25.27 Reopening of cases in which requests for access authorizations are canceled.

(a) In conjunction with a new request for access authorization (NRC Form 237 or CSA equivalent) for individuals whose cases were previously canceled, new fingerprint cards (FD-257) in duplicate and a new Security Acknowledgment (NRC Form 176), or CSA equivalent, must be furnished to the CSA along with the request.

(b) Additionally, if 90 days or more have elapsed since the date of the last Questionnaire for National Security Positions (SF-86), or CSA equivalent, the individual must complete a personnel security packet (see §25.17(d)). The CSA, based on investigative or other needs, may require a complete personnel security packet in other cases as well. A fee, equal to the amount paid for an initial request, will be charged only if a new or updating investigation by the NRC is required.

[62 FR 17689, Apr. 11, 1997, as amended at 64 FR 15648, Apr. 1, 1999]

§ 25.29 Reinstatement of access authorization.

(a) An access authorization can be reinstated provided that:

(1) No more than 24 months has lapsed since the date of termination of the clearance;

(2) There has been no break in employment with the employer since the date of termination of the clearance;

(3) There is no known adverse information;

(4) The most recent investigation must not exceed 5 years (Top Secret, Q) or 10 years (Secret, L); and

(5) The most recent investigation must meet or exceed the scope of the investigation required for the level of access authorization that is to be reinstated or granted.

(b) An access authorization can be reinstated at the same, or lower, level by

§ 25.31

submission of a CSA-designated form to the CSA. The employee may not have access to classified information until receipt of written confirmation of reinstatement and an up-to-date personnel security packet will be furnished with the request for reinstatement of an access authorization. A new Security Acknowledgement will be obtained in all cases. Where personnel security packets are not required, a request for reinstatement must state the level of access authorization to be reinstated and the full name and date of birth of the individual to establish positive identification. A fee, equal to the amount paid for an initial request, will be charged only if a new or updating investigation by the NRC is required.

[62 FR 17689, Apr. 11, 1997]

§ 25.31 Extensions and transfers of access authorizations.

(a) The NRC Division of Facilities and Security may, on request, extend the authorization of an individual who possesses an access authorization in connection with a particular employer or activity to permit access to classified information in connection with an assignment with another employer or activity.

(b) The NRC Division of Facilities and Security may, on request, transfer an access authorization when an individual's access authorization under one employer or activity is terminated, simultaneously with the individual being granted an access authorization for another employer or activity.

(c) Requests for an extension or transfer of an access authorization must state the full name of the person, date of birth, and level of access authorization. The Director, Division of Facilities and Security, may require a new personnel security packet (see § 25.17(c)) to be completed by the applicant. A fee, equal to the amount paid for an initial request, will be charged only if a new or updating investigation by the NRC is required.

(d) The date of an extension or transfer of access authorization may not be used to determine when a request for renewal of access authorization is required. Access authorization renewal

10 CFR Ch. I (1-1-06 Edition)

requests must be timely submitted, in accordance with § 25.21(c).

[45 FR 14481, Mar. 5, 1980, as amended at 48 FR 24320, June 1, 1983; 57 FR 3721, Jan. 31, 1992; 62 FR 17689, Apr. 11, 1997; 64 FR 15648, Apr. 1, 1999]

§ 25.33 Termination of access authorizations.

(a) Access authorizations will be terminated when:

(1) An access authorization is no longer required;

(2) An individual is separated from the employment or the activity for which he or she obtained an access authorization for a period of 90 days or more; or

(3) An individual, pursuant to 10 CFR part 10 or other CSA-approved adjudicatory standards, is no longer eligible for an access authorization.

(b) A representative of the licensee or other organization that employs the individual whose access authorization will be terminated shall immediately notify the CSA when the circumstances noted in paragraph (a)(1) or (a)(2) of this section exist; inform the individual that his or her access authorization is being terminated, and the reason; and that he or she will be considered for reinstatement of an access authorization if he or she resumes work requiring the authorization.

(c) When an access authorization is to be terminated, a representative of the licensee or other organization shall conduct a security termination briefing of the individual involved, explain the Security Termination Statement (NRC Form 136 or CSA approved form) and have the individual complete the form. The representative shall promptly forward the original copy of the completed Security Termination Statement to CSA.

[62 FR 17689, Apr. 11, 1997, as amended at 64 FR 15649]

CLASSIFIED VISITS

§ 25.35 Classified visits.

(a) The number of classified visits must be held to a minimum. The licensee, certificate holder, or other facility shall determine that the visit is necessary and that the purpose of the visit cannot be achieved without access