this chapter but is subject to the regulations in this part who knowingly and consciously fails to provide the notice required as by § 21.21 shall be subject to a civil penalty equal to the amount provided by section 234 of the Atomic Energy Act of 1954, as amended.

(b) Any NRC licensee or applicant for a license (including an applicant for, or holder of, a permit), applicant for a design certification under part 52 of this chapter during the pendency of its application, applicant for a design certification after Commission adoption of a final design certification rule for that design, or applicant for or holder of a standard design approval under part 52 of this chapter subject to the regulations in this part who fails to provide the notice required by § 21.21, or otherwise fails to comply with the applicable requirements of this part shall be subject to a civil penalty as provided by Section 234 of the Atomic Energy Act of 1954, as amended.

(c) The dedicating entity, pursuant to § 21.21(c) of this part, is responsible for identifying and evaluating deviations, reporting defects and failures to comply for the dedicated item, and maintaining auditable records of the dedication process. NRC enforcement action can be taken for failure to identify and evaluate deviations, failure to report defects and failures to comply, or failure to maintain auditable records.

[60 FR 48374, Sept. 19, 1995, as amended at 72 FR 49488, Aug. 28, 2007]

§ 21.62 Criminal penalties.

(a) Section 223 of the Atomic Energy Act of 1954, as amended, provides for criminal sanctions for willful violation of, attempted violation of, or conspiracy to violate, any regulation issued under sections 161b, 161i, or 161o of the Act. For purposes of section 223, all the regulations in part 21 are issued under one or more of sections 161b, 161i, or 161o, except for the sections listed in paragraph (b) of this section.

(b) The regulations in part 21 that are not issued under sections 161b, 161i, or 161o for the purposes of section 223 are as follows: §§ 21.1, 21.2, 21.3, 21.4 21.5, 21.7, 21.8, 21.61, and 21.62.

[57 FR 55071, Nov. 24, 1992]

PART 25—ACCESS AUTHORIZATION

GENERAL PROVISIONS

ACCESS AUTHORIZATIONS

CLASSIFIED VISITS

VIOLATIONS

AUTHORITY: Atomic Energy Act of 1954, secs. 145, 161, 223, 234 (42 U.S.C. 2165, 2201, 2273, 2282); Energy Reorganization Act of 1974, sec. 201 (42 U.S.C. 5841); 44 U.S.C. 3504 note; E.O. 10865, 25 FR 1583, as amended, 3 CFR, 1959–1963 Comp., p. 398; E.O. 12829, 58 FR 3479, 3 CFR, 1993 Comp., p. 570; E.O. 13526, 75 FR 707, 3 CFR, 2009 Comp., p. 298; E.O. 12968, 60 FR 40245, 3 CFR, 1995 Comp., p. 391.

Section 25.17(f) and Appendix A also issued under 31 U.S.C. 9701; 42 U.S.C. 2214.

SOURCE: 45 FR 14481, Mar. 5, 1980, unless otherwise noted.

GENERAL PROVISIONS

§ 25.1 Purpose.

The regulations in this part establish procedures for granting, reinstating,

extending, transferring, and terminating access authorizations of licensee personnel, licensee contractors or agents, and other persons (e.g., individuals involved in adjudicatory procedures as set forth in 10 CFR part 2, subpart I) who may require access to classified information.

[62 FR 17687, Apr. 11, 1997]

§ 25.3 Scope.

The regulations in this part apply to licensees, certificate holders, and others who may require access to classified information related to a license, certificate, an application for a license or certificate, or other activities as the Commission may determine.

[70 FR 32227, June 2, 2005]

§ 25.5 Definitions.

Access authorization means an administrative determination that an individual (including a consultant) who is employed by or an applicant for employment with the NRC, NRC contractors, agents, licensees and certificate holders, or other person designated by the Executive Director for Operations, is eligible for a security clearance for access to classified information.

Act means the Atomic Energy Act of 1954 (68 Stat. 919), as amended.

Certificate holder means a facility operating under the provisions of parts 71 or 76 of this chapter.

Classified information means either classified National Security Information, Restricted Data, or Formerly Restricted Data or any one of them. It is the generic term for information requiring protection in the interest of National Security whether classified under an Executive Order or the Atomic Energy Act.

Classified National Security Information means information that has been determined under E.O. 13526, as amended, or any predecessor or successor order to require protection against unauthorized disclosure and that is so designated.

Cognizant Security Agency (CSA) means agencies of the Executive Branch that have been authorized by E.O. 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. industry. These agencies are the Department of Defense, the Department of Energy, the Central Intelligence Agency, and the Nuclear Regulatory Commission. A facility has a single CSA which exercises primary authority for the protection of classified information at the facility. The CSA for the facility provides security representation for other government agencies with security interests at the facility. The Secretary of Defense has been designated as Executive Agent for the National Industrial Security Program.

Commission means the Nuclear Regulatory Commission or its duly authorized representatives.

''L'' access authorization means an access authorization granted by the Commission that is normally based on a Tier 3 (T3) investigation conducted by the Defense Counterintelligence and Security Agency (DCSA).

License means a license issued pursuant to 10 CFR parts 50, 52, 60, 63, 70, or 72.

Matter means documents or material.

National Security Information means information that has been determined pursuant to Executive Order 12958, as amended, or any predecessor order to require protection against unauthorized disclosure and that is so designated.

Need-to-know means a determination made by an authorized holder of classified information that a prospective recipient requires access to a specific classified information to perform or assist in a lawful and authorized governmental function under the cognizance of the Commission.

Person means (1) any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, government agency other than the Commission or the Department of Energy (DOE), except that the DOE shall be considered a person to the extent that its facilities are subject to the licensing and related regulatory authority of the Commission pursuant to section 202 of the Energy Reorganization Act of 1974 and sections 104, 105 and 202 of the Uranium Mill Tailings Radiation Control Act of 1978, any State or any political subdivision

of, or any political entity within a State, any foreign government or nation or any political subdivision of any such government or nation, or other entity; and (2) any legal successor, representative, agent, or agency of the foregoing.

''*Q*'' *access authorization* means an access authorization granted by the Commission normally based on a Tier 5 (T5) investigation conducted by the Defense Counterintelligence and Security Agency, the Federal Bureau of Investigation, or other U.S. Government agency that conducts personnel security investigations.

Restricted Data means all data concerning design, manufacture or utilization of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142 of the Act.

Visit authorization letters (VAL) means a letter, generated by a licensee, certificate holder or other organization under the requirements of 10 CFR parts 25 and/or 95, verifying the need-to-know and access authorization of an individual from that organization who needs to visit another authorized facility for the purpose of exchanging or acquiring classified information related to the license.

[45 FR 14481, Mar. 5, 1980, as amended at 46 FR 58283, Dec. 1, 1981; 47 FR 38683, Sept. 2, 1982; 48 FR 24320, June 1, 1983; 50 FR 36984, Sept. 11, 1985; 55 FR 11574, Mar. 29, 1990; 62 FR 17687, Apr. 11, 1997; 64 FR 15647, Apr. 1, 1999; 70 FR 32227, June 2, 2005; 75 FR 73941, Nov. 30, 2010; 86 FR 43401, Aug. 9, 2021; 87 FR 45241, July 28, 2022]

§ 25.7 Interpretations.

Except as specifically authorized by the Commission in writing, no interpretation of the meaning of the regulations in this part by any officer or employee of the Commission other than a written interpretation by the General Counsel will be recognized to be binding upon the Commission.

§ 25.8 Information collection requirements: OMB approval.

(a) The Nuclear Regulatory Commission has submitted the information collection requirements contained in this part to the Office of Management and Budget (OMB) for approval as required by the Paperwork Reduction Act (44 U.S.C. 3501 *et seq.*). The NRC may not conduct or sponsor and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. OMB has approved the information collection requirements contained in this part under control number 3150–0046.

(b) The approved information collection requirements contained in this part appear in §§ 25.11, 25.17, 25.21, 25.23, 25.25, 25.27, 25.29, 25.31, 25.33, and 25.35.

(c) This part contains information collection requirements in addition to those approved under the control number specified in paragraph (a) of this section. These information collection requirements and the control numbers under which they are approved are as follows:

(1) In §§ 25.17(b), 25.21(c), 25.27(a), 25.29, and 25.31, NRC Form 237 is approved under control number 3150–0050.

(2) In §§ 25.17(c), 25.21(c), 25.27(b), 25.29, and 25.31, the ''Electronic Questionnaire for Investigations Processing (e-QIP), SF–86—Questionnaire for National Security Positions'' is approved under control number 3206–0005.

(3) In § 25.21(b), NRC Form 354 is approved under control number 3150–0026.

(4) In § 25.33, NRC Form 136 is approved under control number 3150–0049.

(5) In § 25.35, NRC Form 277 is approved under control number 3150–0051.

[49 FR 19624, May 9, 1984, as amended at 57 FR 3720, Jan. 31, 1992; 62 FR 17687, Apr. 11, 1997; 62 FR 52185, Oct. 6, 1997; 87 FR 45241, July 28, 2022]

§ 25.9 Communications.

Except where otherwise specified, communications and reports concerning the regulations in this part should be addressed to the Director, Division of Facilities and Security, Mail Stop T7–D57, and sent either by mail to the U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001; by hand delivery to the NRC's offices at 11555 Rockville Pike, Rockville, Maryland; or, where practicable, by electronic submission, for example, Electronic Information Exchange, or CD-

ROM. Electronic submissions must be made in a manner that enables the NRC to receive, read, authenticate, distribute, and archive the submission, and process and retrieve it a single page at a time. Detailed guidance on making electronic submissions can be obtained by visiting the NRC's Web site at *http://www.nrc.gov/site-help/e-submittals.html;* by e-mail to *MSHD.Resource@nrc.gov;* or by writing the Office of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001. The guidance discusses, among other topics, the formats the NRC can accept, the use of electronic signatures, and the treatment of nonpublic information.

[68 FR 58803, Oct. 10, 2003, as amended at 74 FR 62681, Dec. 1, 2009; 80 FR 74979, Dec. 1, 2015]

§ 25.11 Specific exemptions.

The NRC may, upon application by any interested person or upon its own initiative, grant exemptions from the requirements of the regulations of this part, that are—

(a) Authorized by law, will not present an undue risk to the public health and safety, and are consistent with the common defense and security; or

(b) Coincidental with one or more of the following:

(1) An application of the regulation in the particular circumstances conflicts with other NRC rules or requirements;

(2) An application of the regulation in the particular circumstances would not serve the underlying purpose of the rule or is not necessary to achieve the underlying purpose of the rule;

(3) When compliance would result in undue hardship or other costs that significantly exceed those contemplated when the regulation was adopted, or that significantly exceed those incurred by others similarly situated;

(4) When the exemption would result in benefit to the common defense and security that compensates for any decrease in the security that may result from the grant of the exemption;

(5) When the exemption would provide only temporary relief from the applicable regulation and the licensee or applicant has made good faith efforts to comply with the regulation;

(6) When there is any other material circumstance present that was not considered when the regulation was adopted that would be in the public interest 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 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:

(i) Electronic Questionnaire for Investigations Processing (e-QIP), SF–86 Questionnaire for National Security Positions;

(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) The Defense Counterintelligence and Security Agency (DCSA) bills the NRC for the cost of each background investigation conducted in support of an application for access authorization (application). The combined cost of the DCSA investigation and the NRC's application processing overhead (NRC processing fee) are recovered through an access authorization fee imposed on applicants for access authorization.

(1) Each application for access authorization, renewal, or change in level must be accompanied by a remittance, payable to the U.S. Nuclear Regulatory Commission, which is equal to the NRC access authorization fee. This fee must be determined using the following formula: the DCSA investigation billing rates on the day the NRC receives the application + the NRC processing fee = the NRC access authorization fee. The

NRC processing fee is determined by multiplying the DCSA investigation billing rate on the day the NRC receives the application by 90.2 percent (*i.e.*, DCSA rate × 90.2 percent).

(2) Updated DCSA investigation billing rates are published periodically in a Federal Investigations Notice (FIN) issued by the DCSA's Federal Investigative Services. Copies of the current DCSA investigation billing rates schedule can be obtained by contacting the NRC's Personnel Security Branch, Division of Facilities Security, Office of Administration by email to *Licensee_ Access_ Authorization_ Fee.Resource@nrc.gov*

(3) The NRC's Information Access Authority Program (IAAP) is considered reimbursable work representing services provided to an organization for which the NRC is entitled payment. The NRC is authorized to receive and retain fees from licensees for services performed. The NRC's Office of the Chief Financial Officer periodically reviews the fees charged for IAAP and makes recommendations on revising those charges to reflect costs incurred by the NRC in providing those services. The reviews are performed using cost analysis techniques to determine the direct and indirect costs. Based on this review, the IAAP fees are adjusted to reflect the current cost for the program. IAAP requests for reciprocity will be charged a flat fee rate of $95.00 as referenced in paragraph (f)(4) of this section. This flat fee is aligned with the level of effort that has been expended by DCSA to process reciprocity requests, and accounts for inflation as well as recovery of the appropriate cost for conducting the investigations. Copies of the current NRC access authorization fee may be obtained by contacting the NRC's Personnel Security Branch, Division of Facilities and Security, Office of Administration by email at: Licensee__Access__ Authorization__

change in the NRC's access authorization fee will be applicable to each access authorization request received on or after the effective date of the DCSA's most recently published investigation billing rates schedule.

(4) Certain applications from individuals having current Federal access authorizations may be processed more expeditiously and at less cost because 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.

(i) Applications for reciprocity will be processed at the NRC flat fee rate of $95 per request, as referenced in the following table:

The NRC application fee for an access authorization of type . . .	NRC fee rate
(A) NRC–L based on certification of comparable investigation [1]	$95
(B) NRC–Q based on certification of comparable investigation [2]	95

[1] If the NRC determines, based on its review of available data, that a Tier 3 investigation is necessary, the appropriate NRC–L fee will be assessed as shown in appendix A to this part before the conduct of the investigation.

[2] If the NRC determines, based on its review of available data, that a Tier 5 investigation is necessary, the appropriate NRC–Q fee will be assessed as shown in appendix A to this part before the conduct of the investigation.

(ii) Applicants shall, in cases where reciprocity is not acceptable and it is necessary to perform a background investigation, be charged the appropriate fee referenced in appendix A to this part. Applicants shall calculate the access authorization fee according to the stated formula (*i.e.*, DCSA rate × 90.2 percent).

[62 FR 17687, Apr. 11, 1997, as amended at 68 FR 62512, Nov. 5, 2003; 70 FR 32227, June 2, 2005; 72 FR 27411, May 16, 2007; 77 FR 26153, May 3, 2012; 77 FR 46258, Aug. 3, 2012; 86 FR 43401, Aug. 9, 2021; 86 FR 47209, Aug. 24, 2021; 87 FR 45241, July 28, 2022]

§ 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 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 discontinued. 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 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 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, Apr. 1, 1999]

CLASSIFIED VISITS

§ 25.35 Classified visits.

(a) The number of classified visits must be held to a minimum. The licensee, certificate holder, applicant for a standard design certification under part 52 of this chapter (including an applicant after the Commission has adopted a final standard design certification rule under part 52 of this chapter), or other facility, or an applicant for or holder of a standard design approval under part 52 of this chapter shall determine that the visit is necessary and that the purpose of the visit cannot be achieved without access to, or disclosure of, classified information. All classified visits require advance notification to, and approval of, the organization to be visited. In urgent cases, visit information may be furnished by telephone and confirmed in writing.

(b) Representatives of the Federal Government, when acting in their official capacities as inspectors, investigators, or auditors, may visit a licensee, certificate holder, or other facility without furnishing advanced notification, provided these representatives present appropriate Government credentials upon arrival. Normally, however, Federal representatives will provide advance notification in the form of an NRC Form 277, ''Request for Visit or Access Approval,'' with the ''need-to-know'' certified by the appropriate NRC office exercising licensing or regulatory authority and verification of an NRC access authorization by the Division of Facilities and Security.

(c) The licensee, certificate holder, or others shall include the following information on all Visit Authorization Letters (VAL) which they prepare.

(1) Visitor's name, address, and telephone number and certification of the level of the facility security clearance;

(2) Name, date and place of birth, and citizenship of the individual intending to visit;

(3) Certification of the proposed visitor's personnel clearance and any special access authorizations required for the visit;

(4) Name of person(s) to be visited;

(5) Purpose and sufficient justification for the visit to allow for a determination of the necessity of the visit; and

(6) Date or period during which the VAL is to be valid.

(d) Classified visits may be arranged for a 12 month period. The requesting facility shall notify all places honoring these visit arrangements of any change in the individual's status that will cause the visit request to be canceled before its normal termination date.

(e) The responsibility for determining need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit. The licensee, certificate holder or other facility shall establish procedures to ensure positive identification of visitors before the disclosure of any classified information.

[62 FR 17689, Apr. 11, 1997, as amended at 64 FR 15649, Apr. 1, 1999; 72 FR 49488, Aug. 28, 2007]

VIOLATIONS

§ 25.37 Violations.

(a) An injunction or other court order may be obtained to prohibit a violation of any provision of:

(1) The Atomic Energy Act of 1954, as amended;

(2) Title II of the Energy Reorganization Act of 1974, as amended; or

(3) Any regulation or order issued under these Acts.

(b) National Security Information is protected under the requirements and sanctions of Executive Order 13526, as amended, or any predecessor or successor orders.

[48 FR 24320, June 1, 1983, as amended at 57 FR 55072, Nov. 24, 1992; 64 FR 15649, Apr. 1, 1999; 70 FR 32227, June 2, 2005; 75 FR 73941, Nov. 30, 2010]

§ 25.39 Criminal penalties.

(a) Section 223 of the Atomic Energy Act of 1954, as amended, provides for criminal sanctions for willful violation of, attempted violation of, or conspiracy to violate, any regulation issued under sections 161b, 161i, or 161o of the Act. For purposes of section 223, all the regulations in part 25 are issued under one or more of sections 161b, 161i, or 161o, except for the sections listed in paragraph (b) of this section.

(b) The regulations in part 25 that are not issued under sections 161b, 161i, or 161o for the purposes of section 223 are as follows: §§ 25.1, 25.3, 25.5, 25.7, 25.8, 25.9, 25.11, 25.19, 25.25, 25.27, 25.29, 25.31, 25.37, and 25.39.

[57 FR 55072, Nov. 24, 1992]

APPENDIX A TO PART 25—FEES FOR NRC ACCESS AUTHORIZATION

The NRC application fee for an access authorization of type . . .	Is the sum of the current DCSA investigation billing rate charged for an investigation of type . . .	Plus the NRC's processing fee (rounded to the nearest dollar), which is equal to the investigation billing rate for the type of investigation referenced multiplied by . . . (%)
Initial "L" access authorization [1]	Tier 3 (T3) (Standard Service)	90.2
Reinstatement of "L" access authorization [2]	No fee assessed for most applications.	
Renewal of "L" access authorization [1]	Tier 3 Reinvestigation (T3R) (Standard Service).	90.2
Initial "Q" access authorization	Tier 5 (T5) (Standard Service)	90.2
Initial "Q" access authorization	T5 (Priority Handling)	90.2
Reinstatement of "Q" access authorization [2]	No fee assessed for most applications.	
Renewal of "Q" access authorization [1]	Tier 5 Reinvestigation (T5R) (Standard Service).	90.2
Renewal of "Q" access authorization [1]	Tier 5 Reinvestigation (T5R) (Priority Handling).	90.2

[1] If the NRC determines, based on its review of available data, that a Tier 5 investigation is necessary, the appropriate fee for an Initial "Q" access authorization will be assessed before the conduct of investigation.
[2] Full fee will only be charged if an investigation is required.

[87 FR 45242, July 28, 2022]

PART 26—FITNESS FOR DUTY PROGRAMS

Subpart A—Administrative Provisions

Subpart B—Program Elements

Subpart C—Granting and Maintaining Authorization