§ 81.53 Notice of designation of the Board.
The Executive Director for Operations of the Nuclear Regulatory Commission will advise the appellant of the designation of the Board, its composition, and Chairman.

[40 FR 8793, Mar. 3, 1975]

§ 81.53 Review by the Board.
(a) The Board shall determine the propriety of any decision concerning the grant, denial, interpretation, modification, or revocation of a license according to the policy and criteria of these regulations, including §81.11, on the record and evidence submitted by an appellant and the Commission to the Board.

(b) A hearing may be requested by the Commission or an appellant within fifteen (15) days after the notice set forth under §81.52(c). An appellant and the Commission shall be given a minimum of fifteen (15) days' notice of the time and place of a hearing. The Commission and the appellant shall have an opportunity to make oral arguments before the Board.

(c) The Board shall make findings of fact and reach a conclusion with respect to the propriety of the decision of the Commission, which conclusion shall constitute the final action of the Commission.
Nuclear Regulatory Commission

GENERAL PROVISIONS

§ 95.1 Purpose.
The regulations in this part establish procedures for obtaining facility security clearance and for safeguarding Secret and Confidential National Security Information and Restricted Data received or developed in conjunction with activities licensed, certified or regulated by the Commission. This part does not apply to Top Secret information because Top Secret information may not be forwarded to licensees, certificate holders, or others within the scope of an NRC license or certificate.


§ 95.3 Scope.
The regulations in this part apply to licensees, certificate holders and others who may require access to classified National Security Information and/or Restricted Data and/or Formerly Restricted Data (FRD) that is used, processed, stored, reproduced, transmitted, transported, or handled in connection with a license or certificate or an application for a license or certificate, or other activities as the Commission may determine.

[70 FR 32227, June 2, 2005]

§ 95.5 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 persons designated by the Executive Director for Operations, is eligible for a security clearance for access to classified information.


Classified mail address means a mail address established for each facility approved by the NRC to which all classified information for the facility is to be sent.

Classified matter means documents or material containing classified information.

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

Classified shipping address means an address established for a facility, approved by the NRC to which classified material that cannot be transmitted as normal mail is to be sent.

Closed area means an area that meets the requirements of the CSA, for the purpose of safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during non-working hours in approved containers.

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 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 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 as Executive Agent for the National Industrial Security Program.

Combination lock means a three position, manipulation resistant, dial type lock bearing an Underwriters' Laboratories, Inc. certification that it is a Group 1 or Group IR unit.

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

Facility (Security) Clearance (FCL) means an administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

Foreign ownership, control, or influence (FOCI) means a foreign interest that has the power, direct or indirect, whether or not exercised, and whether...
or not exercisable through the ownership of a U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may affect adversely the performance of classified contracts.

Infraction means any knowing, willful, or negligent action contrary to the requirements of E.O. 12958, as amended, or its implementing directives, that does not comprise a “violation,” as defined in this section.

Intrusion alarm means a tamper-indicating electrical, electro-mechanical, electro-optical, electronic or similar device which will detect unauthorized intrusion by an individual into a building, protected area, security area, vital area, or material access area, and alert guards or watchmen by means of activated visible and audible signals.

License means a license issued under 10 CFR parts 50, 52, 54, 60, 63, 70, or 72.

Material means chemical substance without regard to form; fabricated or processed item; or assembly, machinery or equipment.

Matter means documents or material.

National security means the national defense or foreign relations of the United States.

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

NRC “L” access authorization means an access authorization granted by the Commission normally based on a national agency check with law and credit investigation (NACLC) or an access national agency check and inquiries investigation (ANACI) conducted by the Office of Personnel Management.

NRC “Q” access authorization means an access authorization granted by the Commission normally based on a single scope background investigation conducted by the Office of Personnel Management, the Federal Bureau of Investigation, or other U.S. Government agency that conducts personnel security investigations.

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.

Protective personnel means guards or watchmen as defined in 10 CFR part 73 or other persons designated responsibility for the protection of classified matter.

Restricted area means a controlled access area established to safeguard classified material, that, because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but that is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.

Restricted data means all data concerning design, manufacture or utilization of atomic weapons, the production 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.

Security area means a physically defined space containing classified material and subject to physical protection and personnel access controls.

Security container includes any of the following repositories:

(1) A security filing cabinet—one that bears a Test Certification Label on the side of the locking drawer, inside wall adjacent to the locking drawer, or interior door plate, or is marked,
“General Services Administration Approved Security Container” on the exterior of the top drawer or door.

(2) A safe—burglar-resistive cabinet or chest which bears a label of the Underwriters’ Laboratories, Inc., certifying the unit to be a TL–15, TL–30, or TRTL–30, and has a body fabricated of not less than 1 inch of steel and a door fabricated of not less than 1 1/2 inches of steel exclusive of the combination lock and bolt work; or bears a Test Certification Label on the inside of the door, or is marked “General Services Administration Approved Security Container” and has a body of steel at least ½ inch thick, and a combination locked steel door at least 1 inch thick, exclusive of bolt work and locking devices; and an automatic unit locking mechanism.

(3) A vault—a windowless enclosure constructed with walls, floor, roof, and door(s) that will delay penetration sufficient to enable the arrival of emergency response forces capable of preventing theft, diversion, damage, or compromise of classified information or matter, when delay time is assessed in conjunction with detection and communication subsystems of the physical protection system.

(4) A vault-type room—a room that has a combination lock door and is protected by an intrusion alarm system that alarms upon the unauthorized penetration of a person anywhere into the room.

(5) Other repositories that would provide comparable physical protection in the judgment of the Division of Facilities and Security.

Security facility—any facility which has been approved by NRC for using, processing, storing, reproducing, transmitting or handling classified matter.

Security reviews means aperiodic security reviews of cleared facilities conducted to ensure that safeguards employed by licensees and others are adequate for the protection of classified information.

Supplemental protection means additional security procedures such as intrusion detection systems, security guards, and access control systems.

Violation means any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information or any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of E.O. 12958, as amended, or its implementing directives.


§ 95.7 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.

§ 95.8 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 3150–0047.

(b) The approved information collection requirements contained in this part appear in §§95.11, 95.15, 95.17, 95.18, 95.21, 95.25, 95.33, 95.34, 95.36, 95.37, 95.39, 95.41, 95.43, 95.45, 95.47, 95.53, and 95.57.


§ 95.9 Communications.

Except where otherwise specified, all communications and reports concerning the regulations in this part should be submitted as follows:

(a) By mail addressed to: ATTN: Document Control Desk, Director, Division of Nuclear Security, Office of Nuclear
§ 95.11 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 rules or requirements of the NRC;

(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 are significantly in excess of those contemplated when the regulation was adopted, or that are significantly in excess of 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 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 not considered when the regulation was adopted for which it would be in the public interest to grant an exemption. If such a 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 15650, Apr. 1, 1999]

§ 95.13 Maintenance of records.

(a) Each licensee, certificate holder or other person granted facility clearance 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, or specifications must include all pertinent information such as stamps, initials, and signatures. The licensee, certificate holder, or other...
Nuclear Regulatory Commission

§ 95.17 Processing facility clearance.

(a) Following the receipt of an acceptable request for facility clearance, the NRC will either accept an existing facility clearance granted by a current CSA and authorize possession of license or certificate related classified information, or process the facility for a facility clearance. Processing will include—

(1) A determination based on review and approval of a Standard Practice Procedures Plan that granting of the Facility Clearance would not be inconsistent with the national interest, including a finding that the facility is not under foreign ownership, control, or influence to such a degree that a determination could not be made. An NRC finding of foreign ownership, control, or influence is based on factors concerning the foreign intelligence threat, risk of unauthorized technology transfer, type and sensitivity of the information that requires protection, the extent of foreign influence, record of compliance with pertinent laws, and the nature of international security and information exchange agreements. The licensee, certificate holder, or other person must advise the NRC within 30 days of any significant events or changes that may affect its status concerning foreign ownership, control, or influence (e.g., changes in ownership; changes that affect the company’s answers to original FOCI questions; indebtedness; and changes in the required form that identifies owners, officers, directors, and executive personnel).

(2) An acceptable security review conducted by the NRC;

(3) Submitting key management personnel for personnel clearances (PCLs); and

(4) Appointing a U.S. citizen employee as the facility security officer.

(b) The request must include the name of the facility, the location of the facility and an identification of any facility clearance issued by another government agency. If there is no existing facility clearance, the request must include a security Standard Practice Procedures Plan that outlines the facility’s proposed security procedures and controls for the protection of classified information, a floor plan of the area in which the matter is to be used, processed, stored, reproduced, transmitted, transported or handled; and Foreign Ownership, Control or Influence information.

(c) NRC will promptly inform applicants of the acceptability of the request for further processing and will notify the licensee or other person of their decision in writing.

§ 95.18 Key personnel.

The senior management official and the Facility Security Officer must always be cleared to a level commensurate with the Facility Clearance. Other key management officials, as determined by the CSA, must be granted an access authorization or be excluded from classified access. When formal exclusion action is required, the organization’s board of directors or similar executive body shall affirm the following, as appropriate.

(a) Officers, directors, partners, regents, or trustees (designated by name) that are excluded may not require, may not have, and can be effectively excluded from access to all classified information disclosed to the organization. These individuals also may not occupy positions that would enable them to adversely affect the organization’s policies or practices in the performance of activities involving classified information. This action will be made a matter of record by the organization’s executive body. A copy of the resolution must be furnished to the CSA.

(b) Officers, directors, partners, regents, or trustees (designated by name) that are excluded may not require, may not have, and can be effectively denied access to higher-level classified information (specify which higher level(s)). These individuals may not occupy positions that would enable them to adversely affect the organization’s policies or practices in the protection of classified information. This action will be made a matter of record by the organization’s executive body. A copy of the resolution must be furnished to the CSA.

§ 95.19 Changes to security practices and procedures.

(a) Except as specified in paragraph (b) of this section, each licensee, certificate holder, or other person shall obtain prior CSA approval for any proposed change to the name, location, security procedures and controls, or floor plan of the approved facility. A written description of the proposed change must be furnished to the CSA and the NRC Regional Administrator of the cognizant Regional Office listed in appendix A to part 73 of this chapter, and, if the NRC is not the CSA, also to the Director, Division of Nuclear Security, Office of Nuclear Security and Incident Response; the communications to NRC personnel should be by an appropriate method listed in §95.9. These substantive changes to the Standard Practice Procedures Plan that affect the security of the facility must be submitted to the NRC Division of Nuclear Security, or CSA, at least 30 days prior to the change so that they may be evaluated. The CSA shall promptly respond in writing to all such proposals. Some examples of substantive changes requiring prior CSA approval include—

1. A change in the approved facility’s classified mail address; or

2. A temporary or permanent change in the location of the approved facility (e.g., moving or relocating NRC’s classified interest from one room or building to another). Approved changes will be reflected in a revised Standard Practice Procedures Plan submission within 30 days of approval. Page changes rather than a complete rewrite of the plan may be submitted.

(b) A licensee, certificate holder, or other person may effect a minor, non-substantive change to an approved Standard Practice Procedures Plan for the safeguarding of classified information without receiving prior CSA approval. These minor changes that do not affect the security of the facility may be submitted to the addresses noted in paragraph (a) of this section within 30 days of the change. Page changes rather than a complete rewrite of the plan may be submitted. Some examples of minor, non-substantive changes to the Standard Practice Procedures Plan include—

1. The designation/appointment of a new facility security officer; or

2. A revision to a protective personnel patrol routine, provided the new routine continues to meet the minimum requirements of this part.
(c) A licensee, certificate holder, or other person must update its NRC facility clearance every five years either by submitting a complete Standard Practice Procedures Plan or a certification that the existing plan is fully current to the Division of Nuclear Security.


§ 95.25 Protection of National Security Information and Restricted Data in storage.

(a) Secret matter, while unattended or not in actual use, must be stored in—

(1) A safe, steel file cabinet, or safe-type steel file container that has an automatic unit locking mechanism. All such receptacles will be accorded supplemental protection during non-working hours; or

(2) Any steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets, or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock. The keepers of the rigid metal lock bar must be secured to the cabinet by welding, rivets, or bolts, so they cannot be removed and replaced without leaving evidence of the entry. The drawers of the container must be held securely so their contents cannot be removed without forcing open the drawer. This type of cabinet will be accorded supplemental protection during non-working hours.

(b) Confidential matter while unattended or not in use must be stored in the same manner as SECRET matter except that no supplemental protection is required.

(c) Classified lock combinations.

(1) A minimum number of authorized persons may know the combinations to authorized storage containers. Security containers, vaults, cabinets, and other authorized storage containers must be kept locked when not under the direct supervision of an authorized person entrusted with the contents.
§ 95.27 Protection while in use.

While in use, classified matter must be under the direct control of an authorized individual to preclude physical, audio, and visual access by persons who do not have the prescribed access authorization or other written CSA disclosure authorization (see §95.36 for additional information concerning disclosure authorizations).

§ 95.29 Establishment of Restricted or Closed areas.

(a) If, because of its nature, sensitivity or importance, classified matter cannot otherwise be effectively controlled in accordance with the provisions of §§95.25 and 95.27, a Restricted or Closed area must be established to protect this matter.

(b) The following measures apply to Restricted Areas:

(1) Restricted areas must be separated from adjacent areas by a physical barrier designed to prevent unauthorized access (physical, audio, and visual) into these areas.
§ 95.33 Security education.

All cleared employees must be provided with security training and briefings commensurate with their involvement with classified information. The facility may obtain defensive security, threat awareness, and other education and training information and material from their CSA or other sources.

(a) Facility Security Officer training. Licensees and others are responsible for ensuring that the Facility Security Officer is received by all cleared employees who have access to nuclear power plant classified information, and shall be updated each year to inform the Facility Security Officer of current developments in protective security and classified information protection.

The Facility Security Officer shall be responsible for:

1. Coordinating the preparation and implementation of the facility's security program.
2. Ensuring that the facility's security program is in compliance with NRC regulations and current guidance.
3. Coordinating with other facilities, such as nuclear power plants, defense installations, or other facilities with classified information.
4. Providing briefings and training to all cleared employees who have access to classified information.

(b) All cleared employees shall receive security training commensurate with their need-to-know.

The training shall:

1. Include defensive security and threat awareness training.
2. Provide instructions on how to handle classified information.
3. Include procedures for handling classified information.
4. Provide instructions on how to handle classified information.
5. Include procedures for handling classified information.
6. Include procedures for handling classified information.
7. Include procedures for handling classified information.
8. Include procedures for handling classified information.
9. Include procedures for handling classified information.
10. Include procedures for handling classified information.

The training shall be provided by qualified security professionals.

(2) Controls must be established to prevent unauthorized access to and removal of classified matter.

(3) Access to classified matter must be limited to persons who possess appropriate access authorization or other written CSA disclosure authorization and who require access in the performance of their official duties or regulatory obligations.

(4) Persons without appropriate access authorization for the area visited must be escorted by an appropriate CSA access authorized person at all times while within Restricted or Closed Areas.

(5) Each individual authorized to enter a Restricted or Closed Area must be issued a distinctive form of identification (e.g., badge) when the number of employees assigned to the area exceeds thirty per shift.

(6) During nonworking hours, admittance must be controlled by protective personnel. Protective personnel shall conduct patrols during nonworking hours at least every 8 hours and more frequently if necessary to maintain a commensurate level of protection. Entries must be continuously monitored by protective personnel or by an approved alarm system.

(c) Due to the size and nature of the classified material, or operational necessity, it may be necessary to construct Closed Areas for storage because GSA-approved containers or vaults are unsuitable or impractical. Closed Areas must be approved by the CSA. The following measures apply to Closed Areas:

1. Access to Closed Areas must be controlled to preclude unauthorized access. This may be accomplished through the use of a cleared employee or by a CSA approved access control device or system.
2. Access must be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified matter within the area. Persons without the appropriate level of clearance and/or need-to-know must be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented.
3. The Closed Area must be accorded supplemental protection during nonworking hours. During these hours, admittance to the area must be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. However, doors secured from the inside with a panic bolt (for example, actuated by a panic bar), a dead bolt, a rigid wood or metal bar, or other means approved by the CSA, do not require additional locking devices.
4. Open shelf or bin storage of classified matter in Closed Areas requires CSA approval. Only areas protected by an approved intrusion detection system will qualify for approval.


§ 95.31 Protective personnel.

Whenever protective personnel are used to protect classified information, they shall:

(a) Possess an "L" access authorization (or CSA equivalent) if the licensee, certificate holder, or other person possesses information classified Confidential National Security Information, Confidential Restricted Data or Secret National Security Information.

(b) Possess a "Q" access authorization (or CSA equivalent) if the licensee, certificate holder, or other person possesses Secret Restricted Data related to nuclear weapons design, manufacturing and vulnerability information; and certain particularly sensitive Naval Nuclear Propulsion Program information (e.g., fuel manufacturing technology) and the protective personnel require access as part of their regular duties.

[72 FR 49562, Aug. 28, 2007]
§ 95.34 Control of visitors.

(a) Uncleared visitors. Licensees, certificate holders, or other persons subject to this part shall take measures to preclude access to classified information by uncleared visitors.

(b) Foreign visitors. Licensees, certificate holders, or other persons subject to this part shall take measures as may be necessary to preclude access to classified information by foreign visitors.

§ 95.35 Access to matter classified as National Security Information and Restricted Data.

(a) Except as the Commission may authorize, no licensee, certificate holder or other person subject to the regulations in this part may receive or may
permit any other licensee, certificate holder, or other person to have access to matter revealing Secret or Confidential National Security Information or Restricted Data unless the individual has:

(1)(i) A “Q” access authorization which permits access to matter classified as Secret and Confidential Restricted Data or Secret and Confidential National Security Information which includes intelligence information, CRYPTO (i.e., cryptographic information) or other classified communications security (COMSEC) information, or

(ii) An “L” access authorization which permits access to matter classified as Confidential Restricted Data and Secret and Confidential National Security Information other than that noted in paragraph (a)(1)(i) of this section except that access to certain Confidential COMSEC information is permitted as authorized by a National Communications Security Committee waiver dated February 14, 1984.

(2) An established “need-to-know” for the matter (See Definitions, §95.5).

(3) NRC-approved storage facilities if classified documents or material are to be transmitted to the licensee, certificate holder, or other person.

(b) Matter classified as National Security Information or Restricted Data shall not be released by a licensee or other person subject to part 95 to any personnel other than properly access authorized Commission licensee employees, or other individuals authorized access by the Commission.

(c) Access to matter which is National Security Information at NRC-licensed facilities or NRC-certified facilities by authorized representatives of IAEA is permitted in accordance with §95.36.

§95.36 Access by representatives of the International Atomic Energy Agency or by participants in other international agreements.

(a) Based upon written disclosure authorization from the NRC Division of Nuclear Security that an individual is an authorized representative of the International Atomic Energy Agency (IAEA) or other international organization and that the individual is authorized to make visits or inspections in accordance with an established agreement with the United States Government, a licensee, certificate holder, or other person subject to this part shall permit the individual (upon presentation of the credentials specified in §75.7 of this chapter and any other credentials identified in the disclosure authorization) to have access to matter classified as National Security Information that is relevant to the conduct of a visit or inspection. A disclosure authorization under this section does not authorize a licensee, certificate holder, or other person subject to this part to provide access to Restricted Data.

(b) For purposes of this section, classified National Security Information is relevant to the conduct of a visit or inspection if—

(1) In the case of a visit, this information is needed to verify information according to §75.13 of this chapter; or

(2) In the case of an inspection, an inspector is entitled to have access to the information under §75.42 of this chapter.

(c) In accordance with the specific disclosure authorization provided by the Division of Nuclear Security, licensees, certificate holders, or other persons subject to this part are authorized to release (i.e., transfer possession of) copies of documents that contain classified National Security Information directly to IAEA inspectors and other representatives officially designated to request and receive classified National Security Information documents. These documents must be marked specifically for release to IAEA or other international organizations in accordance with instructions contained in the NRC’s disclosure authorization letter. Licensees, certificate holders, and other persons subject to this part may also forward these documents through the NRC to the international organization’s headquarters in accordance with the NRC disclosure authorization. Licensees, certificate holders, and other persons may not reproduce documents containing classified National Security Information except as provided in §95.43.
(d) Records regarding these visits and inspections must be maintained for 5 years beyond the date of the visit or inspection. These records must specifically identify each document released to an authorized representative and indicate the date of the release. These records must also identify (in such detail as the Division of Nuclear Security, by letter, may require) the categories of documents that the authorized representative has had access and the date of this access. A licensee, certificate holder, or other person subject to this part shall also retain Division of Nuclear Security disclosure authorizations for 5 years beyond the date of any visit or inspection when access to classified information was permitted.

(e) Licensees, certificate holders, or other persons subject to this part shall take such measures as may be necessary to preclude access to classified matter by participants of other international agreements unless specifically provided for under the terms of a specific agreement.

§ 95.37 Classification and preparation of documents.

(a) Classification. Classified information generated or possessed by a licensee, certificate holder, or other person must be appropriately marked. Classified material which is not conducive to markings (e.g., equipment) may be exempt from this requirement. These exemptions are subject to the approval of the CSA on a case-by-case basis. If a person or facility generates or possesses information that is believed to be classified based on guidance provided by the NRC or by derivation from classified documents, but which no authorized classifier has determined to be classified, the information must be protected and marked with the appropriate classification markings pending review and signature of an NRC authorized classifier. This information shall be protected as classified information pending final determination.

(b) Classification consistent with content. Each document containing classified information shall be classified Secret or Confidential according to its content. NRC licensees, certificate holders, or other persons subject to the requirements of 10 CFR part 95 may not make original classification decisions.

(c) Markings required on face of documents. (1) For derivative classification of classified National Security Information:

(i) Derivative classifications of classified National Security Information must contain the identity of the source document or the classification guide, including the agency and office of origin, on the “Derived From” line and its classification date. If more than one source is cited, the “Derived From” line should indicate “Multiple Sources.” The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document.

(ii) Declassification instructions. When marking derivatively classified documents, the “DECLASSIFY ON” line must carry forward the declassification instructions as reflected in the original document. If multiple sources are used, the instructions will carry forward the longest duration.

(iii) An example of the marking stamp is as follows:

```
Derived from
(Source/Date)
Reason:

Declassify On:
(Date/Event/Exemption)
Classifier:
(Name/Title/Number)
```

(2) For Restricted Data documents:

(i) Identity of the classifier. The identity of the classifier must be shown by completion of the “Derivative Classifier” line. The “Derivative Classifier” line must show the name of the person classifying the document and the basis for the classification. Dates for downgrading or declassification do not apply.

(ii) Classification designation (e.g., Secret, Confidential) and Restricted Data. NOTE: No “Declassification” instructions will be placed on documents containing Restricted Data.

(d) Placement of markings. The highest classification marking assigned to a
document must be placed in a conspicuous fashion in letters at the top and bottom of the outside of the front covers and title pages, if any, and first and last pages on which text appears, on both bound and unbound documents, and on the outside of back covers of bound documents. The balance of the pages must be marked at the top and bottom with:

(1) The overall classification marking assigned to the document;
(2) The highest classification marking required by content of the page; or
(3) The marking UNCLASSIFIED if they have no classified content.

(e) Additional markings. (1) If the document contains any form of Restricted Data, it must bear the appropriate marking on the first page of text, on the front cover and title page, if any. For example: "This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions."

(2) Limitation on reproduction or dissemination. If the originator or classifier determines that reproduction or further dissemination of a document should be restricted, the following additional wording may be placed on the face of the document:

Reproduction or Further Dissemination Requires Approval of

if any portion of this additional marking does not apply, it should be crossed out.

(f) Portion markings. In addition to the information required on the face of the document, each classified document is required, by marking or other means, to indicate clearly which portions are classified (e.g., paragraphs or pages) and which portions are not classified. The symbols (S) for Secret, (C) for Confidential, (U) for Unclassified, or (RD) for Restricted Data may be used immediately preceding or following the text to which it applies, except that the designation must follow titles or subjects. (Portion marking of paragraphs is not required for documents containing Restricted Data.) If this type of portion marking is not practicable, the document must contain a description sufficient to identify the classified information and the unclassified information.

(g) Transmittal document. If a document transmitting classified information contains no classified information or the classification level of the transmittal document is not as high as the highest classification level of its enclosures, then the document must be marked at the top and bottom with a classification at least as high as its highest classified enclosure. The classification may be higher if the enclosures, when combined, warrant a higher classification than any individual enclosure. When the contents of the transmittal document warrants a lower classification than the highest classified enclosure(s) or combination of enclosures or requires no classification, a stamp or marking such as the following must also be used on the transmittal document:

UPON REMOVAL OF ATTACHMENTS
THIS DOCUMENT IS:

(Classification level of transmittal document standing alone or the word "UNCLASSIFIED" if the transmittal document contains no classified information.)

(h) Classification challenges. Licensees, certificate holders, or other persons in authorized possession of classified National Security Information who in good faith believe that the information's classification status (i.e., that the document), is classified at either too high a level for its content (overclassification) or too low for its content (underclassification) are expected to challenge its classification status. Licensees, certificate holders, or other persons who wish to challenge a classification status shall—

(1) Refer the document or information to the originator or to an authorized NRC classifier for review. The authorized classifier shall review the document and render a written classification decision to the holder of the information.

(2) In the event of a question regarding classification review, the holder of the information or the authorized classifier shall consult the NRC Division of
§ 95.39  External transmission of documents and material.

(a) Restrictions. Documents and material containing classified information received or originated in connection with an NRC license, certificate, or standard design approval or standard design certification under part 52 of this chapter must be transmitted only to CSA approved security facilities.

(b) Preparation of documents. Documents containing classified information must be prepared in accordance with the following when transmitted outside an individual installation.

(1) The documents must be enclosed in two sealed opaque envelopes or wrappers.

(2) The inner envelope or wrapper must contain the addressee's classified mail address and the name of the intended recipient. The appropriate classification must be placed on both sides of the envelope (top and bottom) and the additional markings, as appropriate, referred to in §95.37(e) must be placed on the side bearing the address.

(3) The outer envelope or wrapper must contain the addressee's classified mailing address. The outer envelope or wrapper may not contain any classification, additional marking or other notation that indicate that the enclosed document contains classified information. The Classified Mailing Address shall be uniquely designated for the receipt of classified information. The classified shipping address for the receipt of material (e.g., equipment) should be different from the classified mailing address for the receipt of classified documents.

(4) A receipt that contains an unclassified description of the document, the document number, if any, date of the document, classification, the date of transfer, the recipient and the person transferring the document must be enclosed within the inner envelope containing the document and be signed by the recipient and returned to the sender whenever the custody of a Secret document is transferred. This receipt process is at the option of the sender for Confidential information.

(c) Methods of transportation. (1) Secret matter may be transported only by one of the following methods within and directly between the U.S., Puerto Rico, or a U.S. possession or trust territory:

(ii) A cleared "Commercial Carrier."

(3) Other methods as directed, in writing, by the CSA.
§ 95.45 Changes in classification.

(a) Documents containing classified National Security Information must be downgraded or declassified as authorized by the NRC classification guides or as determined by the NRC. Requests for downgrading or declassifying any NRC classified information should be forwarded to the NRC’s Division of Nuclear Security, Nuclear Security and Incident Response, using an appropriate method listed in §95.9. Requests for downgrading or declassifying of Restricted Data will be forwarded to the NRC Division of Nuclear Security for coordination with the Department of Energy.

(b) If a change of classification or declassification is approved, the previous classification marking must be canceled and the following statement, properly completed, must be placed on the first page of the document:

Classification canceled (or changed to)

(insert appropriate classification)
§ 95.47 Destruction of matter containing classified information.

Documents containing classified information may be destroyed by burning, pulping, or another method that ensures complete destruction of the information that they contain. The method of destruction must preclude recognition or reconstruction of the classified information. Any doubts on methods should be referred to the CSA.

[64 FR 15653, Apr. 1, 1999]

§ 95.49 Security of automatic data processing (ADP) systems.

Classified data or information may not be processed or produced on an ADP system unless the system and procedures to protect the classified data or information have been approved by the CSA. Approval of the ADP system and procedures is based on a satisfactory ADP security proposal submitted as part of the licensee's, certificate holder's, or other person's request for facility clearance outlined in § 95.15 or submitted as an amendment to its existing Standard Practice Procedures Plan for the protection of classified information.

[72 FR 49564, Aug. 28, 2007]
Nuclear Regulatory Commission § 95.63

does not relieve any person from compliance with the regulations in this part.

§ 95.57 Reports.

Each licensee, certificate holder, or other person having a facility clearance shall report to the CSA and the Regional Administrator of the appropriate NRC Regional Office listed in 10 CFR part 73, appendix A:

(a) Any alleged or suspected violation of the Atomic Energy Act, Espionage Act, or other Federal statutes related to classified information (e.g., deliberate disclosure of classified information to persons not authorized to receive it, theft of classified information). Incidents such as this must be reported within 1 hour of the event followed by written confirmation within 30 days of the incident; and

(b) Any infractions, losses, compromises, or possible compromise of classified information or classified documents not falling within paragraph (a) of this section. Incidents such as these must be entered into a written log. A copy of the log must be provided to the NRC on a monthly basis. Details of security infractions including corrective action taken must be available to the CSA upon request.

(c) In addition, NRC requires records for all classification actions (documents classified, declassified, or downgraded) to be submitted to the NRC Division of Nuclear Security. These may be submitted either electronically by an on-line system (NRC prefers the use of a dial-in automated system connected to the Division of Nuclear Security) or by paper copy using NRC Form 790.

§ 95.59 Inspections.

The Commission shall make inspections and reviews of the premises, activities, records and procedures of any licensee, certificate holder, or other person subject to the regulations in this part as the Commission and CSA deem necessary to effect the purposes of the Act, E.O. 12958 and/or NRC rules.
[72 FR 49564, Aug. 28, 2007]

VIOLATIONS

§ 95.61 Violations.

(a) The Commission may obtain an injunction or other court order to prevent a violation of the provisions of—

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

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

(3) A regulation or order issued pursuant to those Acts.

(b) The Commission may obtain a court order for the payment of a civil penalty imposed under section 234 of the Atomic Energy Act:

(1) For violations of—

(i) Sections 53, 57, 62, 63, 81, 82, 101, 103, 104, 107, or 109 of the Atomic Energy Act of 1954, as amended;

(ii) Section 206 of the Energy Reorganization Act;

(iii) Any rule, regulation, or order issued pursuant to the sections specified in paragraph (b)(1)(i) of this section;

(iv) Any term, condition, or limitation of any license issued under the sections specified in paragraph (b)(1)(i) of this section.

(2) For any violation for which a license may be revoked under Section 186 of the Atomic Energy Act of 1954, as amended.
[57 FR 55080, Nov. 24, 1992]

§ 95.63 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 95 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 95 that are not issued under sections 161b, 161i, or 161o for the purposes of section 223 are as follows: §§ 95.1, 95.3, 95.5, 95.7,
95.8, 95.9, 95.11, 95.17, 95.19, 95.21, 95.23, 95.55, 95.59, 95.61, and 95.63.

[57 FR 55080, Nov. 24, 1992]

PART 100—REACTOR SITE CRITERIA

Sec.
100.1 Purpose.
100.2 Scope.
100.3 Definitions.
100.4 Communications.
100.8 Information collection requirements: OMB approval.

Subpart A—Evaluation Factors for Stationary Power Reactor Site Applications Before January 10, 1997 and for Testing Reactors

100.10 Factors to be considered when evaluating sites.
100.11 Determination of exclusion area, low population zone, and population center distance.

Subpart B—Evaluation Factors for Stationary Power Reactor Site Applications on or After January 10, 1997

100.20 Factors to be considered when evaluating sites.
100.21 Non-seismic site criteria.
100.23 Geologic and seismic siting criteria.

APPENDIX A TO PART 100—SEISMIC AND GEOLOGIC SITING CRITERIA FOR NUCLEAR POWER PLANTS


SOURCE: 27 FR 3509, Apr. 12, 1962, unless otherwise noted.

§ 100.1 Purpose.

(a) The purpose of this part is to establish approval requirements for proposed sites for stationary power and testing reactors subject to part 50 or part 52 of this chapter.

(b) There exists a substantial base of knowledge regarding power reactor siting, design, construction, and operation. This base reflects that the primary factors that determine public health and safety are the reactor design, construction and operation.

(c) Siting factors and criteria are important in assuring that radiological doses from normal operation and postulated accidents will be acceptably low, that natural phenomena and potential man-made hazards will be appropriately accounted for in the design of the plant, that site characteristics are such that adequate security measures to protect the plant can be developed, and that physical characteristics unique to the proposed site that could pose a significant impediment to the development of emergency plans are identified.

(d) This approach incorporates the appropriate standards and criteria for approval of stationary power and testing reactor sites. The Commission intends to carry out a traditional defense-in-depth approach with regard to reactor siting to ensure public safety. Siting away from densely populated centers has been and will continue to be an important factor in evaluating applications for site approval.

[61 FR 65175, Dec. 11, 1996]

§ 100.2 Scope.

The siting requirements contained in this part apply to applications for site approval for the purpose of constructing and operating stationary power and testing reactors pursuant to the provisions of part 50 or part 52 of this chapter.

[61 FR 65175, Dec. 11, 1996]

§ 100.3 Definitions.

As used in this part:

Combined license means a combined construction permit and operating license with conditions for a nuclear power facility issued pursuant to subpart C of part 52 of this chapter.

Early Site Permit means a Commission approval, issued pursuant to subpart A of part 52 of this chapter, for a site or sites for one or more nuclear power facilities.

Exclusion area means that area surrounding the reactor, in which the reactor licensee has the authority to determine all activities including exclusion or removal of personnel and property from the area. This area may be traversed by a highway, railroad, or waterway, provided these are not so close to the facility as to interfere with normal operations of the facility and...