[AF37-1]

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

April 24, 1996

MEMORANDUM TO: Attached List

FROM: Raymond J. Brady, Director
Division of Security
Office of Administration

SUBJECT: AMENDMENT TO 10 CFR PART 25, "ACCESS AUTHORIZATION FOR LICENSEE PERSONNEL" AND PART 95, "SECURITY FACILITY APPROVAL AND SAFEGUARDING OF NATIONAL SECURITY INFORMATION AND RESTRICTED DATA"

Attached is a redraft of the proposed rule, "Access to and Protection of Classified Information," amending 10 CFR Parts 25 and 95 which you reviewed in March, 1996.

This draft reflects, in redline-strikeout, changes made in response to comments received. Since Office comments were not extensive and did not involve major substantive issues, we would appreciate a quick review. Comments or concurrence via email would be acceptable.

We are circulating this draft to all Offices concurrently to reduce the time required to complete the concurrence process. Please provide comments or concurrence by May 8, 1996.

If you or your staff have any questions, please contact Duane G. Kidd of my staff on 415-7403 or by email at DGK.

Attachment: As stated

Attached List - Memorandum Dated April 24, 1996
SUBJECT: AMENDMENT TO 10 CFR PARTS 25 AND 95

Elizabeth Q. Ten-Eyck, NMSS/FCSS
Frank P. Gillespie, NRR/DISP
Bill M. Morris, RES/DRA
Bradley J. Fewell, OGC

[7590-01-P]

NUCLEAR REGULATORY COMMISSION

10 CFR PARTS 25 AND 95

RIN 3150-AF37

ACCESS TO AND PROTECTION OF CLASSIFIED INFORMATION

AGENCY: Nuclear Regulatory Commission.

ACTION: Proposed rule.

SUMMARY: The Nuclear Regulatory Commission is amending its regulations to conform the requirements for the protection of and access to classified information to new national security policy documents. ~~Specifically, the National Industrial Security Program Operating Manual and Executive Orders 12958, "Classified National Security Information," and 12968, "Access to Classified Information."~~ This proposed rule is necessary to ensure that classified information in the possession of NRC licensees and others under the NRC's regulatory requirements is protected in accordance with current national policies.

DATES: The comment period expires (60 days from date of publication in the Federal Register). Comments received after this date will be considered if it is practical to do so, but the Commission is able to assure consideration only for comments received on or before this date. Comments may be submitted either electronically or in written form. For written comments submit to: The Secretary of the Commission, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, Attention: Docketing and Service Branch. Copies of comments received may be examined at the NRC Public Document Room, 2120 L Street NW. (Lower Level), Washington, DC.

Electronic comments may be submitted, in either ASCII text or WordPerfect format (version 5.1 or later), by calling the NRC Electronic Bulletin Board (BBS) on FedWorld. The bulletin board may be accessed using a personal computer, a modem, and one of the commonly available communications software packages, or directly via Internet. Background documents on the rulemaking are also available, as practical, for downloading and viewing on the bulletin board.

If using a personal computer and modem, the NRC rulemaking subsystem on FedWorld can be accessed directly by dialing the toll free number (800) 303-9672. Communication software parameters should be set as follows: parity to none, data bits to 8, and stop bits to 1 (N,8,1). Using ANSI or VT-100 terminal emulation, the NRC rulemaking subsystem can then be accessed by selecting the "Rules Menu" option from the "NRC Main Menu." Users will find the "FedWorld Online User's Guides" particularly helpful. Many NRC subsystems and data bases also have a "Help/Information Center" option that is tailored to the particular subsystem.

The NRC subsystem on FedWorld can also be accessed by a direct dial phone number for the main FedWorld BBS, (703) 321-3339, or by using Telnet via Internet: fedworld.gov. If using (703) 321-3339 to contact FedWorld, the NRC subsystem will be accessed from the main FedWorld menu by selecting the "Regulatory, Government Administration and State Systems," then selecting "Regulatory Information Mall." At that point, a menu will be displayed that has an option "U.S. Nuclear Regulatory Commission" that will take you to the NRC Online main menu. The NRC Online area also can be accessed directly by typing "/go nrc" at a FedWorld command line. If you access NRC from FedWorld's main menu, you may return to FedWorld by selecting the "Return to FedWorld" option from the NRC Online Main Menu. However, if you access NRC at

FedWorld by using NRC's toll-free number, you will have full access to all NRC systems, but you will not have access to the main FedWorld system.

If you contact FedWorld using Telnet, you will see the NRC area and menus, including the Rules Menu. Although you will be able to download documents and leave messages, you will not be able to write comments or upload files (comments). If you contact FedWorld using FTP, all files can be accessed and downloaded but uploads are not allowed; all you will see is a list of files without descriptions (normal Gopher look). An index file listing all files within a subdirectory, with descriptions, is available. There is a 15-minute time limit for FTP access.

Although FedWorld also can be accessed through the World Wide Web, like FTP that mode only provides access for downloading files and does not display the NRC Rules Menu.

For more information on NRC bulletin boards call Mr. Arthur Davis, Systems Integration and Development Branch, NRC, Washington, DC 20555, telephone (301) 415 5780; e-mail AXD3@nrc.gov.

Single copies of this proposed rulemaking may be obtained by written request or telefax (301) 415-2260) from: Distribution Services, Printing and Mail Services Branch, Office of Administration, U.S. Nuclear Regulatory Commission, Washington DC 20555. Certain documents related to this rulemaking, including comments received, may be examined at the NRC Public Document Room, 2120 L Street NW. (Lower Level), Washington, DC. These same documents may also be viewed and downloaded electronically via the Electronic Bulletin Board established by NRC for this rulemaking as indicated above.

FOR FURTHER INFORMATION CONTACT: Duane G. Kidd, Division of Security, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555-

0001 telephone (301) 415-7403, Email DGK@NRC.GOV.

SUPPLEMENTARY INFORMATION:

Background

The national requirements for the protection of and access to Classified National Security Information have been revised by the issuance of the National Industrial Security Program Operating Manual (NISPOM), Executive Order 12958, "Classified National Security Information," and Executive Order 12968, "Access to Classified Information." In order to conform to these new national security policy documents, the NRC must revise its regulations for the protection of classified information. The requirements of 10 CFR Parts 25 and 95 are substantially based on Executive Order 12356, dated April 6, 1982, which was superseded by Executive Order 12958.

The proposed rule would amend the provisions of 10 CFR Parts 25 and 95 that deal with requirements for access to and protection of classified information that have been changed or added by the NISPOM or the Executive Orders. Specifically changes include revised and added definitions such as Cognizant Security Agency, Classified National Security Information, Classified Information, Facility Security Clearance, Foreign Ownership, Control, or Influence~~. It also includes~~ and numerous amendments to reflect the fact that NRC may permit another Cognizant Security Agency (DOE, DoD, or CIA) to assume some or all of the security oversight functions at an NRC facility under the requirements of 10 CFR Parts 25 and/or 95 when that agency also has a significant security interest at the facility. The proposed rule addresses the intent of Executive Order 12829, "National Industrial Security Program," to reduce wasteful and inefficient duplicative oversight of private

facilities which have classified interests from more than one government agency.

~~Additionally, it~~ The proposed rule would also adopt new requirements in areas where the Executive Orders or the NISPOM mandate specific requirements ~~which were~~ not included in the previous versions of the rules. These new requirements include --

Requiring that key management personnel have personnel security clearances as well as those employees with access to classified information;

Permitting reinstatement of a personnel security clearance up to 24 months after termination instead of the previous 6 months;

Permitting facility security officers to issue visit authorization letters directly rather than through the NRC Division of Security;

Requiring a finding that a facility is not under foreign ownership, control or influence;

Requiring facility security officers to have specific training related to their position;

Permitting the use of reinforced steel filing cabinets with lockbars and key locks for classified information (provided appropriate supplemental protection is in place during non-working hours);

Changing the security classification markings to conform to Executive Order 12958;

Reducing the accountability requirements for Secret documents;

Defining procedures for challenging classification decisions that one believes to be in error;

Allowing for additional methods of transmitting classified information; and

Imposing fewer limitations on a facilities authority to reproduce

classified information when operationally necessary.

## Environmental Impact: Categorical Exclusion

The NRC has determined that this proposed rule is the type of action described in categorical exclusion 10 CFR 51.22(c)(2). Therefore, neither an environmental impact statement nor an environmental assessment has been prepared for this proposed rule.

## Paperwork Reduction Act Statement

This proposed rule amends information collection requirements that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501, et seq.). This rule has been submitted to the Office of Management and Budget for review and approval of the information collection requirements.

The public reporting burden for this collection of information is estimated to average 8.5 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. The U.S. Nuclear Regulatory Commission is seeking public comment on the potential impact of the collection of information contained in the proposed rule and on the following issues:

1. Is the proposed collection of information necessary for the proper performance of the functions of the NRC, including whether the information will have practical utility?
2. Is the estimate of burden accurate?
3. Is there a way to enhance the quality, utility, and clarity of the information to be collected?
4. How can the burden of the information collection be minimized, including the use of automated collection techniques?

Send comments on any aspect of this proposed collection of information, including suggestions for reducing the burden, to the Information and Records Management Branch (T-6 F33), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by Internet electronic mail at BJS1@NRC.GOV; and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-0046, -0047), Office of Management and Budget, Washington, DC 20503. Comments to OMB on the collections of information or on the above issues should be submitted by (insert date 30 days after publication in the Federal Register). Comments received after this date will be considered if it is practical to do so, but assurance of consideration cannot be given to comments received after this date.

Public Protection Notification

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.

Regulatory Analysis

The Commission has prepared a regulatory analysis for this proposed regulation. The analysis examines the costs and benefits of the alternatives considered by the Commission. The analysis is available for inspection in the NRC Public Document Room, 2120 L Street, NW. (Lower Level), Washington, DC. Single copies of the analysis may be obtained from Duane G. Kidd, Division of Security, Office of Administration, U. S. Nuclear Regulatory Commission, Washington, DC 20555, telephone: (301) 415-7403

Regulatory Flexibility Certification

As required by the Regulatory Flexibility Act of 1980, 5 U.S.C. 605(b), the Commission certifies that this rule, if adopted, will not have a

significant economic impact upon a substantial number of small entities. The NRC carefully considered the effect on small entities in developing this proposed rule on the protection of classified information and have determined that none of the facilities affected by this rule would ~~be considered as small~~ qualify as a small entity under the NRC's size standards (10 CFR 2.810).

Backfit Analysis

The NRC has determined that the backfit rule, 10 CFR 50.109, applies to this rulemaking initiative because it falls within the criteria of 10 CFR Part 50.109(a)(1), but that a backfit analysis is not required because this rulemaking qualifies for exemption under 10 CFR 50.109(a)(4)(iii) that reads "That the regulatory action involves . . . redefining what level of protection to the . . . common defense and security should be regarded as adequate."

List of Subjects

10 CFR Part 25

Classified information, Criminal penalties, Investigations, Reporting and recordkeeping requirements, Security measures.

10 CFR Part 95

Classified information, Criminal penalties, Reporting and recordkeeping requirements, Security measures.

For the reasons set out in the preamble and under the authority of the Atomic Energy Act of 1954, as amended, the Energy Reorganization Act of 1974, as amended, and 5 U.S.C. 553, the NRC proposes to adopt the following amendments to 10 CFR Parts 25 and 95.

PART 25 -- ACCESS AUTHORIZATION FOR LICENSEE PERSONNEL

1. The authority citation for Part 23 is revised to read as follows:

AUTHORITY: Secs. 145, 161, 68 Stat. 942, 948, as amended (42 U.S.C. 2165, 2201); sec. 201, 88 Stat. 1242, as amended (42 U.S.C. 5841); E.O. 10865, as amended, 3 CFR 1959 - 1963 COMP., p. 398 (50 U.S.C. 401, note); E.O. 12829; E.O. 12958; E.O. 12968

Appendix A also issued under 96 Stat. 1051 (31 U.S.C. 9701).

2. Section 25.1 is revised to read as follows:

§ 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.

3. Section 25.3 is revised to read as follows:

§ 25.3 Scope.

The regulations in this part apply to licensees and others who may require access to classified information related to a license or an application for a license.

4. Section 25.5 is amended by revising the ~~listed~~ definitions Access authorization and Need to know and by adding the definitions of Certificate holder, Classified information, Classified National Security Information, Cognizant Security Agency, and Visit authorization letters in alphabetical

order to read as follows:

§ 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.

* * * * *

Certificate holder means a facility operating under the provisions of Part 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 pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

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. The

Secretary of Defense (SECDEF) has been designated as Executive Agent for the National Industrial Security Program (NISP).

* * * * *

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.

* * * * *

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.

* * * * *

5. In § 25.8, paragraphs (a) and (b) are revised to read as follows:

§ 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 of 1995 (44 U.S.C. 3501 et seq.). The NRC may not conduct or sponsor a person and 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.

* * * * *

6. In §25.13, paragraph (a) is revised to read as follows:

§ 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

* * * * *

7. Section 25.15 is revised to read as follows:

§ 25.15 Access permitted under ``Q'', ``L'' or equivalent CSA access authorization.

(a) A ``Q'' or CSA equivalent access authorization permits an individual access on a need-to-know basis to Critical Secret Restricted Data and Secret and Confidential Classified National Security Information including intelligence information, CRYPTO (i.e., cryptographic information) or other classified communications security (COMSEC) information.

(b) An ``L'' or CSA equivalent access authorization permits an individual access on a need-to-know basis to Secret and Confidential classified 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 classified information to a Commission or CSA employee on official business when the employee has the appropriate level of access authorization and

need-to-know. Some individuals are permitted to begin NRC employment without an access authorization. However, no NRC or CSA employee is permitted access to any classified information until the appropriate level of access authorization has been granted to that employee by NRC or the CSA.

8. Section 25.17 is revised to read as follows:

§ 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 parts 50, 70, 72, or 76.

(b) The request must be submitted to the facility CSA. If NRC is the CSA, the procedures in §25.17(c) and (d) will be followed. If NRC is not the CSA, the request will be submitted to the CSA in accordance with procedures established by the CSA.

(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) Questionnaire for National Security Positions (SF - 86, parts 1 and 2);

(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 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) prior to submittal.

(f) Applications for access authorization or access authorization renewal processing that are submitted to NRC for processing must be accompanied by a check or money order, payable to the United States Nuclear Regulatory Commission, representing the current cost for the processing of each ``Q'' and ``L'' access authorization, or renewal request. Access authorization and access authorization renewal fees will be published each time the Office of Personnel Management notifies NRC of a change in the rates it charges NRC for the conduct of investigations. Any changed access authorization or access authorization renewal fees will be applicable to each access authorization or access authorization renewal request received upon or after the date of publication. Applications from individuals having current Federal access authorizations may be processed more expeditiously and at less cost, since the Commission may accept the certification of access authorization and investigative data from other Federal Government agencies that grant personnel access authorizations.

9. Section 25.19 is revised to read as follows:

§ 25.19 Processing applications.

Each application for access authorization or access authorization renewal must be submitted to the CSA. If NRC is the CSA, the application

and its accompanying fee must be submitted to the NRC Division of Security. If necessary, the NRC Division of 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 Security shall notify the submitter in writing and return the original application (security packet) and its accompanying fee.

10. Section 25.21 is revised to read as follows:

§ 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 NRC is the CSA, questions as to initial or continued eligibility will be determined in accordance with part 10 of Chapter I. ~~If NRC is not the CSA~~ 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. Such 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, NRC "Q" and "L" access authorizations must be renewed every five 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, 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 NRC to meet NRC's requirements. (The DOE Reinvestigation Program has been determined to meet 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 renewal submission and paperwork requirements, even if less than five years has passed since the date of issuance or renewal of the NRC "Q" or "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" or NRC "L" renewal application to NRC may not exceed seven 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 of the previous submission, shall submit a renewal application to NRC using the forms prescribed in § 25.17(d) before the expiration of the seven-year period.

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

11. Section 25.23 is revised to read as follows:

§ 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 prior to 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 Section 95.33 of thi 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 in which the determination was made as a result of a Personnel Security Hearing or by Personnel Security Review Examiners, or

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

12. Sections 25.25 is revised to read as follows:

§ 25.25 Cancellation of requests for access authorization.

When a request for an individual's access authorization or renewal of access authorization is withdrawn or canceled, the requestor shall notify the CSA immediately by telephone so that the full field investigation, National Agency Check with 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.

13. Section 25.27 is revised to read as follows:

§ 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 equivalents, 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 Sensitive Positions (SF - 86), or CSA equivalent, the individual must complete a personnel security packet (see Section 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 NRC is required.

14. Section 25.29 is revised to read as follows:

§ 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 is no known adverse information;

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

(4) 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 Acknowledgment will be obtained in all cases. Where personnel security packets are not required, a request for reinstatement shall state the level of access authorization to be reinstated and the full name and date of birth of the individual in order 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 NRC is required.

15. In §25.31, paragraphs (a) and (c) are revised to read as follows:

§ 25.31 Extensions and transfers of access authorizations.

(a) The NRC Division of 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.

* * * * *

(c) Requests for extension or transfer of access authorization shall state the full name of the person, his date of birth and level of access authorization. The Director, Division of 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 NRC is required.

* * * * *

16. Section 25.33 is revised to read as follows:

§ 25.33 Termination of access authorizations.

(a) Access authorizations will be terminated when:

(1) Access authorization is no longer required, or

(2) An individual is separated from the employment or the activity for which he 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 access authorization.

(b) A representative of the licensee or other organization which 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 access authorization is being terminated, and the reason; and that he will be considered for reinstatement of access authorization if he resumes work requiring it.

(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.

17. Section 25.35 is revised to read as follows:

§ 25.35 Classified visits.

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

(c) Licensee, certificate holder or others shall include the following information in 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 prior to 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 prior to the disclosure of any classified information.

PART 95--SECURITY FACILITY APPROVAL AND SAFEGUARDING OF NATIONAL SECURITY INFORMATION AND RESTRICTED DATA

18. The authority citation for Part 95 is revised Section continues to read as follows:

AUTHORITY: Secs. 145, 161, 68 Stat. 942, 948, as amended (42 U.S.C. 2165, 2201); sec. 201, 88 Stat. 1242, as amended (42 U.S.C. 5841); E.O. 10865, as amended, 3 CFR 1959-1963 COMP., p. 398 (50 U.S.C. 401, note); E.O. 12958; E.O. 12968; E.O. 12829.

19. Section 95.1 is revised to read as follows:

§ 95.1 Purpose.

The regulations in this part estab.ish procedures for obtaining security facility approval 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 witnin the scope of an NRC license or certificate.

19. Section 95.3 is revised to read as follows:

§ 95.3 Scope.

The regulations in this part apply to licensees, certificate holders and others regulated by the Commission who may require access to Classified National Security Information and/or Restricted Data 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.

20. In §95.5, the definitions for Authorized classifier, National Security Information, NRC access authorization, Security facility approval, and Security survey are removed and the definitions Classified mail address, Infraction, and Need to know are revised and the definitions Access authorization, Classified National security Information, Classified shipping address, Closed area, Cognizant Security Agency, Facility (Security) clearance, Foreign ownership control or influence, Restricted area, Security reviews, and Violation are added.

§ 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 of the NRC, or other person designated by the Executive Director for Operations, is eligible for a security clearance for access to Restricted Data or Classified National Security 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 National Security Information means information that has been determined pursuant to Executive Order 12958 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 ~~which due to its size, bulk, or nature~~ cannot be transmitted as normal mail~~, for the facility~~ 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 nonworking 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 to U.S. Industry. These agencies are the Department of Defense, the Department of Energy, the Central Intelligence Agency, and the Nuclear Regulatory Commission. The Secretary of Defense has been designated as Executive Agent for the National Industrial Security Program.

* * * * *

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 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, or its implementing directives, that does not comprise a "violation," as defined below.

* * * * *

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.

* * * * *

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.

* * * * *

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.

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 Executive Order 12958 or its implementing directives.

21. Section 95.8 is revised to read as follows:

§ 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 of 1995 (44 U.S.C. 3501 et seq.). 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 §§95.15, 95.18, 95.19, 95.21, 95.25, 95.29, ~~95.31~~95.33, 95.36, 95.37, 95.39, 95.41, 95.43, 95.45, 95.47, 95.53, 95.57.

22. In §95.13, paragraph (a) is revised to read as follows:

§ 95.13 Maintenance of records.

(a) Each licensee, certificate holder or other person granted facility clearance under this part shall maintain records prescribed within the part. These records are subject to review and inspection by CSA representatives during security reviews.

* * * * *

23. In §95.15, paragraphs (a) and (b) are revised to read as follows:

§ 95.15 Approval for processing licensees and others for facility clearance.

(a) A licensee, certificate holder or other person who has a need to use, process, store, reproduce, transmit, transport, or handle classified information at any location in connection with Commission related activities shall promptly request an NRC facility clearance.

(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 and 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 as required by §95.17(a).

* * * * *

24. Section 95.17 is revised to read as follows:

§ 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 and Procedure Plan that granting of the Facility Security Clearance would not be inconsistent with the national interest, including a finding that the facility is not under foreign ownership, control, or influence to a such a degree that such a determination could not be made;

(2) An acceptable security survey conducted by NRC;

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

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

(b) An interim Facility Security Clearance may be granted by the CSA on a temporary basis pending completion of the full investigative requirements.

25. Section 95.19 is redesignated as §95.20 and revised to read as follows:

§ 95.20 Grant, denial or termination of facility clearance .

The Division of Security shall provide notification in writing (or orally with written confirmation) to the licensee or other organization of the Commission's grant, acceptance of another agency's Facility Security Clearance, denial, or termination of facility clearance. This information must

also be furnished to representatives of NRC, NRC licensees, NRC Certificate Holders, NRC contractors, or other Federal agencies having a need to transmit classified information to the licensee or other person.

26. Section 95.18 is redesignated as §95.19 and the introductory text of paragraphs (a) and (b) are revised to read as follows:

§ 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 with copies to the Director, Division of Security, Office of Administration, NRC, Washington, DC 20555-0001, and the NRC Regional Administrator of the cognizant Regional Office listed in appendix A of part 73. The CSA shall promptly respond in writing to all such proposals. Some examples of substantive changes requiring prior CSA approval include--

* * * * *

(b) A licensee or other person may effect a minor, non-substantive change to an approved Standard Practice and Procedure Plan for the safeguarding of classified information without receiving prior CSA approval, provided prompt notification of such minor change is furnished to the addressees noted in paragraph (a) of this section, and the change does not decrease the effectiveness of the Standard Practice and Procedure Plan. Some examples of minor, non-substantive changes to the Standard Practice and Procedure Plan include--

* * * * *

27. A new §95.18 is added to read as follows:

§ 95.18 Key personnel.

The senior management official and the Facility Security Officer must always be cleared to the level of the Facility Security Clearance. Other key management officials, as determined by the CSA, must be granted a personnel security clearance 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 or partners (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 performance of higher-level classified contracts (specify higher level(s)). 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.

28. Section 95.21 is revised to read as follows:

§ 95.21 Withdrawal of requests for facility clearance.

When a request for facility clearance is to be withdrawn or canceled, the requester shall notify the NRC Division of Security immediately by telephone so that processing for this approval may be terminated. The notification must identify the full name of the individual requesting discontinuance, his position with the facility, and the full identification of the facility. The requestor shall confirm the telephone notification promptly in writing.

29. Section 95.23 is revised to read as follows:

§ 95.23 Termination of facility clearance.

(a) Facility clearance will be terminated when--

(1) There is no longer a need to use, process, store, reproduce, transmit, transport or handle classified matter at the facility; or

(2) The Commission makes a determination that continued facility clearance is not in the interest of national security.

(b) When facility clearance is terminated, the licensee or other person will be notified in writing of the determination and the procedures outlined in §95.53 apply.

30. In §95.25, paragraphs (a), (b), (c), (d), (g), (h), and (i) are revised and paragraph (j) is added to read as follows:

§ 95.25 Protection of classified information in storage.

(a) Secret documents, 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 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.

(2) Combinations must be changed by a person authorized access to the contents of the container, or by the Facility Security Officer or his or her designee. Combinations must be changed upon--

(i) The initial use of an approved container or lock for the protection of classified material;

(ii) The termination of employment of any person having knowledge of the combination, or when the clearance granted to any such person has been withdrawn, suspended, or revoked;

(iii) The compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended;

(iv) At other times when considered necessary by the Facility Security Officer or CSA; or

(v) In any event at least once every 12 months.

(d) Records of combinations. If a record is made of a combination, the record must be marked with the highest classification of material authorized for storage in the container. Superseded combinations must be destroyed.

* * * * *

(g) Posted information. Containers may not bear external markings indicating the level of classified material authorized for storage. A record of the names of persons having knowledge of the combination must be posted inside the container.

(h) End of day security checks.

(1) Facilities that store classified material shall establish a system of security checks at the close of each working day to ensure that all classified material and security repositories have been appropriately secured.

(2) Facilities operating with multiple work shifts shall perform the security checks at the end of the last working shift in which classified material had been removed from storage for use. The checks are not required during continuous 24-hour operations.

(i) Unattended security container found opened. If an unattended security container housing classified matter is found unlocked, the custodian or an alternate must be notified immediately. The container must be secured by protective personnel and the contents inventoried as soon as possible but not later than the next workday. A report reflecting all actions taken must be submitted to the responsible Regional Office (see appendix A, 10 CFR part 73 for addresses) with an information copy to the NRC Division of Security. The licensee shall retain records pertaining to these matters for three years after completion of final corrective action.

(j) Supervision of keys and padlocks. Use of key-operated padlocks are subject to the following requirements:

(1) A key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for protection of classified material;

(2) A key and lock control register must be maintained to identify keys for each lock and their current location and custody;

(3) Keys and locks must be audited each month;

(4) Keys must be inventoried with each change of custody;

(5) Keys must not be removed from the premises;

(6) Keys and spare locks must be protected equivalent to the level of classified material involved;

(7) Locks must be changed or rotated at least annually, and must be replaced after loss or compromise of their operable keys; and

(8) Master keys may not be made.

31. Section 95.27 is revised to read as follows:

§ 95.27 Protection while in use.

While in use, matter containing classified information 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).

32. Section 95.29 is revised to read as follows:

§ 95.29 Establishment of security areas.

(a) If, because of its nature, sensitivity or importance, matter containing classified information 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 such 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 such areas.

(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

contractual 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 security areas.

(5) Each individual authorized to enter a security 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. Entrances 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 material/information 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 non-working 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 documents in Closed Areas requires CSA approval. Only areas protected by an approved intrusion detection system will qualify for approval.

33. Section 95.31 is revised to read as follows:

§ 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 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 or other person possesses Critical Secret Restricted Data and the protective personnel require access as part of their regular duties.

34. Section 95.33 is revised to read as follows:

§ 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, and others performing security duties, complete security training deemed appropriate by the CSA. Training requirements must be based on the facility's involvement with classified information and may include a Facility Security Officer orientation course and, for Facility Security Officers at facilities with safeguarding capability, a Facility Security Officer Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of Facility Security Officer.

(b) Government-Provided Briefings. The CSA is responsible for providing initial security briefings to the Facility Security Officer, and for ensuring that other briefings required for special categories of information are provided.

(c) Temporary Help Suppliers. A temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, is responsible for ensuring that required briefings are provided to their cleared personnel. The temporary help supplier or the using licensee or other facility may conduct these briefings.

(d) Classified Information Nondisclosure Agreement (SF-312). 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 personnel security clearance must execute an SF-312 prior to being granted access to

classified information. The Facility Security Officer shall forward the executed SF-312 to the CSA for retention. If the employee refuses to execute the SF-312, the licensee or other facility 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.

(e) Initial Security Briefings. Before being granted access to classified information, an employee shall receive an initial security briefing that includes the following topics:

(1) A Threat Awareness Briefing.

(2) A Defensive Security Briefing.

(3) An overview of the security classification system.

(4) Employee reporting obligations and requirements.

(5) Security procedures and duties applicable to the employee's job.

(f) Refresher Briefings. The licensee or other facility shall conduct periodic refresher briefings for all cleared employees. As a minimum, the refresher briefing must reinforce the information provided during the initial briefing and inform employees of appropriate changes in security regulations. This requirement may be satisfied by use of audio/video materials and by issuing written materials on a regular basis.

(g) Debriefings. Licensee and other facilities shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's personnel security clearance is terminated, suspended, or revoked; and upon termination of the Facility Security Clearance.

(h) Records reflecting an individual's initial and refresher security orientations and security termination must be maintained for three years after

termination of the individual's access authorization.

35. Section 95.35 is revised to read as follows:

§ 95.35 Access to Classified Information

(a) Unless authorized by the Commission, a person subject to the regulations in this part may not receive or permit any individual to have access to Secret or Confidential National Security Information or Restricted Data unless the individual has:

(1) One of the following access authorizations.

(i) A U. S. Government granted access authorization based on a Single Scope Background Investigation and issued by the CSA which permits an individual access to--

(A) Critical Secret and Confidential Restricted Data; and

(B) Secret and Confidential National Security Information which includes intelligence information, CRYPTO (i.e., cryptographic information) or other classified communications security (COMSEC) information, or

(ii) A U. S. Government granted access authorization based on a National Agency Check or National Agency Check with Inquiries and issued by the CSA which permits an individual access to Secret and Confidential Restricted Data and Secret and Confidential National Security Information other than that noted in paragraph (a)(1)(i) of this section.

(iii) 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 information. (See

Definitions, §95.5).

(3) CSA approved storage facilities if classified documents or material are to be transmitted to the individual.

(b) Classified information must not be released by a licensee or other person to any personnel other than properly access authorized Commission licensee employees or other individuals authorized access by the Commission.

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

36. Section 95.36 is revised to read as follows:

§ 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 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 which is Classified 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, the information is information to which an inspector is entitled to have access under §75.42 of this chapter.

(c) In accordance with the specific disclosure authorization provided by the Division of Security, licensees or other persons subject to this part are authorized to release (i.e., transfer possession of) copies of documents which 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 organization in accordance with instructions contained in NRC's disclosure authorization letter. Licensees and other persons subject to this part may also forward these documents through NRC to the internationa organization's headquarters in accordance with the NRC disclosure authorization. Licensees 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 five years beyond the date of the visit or inspection. These records must specifically identify each document which has been released to an authorized representative and indicate the date of the release. These records must also identify (in such detail as the Division of Security, by letter, may require) the categories of documents to which the authorized representative has had access and the date of this access. A licensee or other person subject to this

part shall also retain Division of Security disclosure authorizations for five years beyond the date of any visit or inspection when access to classified information was permitted.

(e) Licensees 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.

37. In §95.37, paragraphs (a) and (b) are revised to read as follows:

§ 95.37 Classification and preparation of documents.

(a) Classification. Classified information generated or possessed by a licensee or other person must be appropriately marked. Information must be classified in accordance with classification guidance provided by NRC as part of the facility clearance process. 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 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 final determination should be made within 30 working days. The licensee or other person shall protect the document as classified information at the highest classification at issue while awaiting a final determination.

(b) Classification consistent with content. Each document containing

classified information shall be classified Secret or Confidential according to its content.

(1) For Original classification of Classified National Security Information:

(i) The identity of classifier and office of origin must be shown by the completion of ne "CLASSIFIED BY" line. The "CLASSIFIED BY" line must show the name or the personal identifiers, the position title of the classifier, and the agency or office of origin.

(ii) Reasons for Classification. The classifier shall identify the reason(s) for the decision to classify. The classification must include a brief reference to the pertinent classification category(ies), as identified in Executive Order 12958, Section 1.5, "Classification Categories."

(iii) Declassification Instructions. The duration of the original declassification decision must be placed on the "DECLASSIFY ON" line which will indicate one of the following:

(A) A date or event for declassification that corresponds to the information lapse from national security sensitivity (may not exceed 10 years from date of original classification decision); or

(B) A date that is 10 years from the date of the original decision; or

(C) A brief citation of the pertinent exemption category(ies) from section 1.6(d) of Executive Order 12958, if applicable (e.g., exemption will be identified by the letter "X" plus the identification of the exemption category).

(iv) Information determined to be exempted from declassification at 10 years will be identified by the letter "X" plus the identification of exemption category as identified in section 1.6(d) of Executive Order 12958.

(2) 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 that one source is cited, the "Derived From" line should indicate "Multiple Sources."

(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.

(A) If the document to be declassified contains the declassification instruction, "Originating Agency's Determination Required" (OADR), the document should reflect the date of the original classification of the information as contained in the source document or classification guide. An example might be as follows:

Declassify On: Source Marked :OADR"
Date of Origin: (Date)

(B) The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document.

(3) 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) Classification 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 either with:

(1) The classification marking assigned to the document, or

(2) The classification marking required by their content, 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:

Restricted Data

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.

Example

Pages 1-3 Secret

Pages 4-19 Unclassified

Pages 20-26 Secret

Pages 27-32 Confidential

(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 warrant 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. Persons in authorized possession of Classified National Security Information who in good faith believe that the information's classification status, whether classified or unclassified, is improper are expected to challenge its classification status. Persons who wish to challenge a classification status shall--

(i) 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.

(ii) In the event of a question regarding classification review, the holder of the information or the authorized classifier shall consult the NRC Division of Security, Information Security Branch for assistance.

(iii) Persons who challenge classification decisions have the right to appeal the classification decision to the Interagency Security Classification

Appeals Panel.

(iv) Persons seeking to challenge the classification of information will not be the subject of retribution.

(i) Files, folders or group of documents. Files, folders, binders, or groups of physically connected documents must be marked at least as high as the highest classified document which they contain. A document removed from the files, folders, binders or groups must be handled in accordance with the document's respective classification.

(j) Drafts and working papers. Drafts of documents and working papers which contain or which the originator believes contain classified information must be marked on the top and bottom of each page with the highest level of classification contained, or believed to be contained, and with the Restricted Data marking, if applicable. It is not required that other markings specified in §95.37(c) be applied or that an NRC Form 790 be prepared as indicated in §95.57(c) for drafts and working papers, provided they are not disseminated outside the facility. Prior to any dissemination outside of the facility, drafts and working papers must be reviewed by an authorized derivative classifier, final and complete classification markings applied, and an NRC Form 790 prepared and submitted to the NRC Division of Security, Washington, DC 20555-0001.

38. Section 95.39 is revised to read as follows:

§ 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 or certificate 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) They 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 mail address. The outer envelope or wrapper may not contain any classification, additional marking or other notation that indicates that the enclosed document contains classified information.

(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:

(i) U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail. NOTE: The "Waiver of Signature and Indemnity" block on the U.S. Postal

Service Express Mail Label 11-B may not be executed and the use of external (street side) express mail collection boxes is prohibited.

(ii) A cleared "Commercial Carrier."

(iii) A cleared commercial messenger service engaged in the intracity/local area delivery (same day delivery only) of classified material.

(iv) A commercial delivery company, approved by the CSA, that provides nation wide, overnight service with computer tracing and reporting features. Such companies need not be security cleared.

(v) Other methods as directed, in writing, by the CSA.

(2) Confidential matter may be transported by one of the methods set forth in paragraph (c)(1) of this section, by U.S. first class, express or certified mail. First class, express, or certified mail may be used in transmission of Confidential documents to Puerto Rico or any United States territory or possession.

(d) Telecommunication of classified information. Classified information may not be telecommunicated unless the telecommunication system has been approved by the CSA. Licensees, certificate holders or other persons who may require a secure telecommunication system shall submit a telecommunication plan as part of their request for facility clearance, as outlined in §95.15, or as an amendment to their existing Standard Practice and Procedure Plan for the protection of classified information.

(e) Security of classified information in transit. Classified matter that, because of its nature, cannot be transported in accordance with §95.39(c), may only be transported in accordance with procedures approved by

the CSA. Procedures for transporting classified matter are based on a satisfactory transportation plan submitted as part of the licensee's, certificate holder, or other person's request for facility clearance or submitted as an amendment to its existing Standard Practice Procedure Plan.

39. Section 95.41 is revised to read as follows:

§ 95.41 External receipt and dispatch records.

Each licensee, certificate holder or other person possessing classified information shall maintain a record that reflects:

(a) The date of the material;

(b) The date of receipt or dispatch;

(c) The classification;

(d) An unclassified description of the material; and

(e) The identity of the activity from which the material was received or to which the material was dispatched. Receipt and dispatch records must be retained for 2 years.

39. Section 95.43 is revised to read as follows:

§ 95.43 Authority to reproduce.

(a) Each licensee or other person possessing classified information shall establish a reproduction control system to ensure that reproduction of classified material is held to the minimum consistent with operational requirements. Classified reproduction must be accomplished by authorized

employees knowledgeable of the procedures for classified reproduction. The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified documents is encouraged.

(b) Unless restricted by the CSA, Secret and Confidential documents may be reproduced. Reproduced copies of classified documents are subject to the same protection as the original documents.

(c) All reproductions of classified material must be conspicuously marked with the same classification markings as the material being reproduced. Copies of classified material must be reviewed after the reproduction process to ensure that these markings are visible.

40. Section 95.45 is revised to read as follows:

§ 95.45 Changes in classification.

(a) Documents containing Classified National Security Information and/or Restricted Data must be downgraded or declassified as authorized by NRC classification guides or as determined by NRC. Requests for downgrading or declassifying any NRC classified information should be forwarded to the NRC Division of Security, Office of Administration, Washington, DC 20555-0001. Requests for downgrading or declassifying of Restricted Data will be coordinated as appropriate by the NRC Division of Security 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)

by authority of

---

(Person authorizing change in classification)

by

---

(Signature of person making change and date thereof)

(c) New markings reflecting the current classification status of the document will be applied in accordance with the requirements of §95.37.

(d) Any persons making a change in classification or receiving notice of such a change shall forward notice of the change in classification to holders of all copies as shown on their records.

41. Section 95.47 is revised to read as follows:

§ 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. If the document contains Secret information a record of the subject or title, document number, if any,

originator, its date of origination and the date of destruction must be signed by the person destroying the document and must be maintained in the office of the custodian at the time of destruction. These destruction records must be retained for two years after destruction.

42. Section 95.49 is revised to read as follows:

§ 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 or other person's request for facility clearance outlined in §95.15 or submitted as an amendment to its existing Standard Practice and Procedure Plan for the protection of classified information .

43. Section 95.51 is revised to read as follows:

§ 95.51 Retrieval of classified matter following suspension or revocation of access authorization.

In any case where the access authorization of an individual is suspended or revoked in accordance with the procedures set forth in part 25 of this chapter, or other relevant CSA procedures, the licensee, certificate holder or other organization shall, upon due notice from the Commission of such suspension or revocation, retrieve all classified information possessed by the

individual and take the action necessary to preclude that individual having further access to the information.

45. Section 95.53 is revised to read as follows:

§ 95.53 Termination of facility clearance.

(a) If the need to use, process, store, reproduce, transmit, transport, or handle classified matter no longer exists, the facility clearance will be terminated. The facility may deliver all documents and materials containing classified information to the Commission or to a person authorized to receive them or destroy all such documents and materials. In either case, the facility shall submit a certification of nonpossession of classified information to the NRC Division of Security.

(b) In any instance where facility clearance has been terminated based on a determination of the CSA that further possession of classified matter by the facility would not be in the interest of the national security, the facility shall, upon notice from the CSA, immediately deliver all classified documents and materials to the Commission along with a certificate of nonpossession of classified information.

46. Section 95.55 is revised to read as follows:

§ 95.55 Continued applicability of the regulations in this part.

The suspension, revocation or other termination of access authorization or the termination of facility clearance does not relieve any person from

compliance with the regulations in this part.

47. Section 95.57 is revised to read as follows:

§ 95.57 Reports.

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

(a) Any alleged or suspected violation of the Atomic Energy Act, Espionage Act, or other Federal statutes related to classified information.

(b) Any infractions, losses, compromises or possible compromise of classified information or classified documents not falling within paragraph (a) of this section.

(c) In addition, a licensee, certificate holder or other organization's authorized classifier shall complete an NRC Form 790 (Classification Record) whenever a document containing classified information is generated, its classification is changed or it is declassified. Notification of declassification is not required for any document or material which has an automatic declassification date. Completed NRC Forms 790 must be submitted to the NRC Division of Security, Washington, DC 20555-0001, on a monthly basis.

48. Section 95.59 is revised to read as follows:

§ 95.59 Inspections.

The Commission shall make inspections and surveys of the premises,

activities, records and procedures of any 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.

Dated at Rockville, Maryland, this _____ day of _____ , 1996.

For the Nuclear Regulatory Commission.

_____

James M. Taylor,
Executive Director for Operations.

# REGULATORY ANALYSIS

1. Statement of Problem

On October 31, 1994, the Deputy Secretary of Defense, acting as the Executive Agent for the National Industrial Security Program (NISP), approved the NISP Operating Manual (NISPOM) establishing government-wide requirements for the protection of Classified National Security Information and Restricted Data at industrial facilities, including NRC contractors, and, to the extent feasible within regulatory requirements, NRC licensees and certificate holders. On April 17, 1995 and August 2, 1995, the President signed Executive Orders 12958, "Classified National Security Information," and 12968, "Access to Classified Information," respectively which revised requirements for handling, protecting and accessing classified information. The requirements of these new national security policy documents are applicable to licensees, certificate holders, and others regulated by NRC. The effect of the new Executive Orders and the NISPOM is that 10 CFR Part 25, "Access Authorization for Licensee Personnel," and 10 CFR Part 95, "Security Facility Approval and Safeguarding of National Security Information and Restricted Data," are no longer consistent with national security policies and directives.

2. Objective

The objective of this regulatory initiative is to conform NRC's regulations for the protection of classified information at licensee, certificate holder and other NRC regulated facilities possessing or having employees with access to classified information, with national policies for the protection of such information.

3. Alternatives

There is no reasonable alternative to the revision of these regulations that would achieve the desired result.

4. Consequences

There are approximately 10 affected entities licensed or otherwise regulated by the NRC. Each licensee, certificate holder or other entity who requires access to National Security Information or Restricted Data to conduct official business related to an NRC regulated activity must have a facility clearance under the provisions of Part 95 and individuals, other than USEC personnel who are cleared by DOE, who have access to classified information must have a personnel security clearance granted to them under Part 25 by NRC.

These entities will be required to comply with the requirements of 10 CFR Parts 25 and 95, which will involve costs to these entities. The costs, however, should be no higher than under the current regulations and are likely to be lower since a number of requirements have been reduced (e.g., lesser requirements for accountability of secret information, reduction of requirements for GSA approved security containers and reduction of administrative requirements for classified visits.) These changes will