ROUTING AND RECORD SHEET

SUBJECT: (Optional)

File Physical Security Talk

FROM: [redacted]
Acting Chief, Policy and Plans Group
Office of Security, 4E-70, Hdqs.

EXTENSION: 5311

NO.

DATE: 2 JUL 1979

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. SECOM Attn: [redacted] 3D-39, Hdqs.	3 JUL 1979			1. Thought you might be interested in the attached DOE proposal on safeguarding restricted data. [redacted] STAT [redacted] STAT
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

NOTE - Page 2 discusses [illegible] a security [illegible] a security inspection [illegible]

DEPARTMENT OF ENERGY

Office of the Secretary

[10 CFR Part 795]

Safeguarding of Restricted Data

AGENCY: Department of Energy (DOE).

ACTION: Proposed Rule.

SUMMARY: The Department of Energy proposes a revision of 10 CFR Part 795 which concerns the requirements for the safeguarding and transmission of Secret and Confidential Restricted Data. Part 795 is applicable to all persons who receive or generate Restricted Data under an Access Permit issued pursuant to the regulations in Part 725 "Permits for access to Restricted Data" of 10 CFR, Chapter III.

Continual upgrading of security procedures by DOE, both for DOE held Restricted Data and that data held by DOE contractors, has left a considerable gap between these procedures and Part 795. In addition, areas such as automatic data processing systems are not within the scope of the present Part 795. In an effort to update and upgrade Part 795, this revision is proposed.

The changes vary in complexity and relate in general to the following matters: new definitions; submission of procedures by access permit holders; protection of Restricted Data in storage; establishment of security areas; qualification of protective personnel; certification of DOD and NASA personnel; preparation and transmission of classified documents; shipment of classified material; security of automatic data processing systems; and reports on foreign travel.

DATES: Comments must be received on or before July 11, 1979.

ADDRESSES: Comments should be sent to George Weisz, Director, Office of Safeguards and Security, Department of Energy, 20 Massachusetts Avenue, NW, Washington, D.C. 20545, (301) 353-5108.

FOR FURTHER INFORMATION CONTACT: W. J. Gilbert, Jr., Chief, Programs and Policy Branch, Office of Safeguards and Security, U.S. Department of Energy, Washington, D.C. 20545, 301/353-5690.

SUPPLEMENTARY INFORMATION: Significant changes to 10 CFR Part 795 which would be effected by the proposed revision are as follows:

1. "ERDA" and the titles of former ERDA officials would be changed to "DOE" and the titles of comparable DOE officials throughout the Part.

2. Definitions of the following terms would be added for clarity of the succeeding text.

§ 795.3(c) Automatic data processing system
(d) Authorized derivative classifier
(e) Data
(j) General Counsel
(k) Guard
(l) Information
(n) Material
(o) Matter
(s) Protective Personnel
(x) Security container
(y) Security inspector

3. The requirements of § 795.21(a) and 795.21(b) for protection of Restricted Data in storage would be upgraded for comparability with DOE standards established under the authority of the Atomic Energy Act of 1954, as amended.

4. New § 795.21(f) and 795.21(g) would provide additional procedural guidance for the selection and administrative control of lock combinations.

5. New § 795.21(h), 795.21(i), and 795.21(j) would provide additional procedural guidance for the surveillance and protection of unattended security repositories.

6. New § 795.25(c) and 795.25(e) would provide qualification standards for security inspectors employed for the protection of Restricted Data.

7. Section 795.31 would be revised to provide amplified guidance for the control of access to Restricted Data by employees of the DOD or NASA.

8. Sections 795.32(c), 795.32(d), and 795.32(e) would be revised to provide amplified guidance for the classification marking of Restricted Data documents, including drafts and letters of transmittal.

9. Section 795.33(d) would be revised to delete methods of transportation no longer available, to add additional authorized alternate methods of transportation, and to provide additional guidance for the protection of Restricted Data in transit.

10. New § 795.38 would add the requirement that ADP systems used for processing of Restricted Data must be approved by DOE.

11. New § 795.43(c) would require reports to DOE of travel to Soviet-bloc countries by Access Permittee employees who have had access to C-24 category of information.

Interested persons are invited to submit written comments with respect to the proposed regulations to the address provided above. Comments should be identified on the outside of the envelope and on the documents submitted to DOE with the designation "Safeguarding of Restricted Data." Fifteen (15) copies should be received by DOE by the deadline specified, in order to ensure consideration.

In accordance with section 501(c)(1) of the Department of Energy Organization Act, DOE has determined that these regulations present no substantial issue of fact or law, and are unlikely to have a substantial impact on the economy or large numbers of individuals or businesses. Accordingly, no public hearing is required.

Since this document is unlikely to have any significant effect on the environment, DOE has determined that the provisions of section 7(a)(2) of the Federal Energy Administration Act, as amended, requiring that proposals having such effect be submitted to the Environmental Protection Agency for review and comment, does not apply.

DOE has determined that this document does not contain a major proposal requiring preparation of an inflation impact statement under Executive Order 11821 and OMB Circular A-107.

(Atomic Energy Act of 1954, as amended, Section 161.i., 68 Stat. 948, 42 U.S.C. 2201; Energy Reorganization Act of 1974, Section 104, 88 Stat. 1237, 42 U.S.C. 5814 and Section 105, 88 Stat. 1238, 42 U.S.C. 5815; Department of Energy Orgnization Act, Section 301, 91 Stat. 577, 42 U.S.C. 7140 and Section 641, 91 Stat. 598, 42 U.S.C. 7251)

Dated at Washington, D.C. this 14, of May 1979.

Duane C. Sewell,

Assistant Secretary for Defense Programs.

In accordance with the foregoing, it is proposed that Part 795 of 10 CFR Chapter III, be revised as set forth below.

PART 795—SAFEGUARDING OF RESTRICTED DATA

General Provisions

Sec.
795.1 Purpose.
795.2 Scope.
795.3 Definitions.
795.4 Communications.
795.5 Submission of procedures by Access Permit holder.
795.6 Specific waivers.
795.7 Interpretation.

Physical Security

795.21 Protection of Restricted Data in storage.
795.22 Protection while in use.
795.23 Establishment of security areas.
795.24 Special kinds of classified material.
795.25 Protective personnel.

Control of Information

795.31 Access to Restricted Data.
795.32 Classification and preparation of documents.

Authority: The provisions of Part 795 are issued under the Atomic Energy Act of 1954, as amended, section 161.i., 68 Stat. 948, 42 U.S.C. 2201; Energy Reorganization Act of 1974, section 104, 88 Stat. 1237, 42 U.S.C. 5814 and section 105, 88 Stat. 1238, 42 U.S.C. 5815; Department of Energy Organization Act, section 301, 91 Stat. 577, 42 U.S.C. 7130 and section 641, 91 Stat. 598, 42 U.S.C. 7251].

General Provisions

§ 795.1 Purpose.

The regulations in this part establish requirements for the safeguarding of Secret and Confidential Restricted Data received or developed under an Access Permit. This part does not apply to other categories of classified information.

§ 795.2 Scope.

The regulations in this part apply to persons who receive access to Restricted Data or develop Restricted Data under an Access Permit issued in accordance with the regulations in Part 725 of this chapter.

§ 795.3 Definitions.

(a) "Access authorization" means an administrative determination by DOE that an employee of DOE, a DOE contractor or subcontractor, an employee of a contractor or subcontractor of another Federal agency, an Access Permittee, or an employee of an Access Permittee is eligible for access to Restricted Data.

(b) "Act" means the Atomic Energy Act of 1954 (68 Stat. 919), including any amendments thereto.

(c) "Automatic data processing" means data processing largely performed by an automatic system of electronic or electrical machines including input, processing, and output operations.

(d) "Authorized Derivative Classifier" means an individual who has been designated and authorized by competent Department of Energy (DOE) authority to classify information, work projects, [illegible] Secret or Confidential Restricted Data.

(e) "Data" means all information and material containing Restricted Data, including any such facts or concepts set forth by an ADP system.

(f) "Document" means any piece of recorded information regardless of its physical form or characteristics.

(g) "DOD" means the Department of Defense or its duly authorized representatives.

(h) "DOE" means the Department of Energy or its duly authorized representatives.

(i) "DOE approved" means approved by the responsible DOE safeguards and security office.

(j) "General Counsel" is the principal Attorney of the Department of Energy.

(k) "Guard" means an individual, not necessarily uniformed, who is employed for, and charged with, the protection of classified matter or Government property. Guards shall be armed with non-lethal weapons such as billy-club, "Stun-Gun", or aerosol irritants.

(l) "Information", when automatic data processing is involved, means a representation of facts or concepts producted by an ADP system.

(m) "L(X) access authorization" means a determination by DOE that an individual is eligible for access to Confidential Restricted Data under an Access permit.

(n) "Material" means chemical substances, fabricated items, assemblies, machinery, or equipment.

(o) "Matter" means documents or material.

(p) "NASA" means the National Aeronautics and Space Administration or its duly authorized representatives.

(q) "Permittee" means the holder of an Access Permit issued pursuant to the regulations in part 725 of this chapter.

(r) "Person" means (1) any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, Government agency other than DOE, any State or any political subdivision of, or any political entity within a State, or other entity; and (2) any legal successor, representative, representative, agent or agency of the foregoing.

(s) "Protective personnel" means guards or security inspectors.

(t) "Q(X) access authorization" means a determination by DOE that an individual is eligible for access to Secret and Confidential Restricted Data under an Access Permit.

(u) "Restricted Data" means all data concerning (1) design, manufacture or utilization of atomic weapons; (2) the production of special nuclear materia[l] [illegible] of special nuclear mater[ial] in the production of energy, but shall include data declassified or removed from the Restricted Data category pursuant to section 142 of the Act.

(v) "Security area" means a physica[l] defined space containing classified matter and subject to physical protection and personnel access contr[ol].

(w) "Security clearance" means an administrative determination by DOE that an employee of another Federal government (as opposed to state and local) agency is eligible for access to Restricted Data.

(x) "Security container" means any the following repositories:

(1) *A security filing cabinet*—a met[al] security container of a type approved the General Services Administration f[or] the storage of classified matter and marked "General Services Administration Approved Security Container". This container meets the Class 1 standards of Federal Specification AA-F-357, the Class 5 standards of Federal Specification AA-F-358, or the Class 5 standards of Federal Specification AA-F-363.

(2) *A safe*—a metal security contain[er] of a type approved by the General Services Administration for the storag[e] of classified matter and marked "General Services Administration Approved Security Container", this container meets the standards of Federal Specification AA-S-1518A.

(3) *A vault*—a penetration-resistant, windowless enclosure which: (i) has walls, floor, and ceiling substantially constructed of materials which afford forced penetration resistance at least equivalent to that of 8 inch thick reinforced concrete; (ii) has any openings greater than 96 square inches in area and over 6 inches in the smalle[st] dimension protected by imbedded stee[l] bars at least ⅝ inches in diameter on 6 inch centers both horizontally and vertically; (iii) has a built-in combination locked steel door which in existing structures is at least 1" thick exclusive of bolt work and locking devices and which for new structures a least meets the class 5 standards of Federal Specification AA-D-600B.

(4) *A security room*—one having combination-locked door(s) and protected by a DOE-approved intrusion alarm system actuated by any penetration of walls, floor, ceiling or openings, or by motion within the room.

(y) "Security inspector" means a uniformed individual who is authorized under appropriate state or local authority to carry firearms and who is

employed for, and charged with, the protection of classified matter.

(z) "United States" when used in geographical sense, includes all Territories and Possessions of the United States, the Canal Zone and Puerto Rico.

§ 795.4 Communications.

Communications concerning rule making, i.e., petition to change Part 795, should be addressed to the Assistant Secretary for Defense Programs, U.S. Department of Energy, Washington, D.C. 20545. All other communications concerning the regulations in this part should be addressed to the Department of Energy at the USDOE Operations Office (listed in Appendix "B" of 10 CFR Part 725) administering access permits for the geographical area.

§ 795.5 Submission of procedures by Access Permit holder.

A Permittee is granted access to Restricted Data only after:

(a) submission to the Department of Energy field office administering the permit of a copy of his procedures for the safeguarding of Restricted Data and for the safeguards and security education of his employees, and

(b) Determination by the Manager of the Field Office or his designee and advice in writing to the Permittee that the procedures for the safeguarding of Restricted Data comply with the regulations in this part and the procedures for the safeguards and security education of employees assure that all employees who will have access to Restricted Data will be informed about and understand the regulations in this part.

§ 795.6 Specific waivers.

DOE may, upon application of any interested party, grant such waivers from the requirements of this part as it determines are authorized by law and will not constitute and undue risk to the common defense and security.

§ 795.7 Interpretation.

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

Physical Security

§ 795.21 Protection of restricted data in storage.

(a) Persons shall store Secret Restricted Data documents or material received under an Access Permit, while unattended or not in use, by one of following methods:

(1) When not located within a security area:

(i) In a security container under either DOE-approved alarm protection or protective personnel (security inspector or guard) patrols no less frequent than once each 8-hour shift during non-working hours, or

(ii) In a dual-key bank safe deposit box, provided that the lock and keys to the box are changed immediately prior to such use and the customer's keys are furnished only to persons cleared for and authorized access to the Restricted Data in the box.

(2) When located within a security area:

(i) In a security container or a commercial-type steel filing cabinet equipped with a built-in combination lock, provided the container or the cabinet is equipped with a DOE-approved alarm system or is under protective personnel patrol no less frequent than once every 8 hours during non-working hours.

(ii) In unlocked cabinets or open storage in a DOE-approved vault or security room.

(b) Confidential Restricted Data documents or material while unattended or not in use shall be stored:

(1) Under any of the methods used for Secret Restricted Data documents or material as set forth in paragraph (a) of this section, or

(2) In unlocked cabinets or open storage in a locked room equipped with a DOE-approved alarm system.

(c) *Changes of combinations.* (1) Combinations of locks of repositories containing Restricted Data shall be known only to those persons cleared for and otherwise authorized access to the category of Restricted Data stored therein.

(2) Each Permittee shall change the combination on the lock of a repository:

(i) Whenever the repository is placed in use;

(ii) Whenever a person knowing the combination no longer requires access to a repository. This may be as a result of a change in duties or location in the permittee's organization or termination of employment with the permittee;

(iii) Whenever the combination may have been subjected to compromise; and

(iv) In any event at least once a year.

(d) The record of the combination of a lock on a repository shall be controlled and afforded the same level of security protection required for the highest classification of the matter authorized to be stored in the repository.

(e) *Selection of combinations.* Each combination must require the use of three different numbers. In selecting combinations, multiples and a simple arithmetical ascending or descending series shall be avoided.

(f) *Cautions regarding combinations.* (1) Only a minimum number of persons should possess combinations to repositories.

(2) Combinations should be committe to memory insofar as practicable to reduce possibility of inadvertent compromise.

(3) When closing a combination lock, the dial must be turned at least four times in the same direction.

(4) Combinations shall be changed only by persons authorized access to Secret or Confidential Restricted Data depending upon the matter authorized be stored in the repository.

(g) *Posted information.* (1) The name addresses, and telephone numbers of custodians having knowledge of the combination shall be posted on the outside of each repository containing Restricted Data. A record of the date o last change of combination of each repository shall be maintained on each repository.

(2) A monitor sheet shall be posted the security container approved for the storage of Restricted Data. In any situation when one monitor sheet includes several security containers located in a particular space or room, shall be posted in an easily viewed place within, or at the entrance to, the room or space involved. The monitor sheet shall contain space for the date and initials of the persons locking and checking the container to assure it is secured. It shall be initialed at the end of each work day by the person lockin the container(s) and except when not feasible, by one other person who has physically checked the lock(s), locked drawer(s), or door(s) and all exposed drawers to assure proper security of t container(s).

(h) *Unattended repository found op* In the event that an unattended repository containing Restricted Data found unlocked, one of the custodians shall be notified immediately, the repository shall be secured by a designated person (e.g., a security inspector or guard) and the contents shall be checked not later than the ne workday.

(i) *Security Container Checks.* Whenever protective personnel are required by §§795.21 or 795.23, they shall, as soon as possible after the cl of each normal work day, and, thereafter, at least once every 24 hou of a nonworking period exceeding on

day, physically check each approved security container to assure it is properly secured.

§ 795.22 Protection while in use.

While in use, documents and material containing Restricted Data shall be under the direct control of an appropriately cleared individual and the Restricted Data shall be protected from visual access by unathorized persons.

§ 795.23 Establishment of security areas.

(a) When, because of their nature, size, revealing characteristics, sensitivity or importance, documents or material containing Restricted Data cannot otherwise be effectively controlled in accordance with the provisions of §§ 795.21 and 795.22, a security area to protect such documents and material shall be established.

(b) The following controls shall apply to security areas:

(1) Security areas shall be separated from adjacent areas by a physical barrier designed to prevent entrance into such areas, and access to the Restricted Data within the areas, by unauthorized individuals.

(2) During working hours, admittance shall be controlled by designated appropriately cleared security inspectors, guards, receptionists or other persons assigned for that purpose at each unlocked entrance. Remote identification by television, or coded key card system, may be used where positive identification and access control is assured.

(3) During non-working hours, security areas shall be protected by protective personnel conducting patrols at such frequency, not less than once every 8 hours, as the responsible field office manager deems necessary, or by a DOE-approved alarm system.

(4) Each individual authorized to enter a security area shall be issued a distinctive badge or pass when the number of employees assigned to the area exceeds thirty.

§ 795.24 Special kinds of classified material.

When the Restricted Data contained in material is not ascertainable by observation or examination at the place where the material is located and when the material is not readily removable because of size, weight, radioactivity, or similar factors, DOE may authorize the Permittee to provide such lesser protection than is otherwise required by §§ 795.21 to 795.23, inclusive, as DOE determines to be commensurate with the difficulty of removing the material.

§ 795.25 Protective personnel.

Whenever protective personnel are [illegible] § 795.23(b)(3), they shall:

(a) Possess a "Q", "Q(X)", "L" or "L(X)" access authorization if the Restricted Data being protected is classified Confidential.

(b) Possess a "Q" or "Q(X)" access authorization if the Restricted Data being protected is classified Secret.

(c) Be mentally and physically alert, capable of exercising good judgment, and fully instructed in their duties.

(d) Security inspectors should be armed with side arms of not less than .38 caliber.

(e) Security inspectors shall be initially trained, and refresher trained at least annually, in the safe handling and proficient use of the type of handgun with which they are armed while on duty, and to the extent of their legal authority to act in the protection of classified matter. Records of such training shall be maintained during the tenure of the individual.

Control of Information

§ 795.31 Access to restricted data.

(a) Except as DOE may authorize, no person subject to the regulations in this part shall receive or shall permit any individual to have access to Secret or Confidential Restricted Data in his possession, unless the individual has a "Q" or "Q(X)" access authorization, in the case of Secret Restricted Data, "Q", "QX", or "L" or "LX" access authorization in the case of Confidential Restricted Data and:

(1) The individual is authorized by an Access Permit to receive Restricted Data in the categories and at the classification levels involved.

(2) In the case of a DOE or DOE contractor or subcontractor employee, the individual needs access to the Secret or Confidential Restricted Data in connection with his duties.

(b) As an alternative to DOE access authorization, Department of Defense (DOD) and National Aeronautics and Space Administration (NASA) personnel, officers or employees of one of the services, officers or employees of DOD, NASA, or service contractors or subcontractors, or members of the Armed Forces may be granted access if a request set forth in paragraph (c) of this section is received from DOD or NASA. As an exception, DOE access authorization is required for access by NASA personnel to Restricted Data other than that associated with space or aeronautical programs or activities.

(c) Prior to granting access to individuals referenced in paragraph (b) [illegible] Request for Visit or Access Approval (Form DOE-277), NASA Form 405, or a memorandum or teletype containing the same information, signed by an authorized certifying official will be forwarded for approval to the field office manager who will coordinate with other offices as necessary.

(d) Inquiries concerning the security clearance or access authorization status of individuals, the scope of Access Permits, or the nature of contracts should be addressed to the field office administering the Access Permit or the contract.

§ 795.32 Classification and preparation of documents.

(a) *Classification.* Restricted Data originated by an Access Permit holder must be appropriately classified. "Guide to the Unclassified fields of Research," and other appropriate guides issued by the U.S. DOE Office of Classification, will be furnished each Permittee. In the event an Access Permit holder originates information within the definition of Restricted Data (§ 795.3(u)) or information which he is not positive is not within that definition and the guide does not provide positive classification guidance for such information, he shall mark and handle the information as Confidential Restricted Data and request classification guidance from DOE through the Classification Officer at the Operations Office administering the Permit, who will refer the request to the Director, Office of Classification, U.S. Department of Energy, Washington, D.C. 20545, if he does not have authority to provide the guidance.

(b) *Classification consistent with content.* Each document containing Restricted Data shall be classified Secret or Confidential according to its own content.

(c) *Classification markings.* The highest classification marking assigned to any portion of a document shall be placed in letters not less than one-quarter inch in height at the top and bottom of the outside of the front covers, on title pages, if any, the first page, the back page and on the outside of the back cover, if any.

(d) The balance of the pages shall be marked at the top and bottom either with:

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

(2) the classification marking required by their individual content, or

(3) the marking Unclassified when they have no classified content.

(e) The document shall bear the following additional marking on the first page and on the front cover:

Restricted Data

This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions.

(f) Where the originator of the document is not an authorized derivative classifier, or is not responsible for the classification, the words "DERIVATIVELY CLASSIFIED BY" shall be typed on the face of the document followed by the name, title of position, and organization employing the authorized derivative classifier. The authorized derivative classifier shall sign when feasible.

(g) *Documentation.*

(1) All Secret Restricted Data documents shall bear on the first page a properly completed documentation stamp such as the following:

This document consists of —— pages. Copy No. —— of —— Series ——.

(2) The series designation for finished copy shall be a capital letter beginning with the letter "A" designating the original set of copies prepared. Each subsequent set of copies of the same document shall be identified by the succeeding letter of the alphabet. The series designation for draft copies shall be identified in progressive numerical sequence, as "Draft 1", "Draft 2", etc.

(h) *Letter of transmittal.* (1) A transmittal letter containing no Restricted Data or other Classified information should be marked with the following markings:

(i) "Restricted Data transmittal" or "Document transmitted herewith contains Restricted Data",

(ii) With a classification at least as high as its highest classified enclosure, and

(iii) A stamp or marking such as the following:

When separated from enclosures handle this document as unclassified.

(2) A transmittal letter containing Restricted Data should be marked as follows:

(i) "Restricted Data" on its first page.

(ii) A classification at least as high as its highest classified enclosure or the classification of the letter itself, whichever is higher.

(iii) When the contents of the letter of transmittal warrant a lower classification, a stamp or marking such as the following:

this document as (*lower classification*).

§ 795.33 External transmission of documents and material.

(a) *Restrictions.* (1) Documents and material containing Restricted Data shall be transmitted only to persons who possess appropriate security clearances or access authorization and are otherwise eligible for access under the requirements of § 795.31.

(2) In addition, such documents and material shall be transmitted only to persons who possess DOE-approved facilities for their physical security consistent with this part. Any person subject to the regulations in this part who transmits such documents or material shall have fulfilled his obligations under this subparagraph by securing a written certification from the responsible DOE safeguards and security office that the prospective recipient possesses DOE-approved facilities for physical security thereof consistent with this Part.

(3) Documents and material containing Restricted Data shall not be exported from the United States without prior authorization of DOE.

(b) *Preparation of documents.* Documents containing Restricted Data shall be prepared for transmission outside an individual installation in accordance with the following:

(1) They shall be enclosed in two sealed opaque envelopes or wrappers.

(2) The inner envelope or wrapper shall be addressed in the ordinary manner and sealed with tape. The appropriate classification and the Restricted Data marking referred to in § 795.32(e) shall be placed on both sides of the inner envelope.

(3) The outer envelope or wrapper shall be addressed in the ordinary manner. No classification, additional marking or other notation shall be affixed which indicates that the document enclosed therein contains classified information or Restricted Data.

(4) A receipt, which identifies the document, the date of transfer, the recipient and the person transferring the document shall accompany the document and shall be signed by the recipient and returned to the sender whenever the custody of a Secret document is transferred.

(c) *Preparation of material.* Material, other than documents, containing Restricted Data shall be prepared for shipment outside an individual installation in accordance with the following:

shall be so packaged that the classified characteristics will not be revealed.

(2) A receipt which identifies the material, the date of shipment, the recipient, and the person transferring the material shall accompany the material and the recipient shall sign such receipt and return it to the sender whenever the custody of Secret Restricted Data is transferred.

(d) *Methods of transportation.* (1) Documents and material containing Secret Restricted Data shall be transported only by one of the following methods:

(i) U.S. registered mail.

(ii) Individuals possessing appropriate DOE security clearance or access authorization who have been given written authority by their employers, in cases of operational necessity when U.S. registered mail or classified messenger service is not available or sufficiently timely. The office of departure shall keep a record of the classified matter so transported until the matter has been returned or a classified matter receipt has been received from a consignee.

(iii) Aircraft under DOE contract with pilots holding "Q" access authorization, or U.S. Government aircraft with pilots holding DOE "Q" access authorization or DOD final type Secret clearance, and who maintain continuous custody of the matter entrusted to them.

(iv) Motor vehicles in sealed van service.

(v) Common carrier (rail, truck, or air) approved by the responsible field office manager and meeting the requirements of paragraph (d)(3)(xi) of this section.

(2) Documents and material containing Confidential Restricted Data shall be transported by one of the methods set forth in paragraph (d)(1) of this section or by one of the following methods:

(i) U.S. first class or certified mail, if approved by the Field Office Manager administering the permit. Certified or first class mail may not be used in any transmission of Confidential documents to Alaska, Hawaii, the Canal Zone, Puerto Rico, or any United States territory or possession.

(ii) Aircraft under DOE contract, or U.S. Government aircraft, with pilots holding DOE "L" access authorization or DOD final type Secret clearance.

(iii) Common carrier service (rail, truck, or air) as approved by the field office manager and meeting the requirements of subparagraph (3)(xi) below.

(3) Approved means of shipment for Restricted Data are subject to the

following additional general conditions as appropriate.

(i) Contents shall be packaged, and as required contai[illegible] shall meet appropriate Department of Transportation regulations as to structural strength and materials.

(ii) Contents shall be so packaged that attempted openings or unauthorized inspection will be readily detected en route or upon arrival at destination.

(iii) Contents shall be checked against shipping papers as promptly as practicable after arrival and any unresolved discrepancy shall be reported immediately to the responsible DOE safeguards and security office.

(iv) Additionally, any suspected criminal violations of federal laws or loss of Secret or confidential material outside a security area or loss within a security area if there is no immediate explanation to account for the loss shall be reported to the responsible DOE security office and the Federal Bureau of Investigation.

(v) The classification of the contents shall be indicated inside the package or container to preclude errors in handling and storage after delivery.

(vi) Seals shall be used whenever practicable and shall be placed on cars or van doors, containers, or other positive fastening devices by, or in the presence of a DOE, DOE contractor representative or security cleared permittee employee. Seals shall be serially numbered or distinctively designed and appropriate entry shall be made in bills of lading or other shipping papers. Seal numbers shall be verified by the consignee upon arrival.

(vii) Combination or key padlocks shall be used whenever practicable on shipping containers in addition to seals.

(viii) Receipts, listings, and other papers revealing classified information shall be appropriately marked and wrapped.

(ix) shipping or transfer documents which could reveal classified weights or quantities of material shall be appropriately marked.

(x) Notification of Secret or Confidential Restricted Data shipments, other than packages sent by mail, shall be transmitted prior to departure either to the consignee or to the DOE office exercising administrative jurisdiction over the consignee, with sufficient information to enable proper handling at destination.

(xi) Common carriers shall provide all of the following security procedures:

(A) Surveillance by an authorized carrier employee when the material is outside of the vehicle.

(B) A hand-to-hand signature receipt system which traces the movement of [illegible] shipped until the time it is received.

(C) When storage is required, Restricted Data must be stored in an alarmed or guarded storage area with immediate response by a carrier employee, commercial guard, or police.

(D) Verification of the identity and authorization of persons who pick up material.

(E) Pick-up and delivery in a closed, locked van.

(c) Electrical Transmission of Information. Restricted Data shall not be transmitted electrically unless a system approved by DOE is used.

(f) Telephone Conversations. No discussion of classified information is permitted during a telephone conversation except over secure telephone systems approved by DOE.

§ 795.34 Accountability for matter comprising restricted data.

Each Permittee possessing matter containing Secret Restricted Data shall establish an accountability procedure and shall maintain for a period of 5 years records to clearly show the identification and disposition of all such matter which has been in his custody at any time.

§ 795.35 Authority to reproduce.

Nothing in this part shall be deemed to prohibit any person possessing documents containing Restricted Data from reproducing any Confidential documents, or any Secret documents originated by the Access Permittee by whom he is employed. He shall not reproduce any external generated documents containing Secret Restricted Data without prior authorization from DOE or from the originator of the document.

§ 795.36 Changes in classification.

(a) Documents containing Restricted Data shall not be downgraded to a lower classification or declassified except as authorized by DOE. Requests for downgrading or declassification shall be submitted to the DOE Operations Office administering the Permit, or U.S. Department of Energy, Washington, D.C. 20545, Attention: Office of Classification. If the Department approves a change of classification or declassification, the previous classification marking shall be canceled and the following statement, properly completed, shall 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).

(b) Any person 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 his records.

§ 795.37 Destruction of documents or material containing restricted data.

(a) Documents containing Restricted Data may be destroyed only by shredding and burning, pulping, or by any other method that assures complete destruction of the information which they contain. If the document contains Secret Restricted Data, a record of the subject, title and report number of the document, if any, its date of preparation, its series designation and copy number, and the date of destruction shall be signed by the person destroying the document and shall be maintained in the office of the last custodian for a period of 5 years after the date of destruction.

(b) Restricted Data contained in material, other than documents, may be destroyed only by a method that assures complete obliteration, removal, or destruction of the Restricted Data. A record of destruction of Secret material destroyed shall be maintained for 5 years after the date of destruction of the material.

§ 795.38 Security of automatic data processing systems.

Restricted Data shall not be processed or produced on an ADP system unless the system has been approved by DOE.

§ 795.39 Suspension or revocation of access authorization.

In any case where the access authorization of an individual subject to the regulations in this part is suspended or revoked in accordance with the procedures set forth in Part 710 of this chapter, such individual shall, upon due notice from DOE of such suspension or revocation and demand by DOE deliver to DOE any and all documents or material in his possession containing Restricted Data for safekeeping and such further disposition as DOE determines to be just and proper.

§ 795.40 Expiration, suspension or revocation of access permit.

(a) Upon expiration of an Access Permit, the person to whom such Permit has been issued may, except as provided in paragraph (b) of this section shall:

(1) deliver all documents or material in his possession containing Restricted

Data to DOE or to a person authorized to receive them and file with DOE a certificate of non-possession of Restricted Data; or

(2) destroy them, and file with DOE a certificate of nonpossession, or

(3) file with DOE a certified inventory of Restricted Data attached to a request for approval of retention of such data. A person retaining Restricted Data must maintain an active Access Permit unless otherwise authorized by DOE.

(b) In any case where an Access Permit has expired or has been suspended or revoked and DOE has determined that further possession by the former Access Permit holder of documents or materials containing Restricted Data would endanger the common defense and security, such former Access Permit holder shall upon due notice from DOE of such expiration, suspension, or revocation and of such determination, deliver to DOE any and all documents and material in his possession containing Restricted Data for safekeeping and such further disposition as DOE determines to be just and proper.

§ 795.41 Termination of employment or change of duties.

Each Permittee shall furnish promptly to DOE written notification of the termination of employment of each individual who possesses an access authorization under his Permit or whose duties are changed so that access to Restricted Data is no longer needed. Upon such notification, DOE may:

(a) terminate the individual's access authorization, or

(b) transfer the individual's access authorization to the new employer of the individual to allow continued access to Restricted Data where authorized pursuant to DOE regulations.

§ 795.42 Continued applicability of the regulations in this part.

The expiration, suspension, revocation or other termination of security clearance or access authorization or Access Permit shall not relieve any person from compliance with the regulations in this part.

§ 795.43 Reports.

Each Permittee shall report promptly to the DOE office administering the Access Permit:

(a) All losses of Restricted Data documents or material.

(b) Statutory violations, i.e., any alleged or suspected violation of the Atomic Energy Act or the Espionage Act. An immediate report shall also be made to the nearest office of the Federal Bureau of Investigation.

(c) Proposed foreign travel to Soviet-bloc countries, at least 30 days in advance of proposed travel by any of their employees, who has had access to C-24 information, and inform the same office when the employee returns.

§ 795.44 Inspection.

DOE may make such inspection of the premises, activities, records, and procedures of any person subject to the regulations in this part as DOE deems necessary to effectuate the purposes of the Act.

§ 795.45 Violations.

An injunction or other court order may be obtained prohibiting any violation of any provision of the Act or any regulation or order issued thereunder. Any person who willfully violates, attempts to violate or conspires to violate any provision of the Act or any regulation or order issued thereunder, including the provisions of this part, may be guilty of a crime and upon conviction may be punished by fine or imprisonment, or both, as provided by law.

[FR Doc. 79-18608 Filed 6-8-79; 8:45 am]
BILLING CODE 6450-01-M