may pursue, including enforced collection, judgment lien only, renew judgment lien only, renew judgment lien and enforce collection, program enforcement, foreclosure only, and foreclosure and deficiency judgment.

(c) DOE also shall use the CCLR to refer claims to the DOJ to obtain the DOJ's approval of any proposals to compromise the claims or to suspend or terminate DOE collection activity.

§ 1015.504 Preservation of evidence.

DOE will take care to preserve all files and records that may be needed by the DOJ to prove its claims in court. DOE ordinarily will include certified copies of the documents that form the basis for the claim in the packages referring its claims to the DOJ for litigation. DOE shall provide originals of such documents immediately upon request by the DOJ.

§ 1015.505 Minimum amount of referrals to the Department of Justice.

(a) DOE shall not refer for litigation claims of less than $2,500, exclusive of interest, penalties, and administrative costs, or such other amount as the Attorney General shall from time to time prescribe. The DOJ promptly shall notify DOE if the Attorney General changes this minimum amount.

(b) DOE shall not refer claims of less than the minimum amount unless:

(1) Litigation to collect such smaller claims is important to ensure compliance with DOE's policies or programs;

(2) The claim is being referred solely for the purpose of securing a judgment against the debtor, which will be filed as a lien against the debtor's property pursuant to 28 U.S.C. 3201 and returned to DOE for enforcement; or

(3) The debtor has the clear ability to pay the claim and the Government effectively can enforce payment, with due regard for the exemptions available to the debtor under state and Federal law and the judicial remedies available to the Government.

(4) DOE will consult with the Financial Litigation Staff of the Executive Office for United States Attorneys in the DOJ prior to referring claims valued at less than the minimum amount.

PART 1016—SAFEGUARDING OF RESTRICTED DATA BY ACCESS PERMITTEES

GENERAL PROVISIONS

PHYSICAL SECURITY

CONTROL OF INFORMATION

AUTHORITY: Sec. 161i of the Atomic Energy Act of 1954, 68 Stat. 948 (42 U.S.C. 2201).

SOURCE: 48 FR 36432, Aug. 10, 1983, unless otherwise noted.

GENERAL PROVISIONS

§ 1016.1 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 Top Secret information since no such information may be forwarded to an access permittee within the scope of this regulation.

§ 1016.2 Scope.

The regulations in this part apply to all persons who may require access to Retricted Data used, processed, stored, reproduced, transmitted, or handled in connection with an access permit.

§ 1016.3 Definitions.

(a) *Access authorization*. An administrative determination by DOE that an individual who is either a DOE employee, applicant for employment, consultant, assignee, other Federal department or agency employee (or other persons who may be designated by the Secretary of Energy), or a DOE contractor or subcontractor employee, or an access permittee is eligible for access to Restricted Data. Access authorizations granted by DOE are designated as ''Q,'' ''Q(X),'' ''L,'' or ''L(X).''

(1) ''Q'' access authorizations are based upon single scope background investigations as set forth in applicable DOE and national-level directives. They permit an individual who has ''need to know'' access to Top Secret, Secret and Confidential Restricted Data, Formerly Restricted Data, National Security Information, or special nuclear material in Category I or II quantities as required in the performance of duties, subject to additional determination that permitting this access will not endanger the common defense or national security of the United States. There may be additional requirements for access to specific types of RD information.

(2) ''Q(X)'' access authorizations are based upon the same level of investigation required for a Q access authorization. When ''Q'' access authorizations are granted to access permittees they are identified as ''Q(X)'' access authorizations and, as need-to-know applies, authorize access only to the type of Secret Restricted Data as specified in the permit and consistent with appendix A, 10 CFR part 725, ''Categories of Restricted Data Available.''

(3) ''L'' access authorizations are based upon a Tier III (formerly National Agency Check with Local Agency Checks and Credit Checks (NACLC)/Access National Agency Check with Inquiries (ANACI)) background investigation as set forth in applicable national-level directives. They permit an individual who has ''need to know'' access to Confidential Restricted Data, Secret and Confidential Formerly Restricted Data, or Secret and Confidential National Security Information, required in the performance of duties, provided such information is not designated ''CRYPTO'' (classified cryptographic information), ''COMSEC'' (communications security), or intelligence information and subject to additional determination that permitting this access will not endanger the common defense or national security of the United States. There may be additional requirements for access to specific types of RD information.

(4) ''L(X)'' access authorizations are based upon the same level of investigation required for an ''L'' access authorization. When ''L'' access authorizations are granted to access permittees, they are identified as ''L(X)'' access authorizations and, as need to know applies, authorize access only to the type of Confidential Restricted Data as specified in the permit and consistent with appendix A, 10 CFR part 725, ''Categories of Restricted Data Available.''

(b) *Act*. The Atomic Energy Act of 1954 (68 Stat. 919) as amended.

(c) *Classified mail address*. A mail address established for each access permittee and approved by the DOE to be used when sending Restricted Data to the permittee.

(d) *Classified matter*. Anything in physical form (including, but not limited to documents and material) that

contains or reveals classified information.

(e) *Combination lock.* A built-in combination lock on a security container which is of tempered steel alloy hard plate, at least ¼″ in thickness and Rockwell hardness of C–63 to C–65, of sufficient size and so located as to sufficiently impede access to the locking mechanism by drilling of the lock or container.

(f) *DOE.* The United States Department of Energy or its duly authorized representatives.

(g) *Formerly Restricted Data.* Classified information jointly determined by the DOE and the Department of Defense to be related primarily to the military utilization of atomic weapons and removed by the DOE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act of 1954, as amended.

(h) *Infraction.* An act or omission involving failure to comply with DOE safeguards and security orders, directives, or approvals and may include a violation of law.

(i) *Intrusion detection system.* A security system consisting of sensors capable of detecting one or more types of phenomena, signal media, annunciators, energy sources, alarm assessment systems, and alarm reporting elements including alarm communications and information display equipment.

(j) *National Security.* The national defense and foreign relations of the United States.

(k) *National Security Information.* Information that has been determined pursuant to Executive Order 13526, as amended ''Classified National Security Information'' or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(l) ''*Need to know.*'' A determination by persons having responsibility for classified information or matter, that a proposed recipient's access to such classified information or matter is necessary in the performance of official, contractual, or access permit duties of employment under cognizance of the DOE.

(m) *Permittee.* The holder of an Access Permit issued pursuant to the regulations set forth in 10 CFR part 725, ''Permits For Access to Restricted Data.''

(n) *Person.* 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 any legal successor, representative, agency, or agency of the foregoing.

(o) *Protective personnel.* Guards or watchmen or other persons designated responsibility for the protection of classified matter.

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

(q) *Security area.* A physically defined space containing classified matter and subject to physical protection and personnel access controls.

(r) *Security clearance.* See access authorization.

(s) *Security facility.* Any facility, including an access permittee, which has been approved by the DOE for using, processing, storing, reproducing, transmitting, or handling classified matter.

(t) *Security facility approval.* A determination by the DOE that a facility, including an access permittee, is eligible to use, process, store, reproduce, transmit, or handle classified matter.

(u) *Security Plan.* A written plan by the access permittee, and submitted to the DOE for approval, which outlines the permittee's proposed security procedures and controls for the protection of Restricted Data and which includes a floor plan of the area in which the classified matter is to be used, processed, stored, reproduced, transmitted, or handled.

(v) *Security survey.* An onsite examination by a DOE representative of all

devices, equipment, and procedures employed at a security facility to safeguard classified matter.

[48 FR 36432, Aug. 10, 1983, as amended at 71 FR 68735, Nov. 28, 2006; 82 FR 41505, Sept. 1, 2017]

§ 1016.4 Communications.

Communications concerning rulemaking, *i.e.*, petition to change this part, should be addressed to the Director, Office of Environment, Health, Safety and Security, EHSS–1/Forrestal Building, Office of Environment, Health, Safety and Security, U.S. Department of Energy, 1000 Independence Avenue SW., Washington, DC 20585. All other communications concerning the regulations in this part should be addressed to the cognizant DOE or National Nuclear Security Administration (NNSA) office.

[82 FR 41505, Sept. 1, 2017, as amended at 88 FR 41294, June 26, 2023]

§ 1016.5 Submission of procedures by access permit holder.

No access permit holder shall have access to Restricted Data until he has submitted to the DOE a written statement of his procedures for the safeguarding of Restricted Data and for the security education of his employees, and DOE shall have determined and informed the permittee that his procedures for the safeguarding of Restricted Data are in compliance with the regulations in this part and that his procedures for the security education of his employees, who will have access to Restricted Data, are informed about and understand the regulations in this part. These procedures must ensure that employees with access to Restricted Data are informed about and understand who is authorized or required to classify and declassify RD and FRD information and classified matter as well as how documents containing RD or FRD are marked (see 10 CFR part 1045) and safeguarded.

[82 FR 41506, Sept. 1, 2017]

§ 1016.6 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 an undue risk to the common defense and security.

§ 1016.7 Interpretations.

Except as specifically authorized by the Secretary of Energy 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

§ 1016.8 Request for security facility approval.

(a) An access permittee who has a need to use, process, store, reproduce, transmit, or handle Restricted Data at any location in connection with its permit shall promptly request a DOE security facility approval.

(b) The request shall include the following information: The name and address of the permittee; the extent and scope of the classified activity and the highest classification of Restricted Data to be received; a written statement in the form of a security plan which outlines the permittee's proposed security procedures and controls for the protection of Restricted Data, including a floor plan of the areas(s) in which the classified matter is to be used, processed, stored, reproduced, transmitted, and handled.

(c) The DOE will promptly inform the permittee of the acceptability of the request for further processing and will notify the permittee of its decision in writing.

§ 1016.9 Processing security facility approval.

Following receipt of an acceptable request for security facility approval, the DOE will perform an initial security survey of the permittee's facility to determine that granting a security facility approval would be consistent with the national security. If DOE makes such a determination, security facility approval will be granted. If not, security facility approval will be withheld pending compliance with the security survey recommendations or

until a waiver is granted pursuant to §1016.6.

[82 FR 41506, Sept. 1, 2017]

§1016.10 Granting, denial, or suspension of security facility approval.

Notification of the DOE's granting, denial, or suspension of security facility approval will be furnished the permittee in writing, or orally with written confirmation. This information may also be furnished to representatives of the DOE, DOE contractors, or other Federal agencies having a need to transmit Restricted Data to the permittee.

[82 FR 41506, Sept. 1, 2017]

§1016.11 Cancellation of requests for security facility approval.

When a request for security facility approval is to be withdrawn or cancelled, the cognizant DOE Office will be notified by the requester immediately by telephone and confirmed in writing so that processing of this approval may be terminated.

[82 FR 41506, Sept. 1, 2017]

§1016.12 Termination of security facility approval.

(a) Security facility approval will be terminated when:

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

(2) The DOE makes a determination that continued security facility approval is not in the interest of common defense and security.

(b) The permittee will be notified in writing of a determination to terminate facility approval, and the procedures outlined in §1016.27 will apply.

[82 FR 41506, Sept. 1, 2017]

§1016.13 Protection of Restricted Data in storage.

(a) Persons who possess Restricted Data pursuant to an Access Permit shall store the Restricted Data classified matter when not in use in a locked storage container or DOE-approved vault to which only persons with appropriate access authorization and a need to know the information contained have access. Storage containers used for storing classified matter must conform to U.S. General Services Administration (GSA) standards and specifications.

(b) Each permittee shall change the combination on locks of his safekeeping equipment whenever such equipment is placed in use, whenever an individual knowing the combination no longer requires access to the repository as a result of change in duties or position in the permittee's organization, or termination of employment with the permittee or whenever the combination has been subjected to compromise, and in any event at least once a year. Permittees shall classify records of combinations no lower than the highest classification of the classified matter authorized for storage in the safekeeping equipment concerned.

[82 FR 41506, Sept. 1, 2017]

§1016.14 Protection of Restricted Data while in use.

While in use, classified matter containing Restricted Data shall be under the direct control of a person with the appropriate access authorization and need to know. Unauthorized access to the Restricted Data shall be precluded.

[82 FR 41506, Sept. 1, 2017]

§1016.15 Establishment of security areas.

(a) When, because of their nature or size, it is impracticable to safeguard classified matter containing Restricted Data in accordance with the provisions of §§1016.13 and 1016.14, a security area to protect such classified matter 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 an appropriately cleared individual posted at each unlocked entrance.

(3) During nonworking hours, admittance shall be controlled by protective personnel on patrol, with protective

personnel posted at unlocked entrances, or by such intrusion detection system as DOE approves.

(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.

[82 FR 41506, Sept. 1, 2017]

§ 1016.16 Special handling 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 §§ 1016.21 to 1016.23 inclusive, as DOE determines to be commensurate with the difficulty of removing the material.

[48 FR 36432, Aug. 10, 1983. Redesignated at 82 FR 41506, Sept. 1, 2017

§ 1016.17 Protective personnel.

Whenever armed protective personnel are required in accordance with § 1016.15, such protective personnel shall:

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

(b) Be armed with sidearms of 9mm or greater.

[82 FR 41507, Sept. 1, 2017]

CONTROL OF INFORMATION

§ 1016.18 Access to Restricted Data.

(a) Except as DOE may authorize, no person subject to the regulations in this part shall permit any individual to have access to Restricted Data in his possession unless the individual has an appropriate access authorization granted by DOE, or has been certified by DOD or NASA through DOE; and

(1) The individual is authorized by an Access Permit to receive Restricted Data in the categories involved and the permittee determines that such access is required in the course of his duties; or

(2) The individual needs such access in connection with such duties as a DOE employee or DOE contractor employee, or as certified by DOD or NASA.

(b) Inquiries concerning the access authorization status of individuals, the scope of Access Permits, or the nature of contracts should be addressed to the cognizant DOE or NNSA office.

[82 FR 41507, Sept. 1,2017]

§ 1016.19 Review, classification and marking of classified information.

(a) *Classification*. Restricted Data generated or possessed by an Access Permit holder must be appropriately classified and marked in accordance with 10 CFR part 1045. CG–DAR–2, ''Guide to the Declassified Areas of Nuclear Energy Research U 08/98,'' will be furnished each permittee. In the event a permittee originates classified information which falls within the definition of Restricted Data or information for which the permittee is not positive that the information is outside of that definition and CG–DAR–2 does not provide positive classification guidance for such information, the permittee shall designate the information as Confidential, Restricted Data and request classification guidance from the DOE through the Classification Officer at the cognizant DOE or NNSA office. If the DOE Classification Officer does not have authority to provide the guidance, he will refer the request to the Director, Office of Classification, EHSS–60/Germantown Building, Office of Environment, Health, Safety and Security, U.S. Department of Energy, 1000 Independence Avenue SW., Washington, DC 20585–1290.

(b) *Challenges.* If a person receives a document or other classified matter which, in his opinion, is not properly classified, or omits the appropriate classification markings, he is encouraged to challenge the classification and there shall be no retribution for submitting a challenge. Challenges shall be submitted in accordance with 10 CFR part 1045.

(c) *Classification markings.* Restricted Data generated or possessed by an individual approved for access must be appropriately identified and marked in accordance with 10 CFR part 1045, Nuclear Classification and Declassification. Questions and requests for additional direction or guidance regarding the marking of classified matter may be submitted to the Director, Office of Classification, EHSS–60/Germantown Building, Office of Environment, Health, Safety and Security, U.S. Department of Energy, 1000 Independence Avenue SW., Washington, DC 20585–1290.

[82 FR 41507, Sept. 1, 2017, as amended at 88 FR 41294, June 26, 2023]

§ 1016.20 External transmission of Restricted Data.

(a) *Restrictions.* (1) Restricted Data shall be transmitted only to persons who possess appropriate access authorization, need to know, and are otherwise eligible for access under the requirements of § 1016.18.

(2) In addition, such classified matter containing Restricted Data shall be transmitted only to persons who possess approved facilities for their physical security consistent with this part. Any person subject to the regulations in this part who transmits such Restricted Data containing Restricted Data shall be deemed to have fulfilled his obligations under this paragraph (a)(2) by securing a written certification from the prospective recipient that such recipient possesses facilities for its physical security consistent with this part.

(3) Restricted Data shall not be exported from the United States without prior authorization from 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 shall be marked on both sides of the envelope, and any additional marking required by 10 CFR part 1045 shall be applied.

(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 document containing Secret Restricted Data is transferred.

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

(1) The classified matter shall be so packaged that the classified characteristics will not be revealed.

(2) A receipt which identifies the classified matter, the date of shipment, the recipient, and the person transferring the classified matter shall accompany the classified matter, and the recipient shall sign such receipt whenever the custody of classified matter containing Secret Restricted Data is transferred.

(d) *Methods of transportation.* (1) Secret classified matter shall be transported only by one of the following methods:

(i) By messenger-courier system specifically created for that purpose and approved for use by DOE.

(ii) Registered mail.

(iii) By protective services provided by United States air or surface commercial carriers under such conditions as may be preserved by the DOE.

(iv) Individuals possessing appropriate DOE access authorization who have been given written authority by their employers.

(2) Confidential classified matter may be transported by one of the methods set forth in paragraph (d)(1) of this section or by U.S. first class, express, or certified mail.

(e) *Telecommunication of classified information.* There shall be no telecommunication of Restricted Data unless the secure telecommunication system has been approved by the DOE.

[82 FR 41507, Sept. 1, 2017]

§ 1016.21 Accountability for Secret Restricted Data.

Each permittee possessing classified matter (including classified matter in electronic format) containing Secret Restricted Data shall establish accountability procedures and shall maintain logs to document access to and record comprehensive disposition information for all such classified matter that has been in his custody at any time.

[82 FR 41507, Sept. 1, 2017]

§ 1016.22 Authority to reproduce Restricted Data.

Secret Restricted Data will not be reproduced without the written permission of the originator, his successor, or high authority. Confidential Restricted Data may be reproduced to the minimum extent necessary consistent with efficient operation without the necessity for permission.

[48 FR 36432, Aug. 10, 1983. Redesiganted at 82 FR 41508, Sept. 1, 2017]

§ 1016.23 Changes in classification.

Classified matter containing Restricted Data shall not be downgraded or declassified except as authorized by DOE and in accordance with 10 CFR part 1045.

[82 FR 41508, Sept. 1, 2017]

§ 1016.24 Destruction of classified matter containing Restricted Data.

Documents containing Restricted Data may be destroyed by burning, pulping, or another method that assures complete destruction of the information which they contain. Restricted Data contained in classified matter, other than documents, may be destroyed only by a method that assures complete obliteration, removal, or destruction of the Restricted Data.

[82 FR 41508, Sept. 1, 2017]

§ 1016.25 Storage, use, processing, transmission and destruction of classified information on computers, computer networks, electronic devices/media and mobile devices.

Storage, use, processing, and transmission of Restricted Data on computers, computer networks, electronic devices/media and mobile devices must be approved by DOE. DOE-approved methods must be used when destroying classified information that is in electronic format.

[82 FR 41508, Sept. 1, 2017]

§ 1016.26 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 10 CFR part 710, such individual shall, upon due notice from DOE of such suspension or revocation and demand by DOE, deliver to DOE any and all Restricted Data in his possession for safekeeping and such further disposition as DOE determines to be just and proper.

[48 FR 36432, Aug. 10, 1983. Redesignated at 82 FR 41508, Sept. 1, 2017]

§ 1016.27 Termination, suspension, or revocation of security facility approval.

(a) In accordance with § 1016.12, if the need to use, process, store, reproduce, transmit, or handle classified matter no longer exists, the security facility approval will be terminated. The permittee may deliver all Restricted Data to the DOE or to a person authorized to receive them; or the permittee may destroy all such Restricted Data. In either case, the facility must submit a certification of non-possession of Restricted Data to the DOE.

(b) In any instance where security facility approval has been suspended or revoked based on a determination of the DOE that further possession of classified matter by the permittee would endanger the common defense and national security, the permittee shall, upon notice from the DOE, immediately deliver all Restricted Data

to the DOE along with a certificate of non-possession of Restricted Data.

[82 FR 41508, Sept. 1, 2017]

§ 1016.28 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.

[48 FR 36432, Aug. 10, 1983. Redesignated at 82 FR 41508, Sept. 1, 2017]

§ 1016.29 Continued applicability of the regulations in this part.

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

[48 FR 36432, Aug. 10, 1983. Redesignated at 82 FR 41508, Sept. 1, 2017]

§ 1016.30 Reports.

Each permittee shall immediately report to the DOE office administering the permit any alleged or suspected violation of the Atomic Energy Act of 1954, as amended, Espionage Act, or other Federal statutes related to Restricted Data. Additionally, the permittee shall report any infractions, losses, compromises, or possible compromise of Restricted Data.

[48 FR 36432, Aug. 10, 1983. Redesignated at 82 FR 41508, Sept. 1, 2017]

§ 1016.31 Inspections.

The DOE shall make such inspections and surveys 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, Executive Order 13526, and DOE orders and procedures.

[82 FR 41508, Sept. 1, 2017]

§ 1016.32 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.

[48 FR 36432, Aug. 10, 1983. Redesignated at 82 FR 41508, Sept. 1, 2017]

PART 1017—IDENTIFICATION AND PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

Subpart A—General Overview

Subpart B—Initially Determining What Information Is Unclassified Controlled Nuclear Information

Subpart C—Review of a Document or Material for Unclassified Controlled Nuclear Information