contractor's facility is authorized only to the GCA, or to a subcontractor as described in paragraph (d) of this section. Any other transmission must be approved by the GCA.

(1) Prior to transmission to another cleared facility, the contractor will verify from the CSA that the facility has been authorized access to CNWDI. When CNWDI is transmitted to another facility, the inner wrapping will be addressed to the personal attention of the FSO or his or her alternate, and in addition to any other prescribed markings, the inner wrapping will be marked: ''Critical Nuclear Weapon Design Information-DoD Instruction 5210.02 Applies.''

(2) The same marking will be used on the inner wrapping of transmissions addressed to the GCA or other USG.

(f) *Records.* Contractors will annotate CNWDI access in the CSA-designated database for all employees who have been authorized access to CNWDI.

(g) *Nuclear weapon data.* Some nuclear weapon data is divided into Sigma categories, the protection of which is prescribed by DOE Order 452.8 (available at: *https://www.directives.doe.gov/directives-documents/400-series/0452.8-border/@@images/file*). However, certain nuclear weapon data has been re-categorized as CNWDI and is protected as described in this section.

§ 117.21 COMSEC.

(a) *General.* The procedures in this section pertaining to classified COMSEC information will apply to contractors when the contractor:

(1) Requires the use of COMSEC systems in the performance of a contract.

(2) Is required to install, maintain, or operate COMSEC equipment for the USG.

(3) Is required to accomplish research, development, or production of COMSEC systems, COMSEC equipment, or related COMSEC material.

(b) *Instructions.* Specific requirements for the management and safeguarding of COMSEC material in industry are established in the COMSEC material control and operating procedures provided to the account manager of each industrial COMSEC account by the agency central office of record (COR) responsible for establishing the account. Such procedures that are above the baseline requirements detailed in the other sections of this rule will be contractually mandated.

(c) *Clearance and access requirements.* (1) Before a COMSEC account can be established and a contractor may receive or possess COMSEC material accountable to a COR, individuals occupying the positions of FSO, COMSEC account manager, and alternate COMSEC account manager must have a final PCL appropriate for the material to be held in the account.

(i) COMSEC account managers and alternate COMSEC account managers having access to operational TOP SECRET keying material marked as CRYPTO must have a final TOP SECRET security clearance based upon a current investigation of a scope that meets or exceeds that necessary for the access required.

(ii) This requirement does not apply to contractors using only data transfer devices and seed key.

(2) Before disclosure of COMSEC information to a contractor, GCAs must first verify with the CSA that appropriate COMSEC procedures are in place at the contractor facility. If procedures are not in place, the GCA will provide a written request and justification to the CSA to establish COMSEC procedures and a COMSEC account, if appropriate, at the facility and to conduct the initial COMSEC or cryptographic access briefings for the FSO and COMSEC account personnel.

(3) Access to COMSEC information by a contractor requires a final entity eligibility determination and a USG-issued final PCL at the appropriate level; however, an Interim TOP SECRET entity eligibility determination or PCL is valid for access to COMSEC at the SECRET and CONFIDENTIAL levels.

(4) If a COMSEC account will be required, the Contract Security Classification Specification, or equivalent, will contain a statement regarding the establishment of a COMSEC account as appropriate.

(d) *Establishing a COMSEC account.* (1) When COMSEC material that is accountable to a COR is to be provided, acquired, or produced under a contract,

the contracting officer will inform the contractor that a COMSEC account must be established. The contractor will forward the names of U.S. citizen employees who will serve as the COMSEC account manager and alternate COMSEC account manager to the CSA. The CSA will forward the names of the FSO, COMSEC account manager, and alternate COMSEC account manager, along with a contractual requirement for the establishment of a COMSEC account (using DD Form 254 or equivalent) to the appropriate COR, with a copy to the GCA, indicating that the persons have been cleared and COMSEC has been briefed.

(2) The COR will then establish the COMSEC account and notify the CSA that the account has been established.

(3) An individual may be appointed as the COMSEC account manager or alternate COMSEC account manager for more than one account only when approved by each COR concerned.

(e) *COMSEC briefing and debriefing.* (1) All contractor employees who require access to classified COMSEC information in the performance of their duties will be briefed before access is granted. Depending on the nature of COMSEC access required, either a COMSEC briefing or a cryptographic access briefing will be given. The FSO, the COMSEC account manager, and the alternate COMSEC account manager will be briefed by a USG representative or their designee. Other contractor employees will be briefed by the FSO, the COMSEC account personnel, or other individual designated by the FSO. The purpose of the briefing is to ensure that the contractor understands:

(i) The unique nature of COMSEC information and its unusual sensitivity.

(ii) The special security requirements for the handling and protection of COMSEC information.

(iii) The penalties prescribed in 18 U.S.C. 793, 794, and 798 for disclosure of COMSEC information.

(2) COMSEC debriefings are not required.

(3) The contractor will maintain a record of all COMSEC briefings as specified by the appropriate COR.

(f) *U.S. classified cryptographic information access briefing and debriefing requirements.* (1) U.S. classified cryptographic information does not include seed key or controlled cryptographic items.

(2) A contractor's employee may be granted access to U.S. classified cryptographic information only if the employee:

(i) Is a U.S. citizen.

(ii) Has a final USG-issued eligibility determination appropriate to the classification of the U.S. cryptographic information to be accessed.

(iii) Has a valid need-to-know to perform duties for, or on behalf of, the USG.

(iv) Receives a security briefing appropriate to the U.S. Classified Cryptographic Information to be accessed.

(v) Acknowledges the granting of access to classified information by executing Section I of Secretary of Defense (SD) Form 572, ''Cryptographic Access Certification and Termination'' (available at: *https://www.esd.whs.mil/Portals/54/Documents/DD/forms/sd/sd0572.pdf*).

(vi) Where so directed by a USG department or agency head, acknowledges the possibility of being subject to a CI scope polygraph examination that will be administered in accordance with department or agency directives and applicable law.

(3) An employee granted access to cryptographic information will be debriefed and execute Section II of the SD 572 not later than 90 days from the date access is no longer required.

(4) The contractor will maintain the SD 572 for a minimum of five years following the debriefing.

(5) Cryptographic access briefings must fully meet the requirements of paragraph (e) of this section.

(g) *Destruction and disposition of COMSEC material.* The appropriate GCA representative, *e.g.*, the contracting officer representative, will provide directions to the contractor when accountable COMSEC material is to be destroyed. These directions may be provided in superseding editions of publications or by specific instructions.

(h) *Subcontracting COMSEC work.* Subcontracts requiring the disclosure of classified COMSEC information will be awarded only upon the written approval of the GCA.

(i) *Unsolicited proposals.* Any unsolicited proposal for a COMSEC system, equipment, development, or study that may be submitted by a contractor to a USG agency will be forwarded to the Deputy National Manager for National Security Systems for review and follow up action at: Deputy National Manager for National Security Systems, NSA, Fort George G. Meade, MD 20755–6000.

§ 117.22 DHS CCIPP.

(a) *General.* DHS will coordinate with other USG agencies that have an equity with a private sector entity and the CCIPP in accordance with § 117.6(f).

(b) *Authority.* (1) The Secretary of Homeland Security has the authority to determine the eligibility for personnel security clearances and to administer the sharing of relevant classified NSI with certain private sectors or non-federal partners for the purpose of furthering cybersecurity information sharing among critical infrastructure partners pursuant to E.O. 13691.

(2) DHS provides security oversight and assumes security responsibilities similar to those of an FSO, unless otherwise provided in this section. Participating entities will cooperate with DHS security officials to ensure the entity is in compliance with requirements in this rule.

§ 117.23 Supplement to this rule: Security Requirements for Alternative Compensatory Control Measures (ACCM), Special Access Programs (SAPs), Sensitive Compartmented Information (SCI), Restricted Data (RD), Formerly Restricted Data (FRD), Transclassified Foreign Nuclear Information (TFNI), and Naval Nuclear Propulsion Information (NNPI).

(a) *General.* Given the sensitive nature of Alternative Compensatory Control Measures (ACCM), SAPs, SCI, RD, FRD, TFNI, and NNPI, the security requirements prescribed in this section exceed baseline standards for this rule and must be applied, as applicable, through specific contract requirements.

(1) *Compliance.* The contractor will comply with the security measures reflected in this section and other documents specifically referenced, when applied by the GCA or designee as part of a contract. Acceptance of the contract security measures is a prerequisite to any negotiations leading to program participation and an area accreditation (*e.g.*, an SCI facility or SAP facility accreditation).

(2) *CSA-imposed higher standards.* In some cases, security or sensitive factors of a CSA-created program may require security measures that exceed the standards of this section. In such cases, the CSA-imposed higher standards specifically detailed in the contract or conveyed through other applicable directives will be binding on USG and contractor participants. In cases of doubt over the specific provisions, the contractor should consult the program security officer and the contracting officer before taking any action or expending program-related funds. In cases of extreme emergencies requiring immediate attention, the action taken should protect the USG's interest and the security of the program from loss or compromise.

(3) *Waivers.* Every effort will be made to avoid waivers to established standards unless they are in the best interest of the USG. In those cases where waivers are deemed necessary, a request will be submitted in accordance with the procedures established by the CSA.

(b) *Intelligence information.* National intelligence is under the jurisdiction and control of the DNI, who establishes security policy for the protection of national intelligence and intelligence sources, methods, and activities. In addition to the guidance in this rule, contractors will follow Intelligence Community directives, policy guidance, standards, and specifications for the protection of classified national intelligence and SCI.

(c) *ACCM.* Contractors may participate in ACCMs, or be directed to participate, only when such access and the associated security plan are identified in DD Form 254 or equivalent. Care must be taken to ensure identification of the security plan does not disclose ACCM-protected data.

(1) *ACCM contracts.* DoD contractors will implement the security requirements for ACCMs, when established by contract, in accordance with applicable