

such Block Certification and shall submit such application to the Department in accordance with §9(a). Applicants seeking to be qualified Sellers of an Approved Product for Homeland Security pursuant to a Block Certification will receive expedited review of their applications and shall not be required to provide information with respect to the technical merits of the Approved Product for Homeland Security that has received Block Certification. Within 60 days (or such other period of time as may be specified in the applicable Block Certification) after the receipt by the Department of a complete application, the Under Secretary shall take one of the following actions:

(i) Approve the application and notify the applicant in writing of such approval; or

(ii) Deny the application, and notify the applicant in writing of such decision, including the reasons for such denial.

(2) If the application is approved, commencing on the date of such approval, the applicant shall be deemed to be a Seller under the applicable Block Certification for all purposes under the SAFETY Act, this part, and such Block Certification. A Block Certification shall be valid and effective for the same period of time for which the related Block Designation is issued. A Block Certification may be renewed by the Under Secretary at his own initiative or in response to an application for renewal submitted by a qualified Seller under such Block Certification in accordance with §25.9(g). Except as otherwise specifically provided in this paragraph, a Block Certification shall be deemed to be a Certification for all purposes under the SAFETY Act and this part.

§25.10 Confidentiality and protection of Intellectual Property.

(a) *General.* The Secretary, in consultation with the Office of Management and Budget and appropriate Federal law enforcement and intelligence officials, and in a manner consistent with existing protections for sensitive or classified information, shall establish confidentiality procedures for safeguarding, maintenance and use of information submitted to the Depart-

ment under this part. Such protocols shall, among other things, ensure that the Department will utilize all appropriate exemptions from the Freedom of Information Act.

(b) *Non-Disclosure.* Except as otherwise required by applicable law or regulation or a final order of a court of competent jurisdiction, or as expressly authorized in writing by the Under Secretary, no person, firm, or other entity may:

(1) Disclose SAFETY Act Confidential Information (as defined above) to any person, firm, or other entity, or

(2) Use any SAFETY Act Confidential Information for his, her, or its own benefit or for the benefit of any other person, firm, or other entity, unless the applicant has consented to the release of such SAFETY Act Confidential Information.

(c) *Legends.* Any person, firm, or other entity that submits data or information to the Department under this Part may place a legend on such data or information indicating that the submission constitutes SAFETY Act Confidential Information. The absence of such a legend shall not prevent any data or information submitted to the Department under this Part from constituting or being considered by the Department to constitute SAFETY Act Confidential Information.

PART 29—PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Sec.

29.1 Purpose and scope.

29.2 Definitions.

29.3 Effect of provisions.

29.4 Protected Critical Infrastructure Information Program administration.

29.5 Requirements for protection.

29.6 Acknowledgment of receipt, validation, and marking.

29.7 Safeguarding of Protected Critical Infrastructure Information.

29.8 Disclosure of Protected Critical Infrastructure Information.

29.9 Investigation and reporting of violation of PCII procedures.

AUTHORITY: Pub. L. 107-296, 116 Stat. 2135 (6 U.S.C. 1 *et seq.*); 5 U.S.C. 301.

SOURCE: 71 FR 52271, Sept. 1, 2006, unless otherwise noted.