

submission of CII may be accomplished by (*i.e.*, come from) a single State or Local governmental entity; private entity or person; or by an ISAO acting on behalf of its members or otherwise. There are two exclusions from this definition:

(1) In the case of any action brought under the securities laws—as is defined in 15 U.S.C. 78c(a)(47)—the term “voluntary” or “voluntarily” does not include:

(i) Information or statements contained in any documents or materials filed pursuant to 15 U.S.C. 781(i) with the U.S. Securities and Exchange Commission or with federal banking regulators; or

(ii) A writing that accompanied the solicitation of an offer or a sale of securities; and

(2) Information or statements previously submitted to DHS in the course of a regulatory proceeding or a licensing or permitting determination are not “voluntarily submitted.” In addition, the submission of information to DHS for purposes of seeking a federal preference or benefit, including CII submitted to support an application for a DHS grant to secure critical infrastructure will be considered a voluntary submission of information. Applications for Support Anti-terrorism by Fostering Effective Technologies Act of 2002 filed pursuant to 6 U.S.C. 441 *et seq.*, or SAFETY Act Designation or Certification under 6 CFR part 25, will also be considered a voluntary submission.

Used directly by such agency, any other Federal, State, or Local authority, or any third party, in any civil action arising under Federal or State law in 6 U.S.C. 673(a)(1)(C) means any use in any proceeding other than a criminal prosecution before any court of the United States or of a State or otherwise, of any PCII, or any drafts or copies of PCII retained by the submitter, including the opinions, evaluations, analyses and conclusions prepared and submitted as CII, as evidence at trial or in any pretrial or other discovery, notwithstanding whether the United States, its agencies, officers, or employees is or are a party to such proceeding.

§ 29.3 FOIA exemptions and restrictions on use of PCII.

(a) *Freedom of Information Act disclosure exemptions.* Information that is separately exempt from public disclosure under the Freedom of Information Act (5 U.S.C. 552) or applicable State, or Local law does not lose its separate exemption from public disclosure due to the applicability of these procedures or any failure to follow them.

(b) *Restriction on use of PCII by regulatory agencies and other Federal, State, and Local agencies.* A Federal, State, or Local government agency that receives PCII may utilize the PCII only for purposes appropriate under the CII Act, including securing critical infrastructure or protected systems. Such PCII may not be utilized for any other collateral regulatory purposes without the written consent of the PCII Program Manager and of the submitting person or entity. The PCII Program Manager or the PCII Program Manager’s Designee will not share PCII with Federal, State, or Local government agencies without instituting appropriate measures to ensure that PCII is used only for appropriate purposes.

§ 29.4 PCII Program administration.

(a) *Cybersecurity and Infrastructure Security Agency.* The Secretary of the Department of Homeland Security hereby designates the Director as the senior DHS official responsible for the direction and administration of the PCII Program. The Director administers this program through the Executive Assistant Director.

(b) *Appointment of a PCII Program Manager.* The Director will:

(1) Appoint a PCII Program Manager serving under the Executive Assistant Director who is responsible for the administration of the PCII Program;

(2) Commit resources necessary for the effective implementation of the PCII Program;

(3) Ensure that sufficient personnel, including detailees or assignees from other federal national security, homeland security, or law enforcement entities, as the Director deems appropriate, are assigned to the PCII Program to facilitate secure information sharing with appropriate authorities; and