(C) Advise the submitting person or entity that the submission can be withdrawn at any time before a final determination is made;

(D) Notify the submitting person or entity that until a final determination is made the submission will be treated as PCII;

(E) Notify the submitting person or entity that any response to the notification must be received by the PCII Program Office no later than thirty calendar days after the date of the notification; and

(F) Request the submitting person or entity to state whether, in the event the PCII Program Office makes a final determination that any such information is not PCII, the submitting person or entity prefers that the information be maintained without the protections of the CII Act or returned to the submitter or destroyed. If a request for withdrawal is made, all such information shall be returned to the submitting person or entity.

(ii) If the information submitted has not been withdrawn by the submitting person or entity, and the PCII Program Office, after following the procedures set forth in paragraph (e)(2)(i) of this section, makes a final determination that any such information is not PCII, the submitting person or entity prefers that the information be maintained without the protections of the CII Act or returned to the submitter or destroyed. If a request for withdrawal is made, all such information shall be returned to the submitting person or entity.

(g) Changing the status of PCII to non-PCII. Once information is validated, only the PCII Program Office may change the status of PCII to that of non-PCII and remove its PCII markings. Status changes may only take place when the submitting person or entity requests in writing that the information no longer be protected under the CII Act; or when the PCII Program Office determines that the information was, at the time of the submission, customarily in the public domain. Upon making an initial determination that a change in status may be warranted, but prior to a final determination, the PCII Program Office, using the procedures in paragraph (e)(2) of this section, shall inform the submitting person or entity of the initial determination of a change in status. Notice of the final change in status of PCII shall be provided to all recipients of that PCII under 6 CFR 29.8.

§ 29.7 Safeguarding of Protected Critical Infrastructure Information.

(a) Safeguarding. All persons granted access to PCII are responsible for safeguarding such information in their possession or control. PCII shall be protected at all times by appropriate storage and handling. Each person who works with PCII is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

(b) Background Checks on Persons with Access to PCII. For those who require access to PCII, DHS will, to the extent practicable and consistent with the purposes of the Act, undertake appropriate background checks to ensure that individuals with access to PCII do not pose a threat to national security.
§ 29.8 Disclosure of Protected Critical Infrastructure Information.

(a) Authorization of access. The Under Secretary for Preparedness, the Assistant Secretary for Infrastructure Protection, or either’s designee may choose to provide or authorize access to PCII under one or more of the subsections below when it is determined that this access supports a lawful and authorized government purpose as enumerated in the CII Act or other law, regulation, or legal authority.

(b) Federal, State and Local government sharing. The PCII Program Manager or the PCII Program Manager’s designees may provide PCII to an employee of the Federal government, provided, subject to subsection (f) of this section, that such information is shared for purposes of securing the critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another appropriate purpose including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to the homeland. PCII may not be used, directly or indirectly, for any collateral regulatory purpose. PCII may be provided to a State or local government entity for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act. The provision of PCII to a State or local government entity will normally be made only pursuant to an arrangement with the PCII Program Manager providing for compliance with the requirements of paragraph (d) of this section and acknowledging the understanding and responsibilities of the recipient. State and local governments receiving such information will acknowledge in such arrangements the primacy of PCII protections under the CII Act; agree to assert all available legal defenses to disclosure of PCII under State, or local public disclosure laws, statutes or ordinances; and will agree to treat breaches of the agreements by their employees or contractors as matters subject to the criminal code or to the applicable employee code of conduct for the jurisdiction.

(c) Disclosure of information to Federal, State and local government contractors. Disclosure of PCII to Federal, State, and local contractors may be made when necessary for an appropriate purpose under the CII Act, and only after the PCII Program Manager or a PCII Officer certifies that the contractor is performing services in support of the purposes of the CII Act. The contractor’s employees who will be handling PCII must sign individual nondisclosure agreements in a form prescribed...