These checks may also be waived in exigent circumstances.

(c) *Use and Storage.* When PCII is in the physical possession of a person, reasonable steps shall be taken, in accordance with procedures prescribed by the PCII Program Manager, to minimize the risk of access to PCII by unauthorized persons. When PCII is not in the physical possession of a person, it shall be stored in a secure environment.

(d) *Reproduction.* Pursuant to procedures prescribed by the PCII Program Manager, a document or other material containing PCII may be reproduced to the extent necessary consistent with the need to carry out official duties, provided that the reproduced documents or material are marked and protected in the same manner as the original documents or material.

(e) *Disposal of information.* Documents and material containing PCII may be disposed of by any method that prevents unauthorized retrieval, such as shredding or incineration.

(f) *Transmission of information.* PCII shall be transmitted only by secure means of delivery as determined by the PCII Program Manager, and in conformance with appropriate federal standards.

(g) *Automated Information Systems.* The PCII Program Manager shall establish security requirements designed to protect information to the maximum extent practicable, and consistent with the Act, for Automated Information Systems that contain PCII. Such security requirements will be in conformance with the information technology security requirements in the Federal Information Security Management Act and the Office of Management and Budget's implementing policies.

§ 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

by the PCII Program Manager, and the contractor must agree by contract, whenever and to whatever extent possible, to comply with all relevant requirements of the PCII Program. The contractor shall safeguard PCII in accordance with these procedures and shall not remove any ''PCII'' markings. An employee of the contractor may, in the performance of services in support of the purposes of the CII Act and when authorized to do so by the PCII Program Manager or the PCII Program Manager's designee, communicate with a submitting person or an authorized person of a submitting entity, about a submittal of information by that person or entity. Contractors shall not further disclose PCII to any other party not already authorized to receive such information by the PCII Program Manager or PCII Program Manager's Designee, without the prior written approval of the PCII Program Manager or the PCII Program Manager's designee.

(d) *Further use or disclosure of information by State, and local governments.* (1) State and local governments receiving information marked ''Protected Critical Infrastructure Information'' shall not share that information with any other party not already authorized to receive such information by the PCII Program Manager or PCII Program Manager's designee, with the exception of their contractors after complying with the requirements of paragraph (c) of this section, or remove any PCII markings, without first obtaining authorization from the PCII Program Manager or the PCII Program Manager's designees, who shall be responsible for requesting and obtaining written consent from the submitter of the information.

(2) State and local governments may use PCII only for the purpose of protecting critical infrastructure or protected systems, or as set forth elsewhere in these rules.

(e) *Disclosure of information to appropriate entities or to the general public.* PCII may be used to prepare advisories, alerts, and warnings to relevant companies, targeted sectors, governmental entities, ISAOs or the general public regarding potential threats and vulnerabilities to critical infrastructure as appropriate pursuant to the CII Act. Unless exigent circumstances require otherwise, any such warnings to the general public will be authorized by the Secretary, Under Secretary for Preparedness, Assistant Secretary for Cyber Security and Telecommunications, or Assistant Secretary for Infrastructure Protection. Such exigent circumstances exist only when approval of the Secretary, the Under Secretary for Preparedness, Assistant Secretary for Cyber Security and Telecommunications, or the Assistant Secretary for Infrastructure Protection cannot be obtained within a reasonable time necessary to issue an effective advisory, alert, or warning. In issuing advisories, alerts and warnings, DHS shall consider the exigency of the situation, the extent of possible harm to the public or to critical infrastructure, and the necessary scope of the advisory or warning; and take appropriate actions to protect from disclosure any information that is proprietary, business sensitive, relates specifically to, or might be used to identify, the submitting person or entity, or any persons or entities on whose behalf the CII was submitted, or is not otherwise appropriately in the public domain. Depending on the exigency of the circumstances, DHS may consult or cooperate with the submitter in making such advisories, alerts or warnings.

(f) *Disclosure for law enforcement purposes and communication with submitters; access by Congress, the Comptroller General, and the Inspector General; and whistleblower protection*—(1) *Exceptions for disclosure.* (i) PCII shall not, without the written consent of the person or entity submitting such information, be used or disclosed for purposes other than the purposes of the CII Act, except—

(A) In furtherance of an investigation or the prosecution of a criminal act by the Federal government, or by a State, local, or foreign government, when such disclosure is coordinated by a Federal law enforcement official;

(B) To communicate with a submitting person or an authorized person on behalf of a submitting entity, about a submittal of information by that person or entity when authorized to do so by the PCII Program Manager or the PCII Program Manager's designee; or

(C) When disclosure of the information is made by any officer or employee of the United States—

(*1*) To either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(*2*) To the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the Government Accountability Office.

(ii) If any officer or employee of the United States makes any disclosure pursuant to these exceptions, contemporaneous written notification must be provided to DHS through the PCII Program Manager.

(2) Consistent with the authority to disclose information for any of the purposes of the CII Act, disclosure of PCII may be made, without the written consent of the person or entity submitting such information, to the DHS Inspector General.

(g) *Responding to requests made under the Freedom of Information Act or State, local, and tribal information access laws.* PCII shall be treated as exempt from disclosure under the Freedom of Information Act and any State or local law requiring disclosure of records or information. Any Federal, State, local, or tribal government agency with questions regarding the protection of PCII from public disclosure shall contact the PCII Program Manager, who shall in turn consult with the DHS Office of the General Counsel.

(h) *Ex parte communications with decisionmaking officials.* Pursuant to section 214(a)(1)(B) of the Homeland Security Act of 2002, PCII is not subject to any agency rules or judicial doctrine regarding ex parte communications with a decisionmaking official.

(i) *Restriction on use of PCII in civil actions.* Pursuant to section 214(a)(1)(C) of the Homeland Security Act of 2002, PCII shall not, without the written consent of the person or entity submitting such information, be used directly by any Federal, State or local authority, or by any third party, in any civil action arising under Federal, State, local, or tribal law.

§ 29.9 Investigation and reporting of violation of PCII procedures.

(a) *Reporting of possible violations.* Persons authorized to have access to PCII shall report any suspected violation of security procedures, the loss or misplacement of PCII, and any suspected unauthorized disclosure of PCII immediately to the PCII Program Manager or the PCII Program Manager's designees. Suspected violations may also be reported to the DHS Inspector General. The PCII Program Manager or the PCII Program Manager's designees shall in turn report the incident to the appropriate Security Officer and to the DHS Inspector General.

(b) *Review and investigation of written report.* The PCII Program Manager, or the appropriate Security Officer shall notify the DHS Inspector General of their intent to investigate any alleged violation of procedures, loss of information, and/or unauthorized disclosure, prior to initiating any such investigation. Evidence of wrongdoing resulting from any such investigations by agencies other than the DHS Inspector General shall be reported to the Department of Justice, Criminal Division, through the DHS Office of the General Counsel. The DHS Inspector General also has authority to conduct such investigations, and shall report any evidence of wrongdoing to the Department of Justice, Criminal Division, for consideration of prosecution.

(c) *Notification to originator of PCII.* If the PCII Program Manager or the appropriate Security Officer determines that a loss of information or an unauthorized disclosure has occurred, the PCII Program Manager or the PCII Program Manager's designees shall notify the person or entity that submitted the PCII, unless providing such notification could reasonably be expected to hamper the relevant investigation or adversely affect any other law enforcement, national security, or homeland security interest.

(d) *Criminal and administrative penalties.* (1) As established in section 214(f) of the CII Act, whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by