

## **Disclaimer**

On 21 December 2022, the Cybersecurity and Infrastructure Security Agency (CISA) published a final rule making technical updates to the PCII regulations. [87 Federal Register 77971]. CISA is releasing this unofficial, informal redline to assist stakeholders in reviewing the changes that the final rule makes to the regulatory text. While CISA has taken steps to ensure the accuracy of this redline, it is not an official version of the final rule and should not be relied upon for regulatory compliance purposes. This redline is not a substitute for reviewing the PCII regulation or the final rule. If any conflicts exist between this redline and the text of the PCII regulation or final rule, the documents published in the Federal Register are the controlling documents.

### **§Part 29 – Protected Critical Infrastructure Information**

#### **Sec.**

**29.1 Purpose and scope.**

**29.2 Definitions.**

**29.3 FOIA Exemptions and Restrictions on Use of PCII.**

**29.4 PCII Program Administration.**

**29.5 Requirements for Protection.**

**29.6 Acknowledgement of Receipt, Validation, and Marking.**

**29.7 Safeguarding of PCII.**

**29.8 Disclosure of PCII**

DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY

UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE

29.9 Investigation and Reporting of Violation of PCII Procedures.

1. Revise the authority citation to read as follows:

AUTHORITY: 6 U.S.C. 671-674; Section 2222-2225 of the Homeland Security Act of 2002, Pub.

L. 107–296, 116 Stat. 2135, as amended by Subtitle B of the Cybersecurity and Infrastructure

Security Act of 2018, Pub. L. 115-278, 132 Stat. 4184. 5 U.S.C. 301.

2. Revise and republish §§ 29.1 through 29.9 to read as follows:

§ 29.1 Purpose and Scope.

(a) Purpose of this Part.

part. This ~~Part~~ implements ~~sections 211 through 215 of the Homeland Security~~ Critical

Infrastructure Information Act of 2002 (HSA) through the establishment of CII Act) by

establishing uniform procedures for the receipt, care, and storage of Critical

Infrastructure Information ~~(CII)~~ voluntarily submitted to the Department of Homeland

Security ~~(DHS)~~.

~~Title II, Subtitle B, of the Homeland Security Act is referred to herein as the Critical~~

~~Infrastructure Information Act of 2002 (CII Act).~~

through CISA. Consistent with the statutory mission of DHS to prevent terrorist attacks

within the United States and reduce the vulnerability of the United States to terrorism,

~~DHSCISA~~ will encourage the voluntary submission of CII by safeguarding and protecting

that information from unauthorized disclosure and by ensuring that such information is, as

necessary, securely shared with State and ~~local government~~ Local governments pursuant to

~~section 214(a) through (g) of the CII Act.~~

~~As required by the CII Act, these rules establish procedures regarding:~~

- ~~(1) The acknowledgement~~ acknowledgment of receipt by ~~DHSCISA~~ DHSCISA of voluntarily submitted CII;

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

(2) The receipt, validation, handling, storage, proper marking, and use of information as PCII;

(3) The safeguarding and maintenance of the confidentiality of such information, and appropriate sharing of such information with State and ~~local~~ Local governments or government agencies pursuant to ~~section 2146 U.S.C. 673(a) through (g) of the HSA.~~

(1)(E); and

(4) The issuance of advisories, notices, and warnings related to the protection of critical infrastructure or protected systems in such a manner ~~as to protect~~, as appropriate, from unauthorized disclosure the source of critical infrastructure information that forms the basis of the warning, and any information that is proprietary or business sensitive, might be used to identify the submitting person or entity, or is otherwise not appropriately in the public domain.

(b) *Scope.*

handle, use, ~~or store~~ ~~PCII~~, or ~~that~~ otherwise accept receipt of PCII.

**§ 29.2 Definitions.**

For purposes of this part:-

(a) ~~Critical Infrastructure~~ has the same meaning stated in section 2 of the Homeland Security Act of 2002 (referencing 6 U.S.C. 101(4) (which cross references the term used in section 1016(e) of Public Law 107-56 (42 U.S.C. 5195c(e))) and means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

(b) ~~Critical Infrastructure Information, or CII~~ has the same meaning as established stated in section 212 of the CII Act of 2006 (U.S.C. 671(1)) and means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records or other information concerning:-

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

(1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, ~~local~~, or ~~tribal~~ Local law, harms interstate commerce of the United States, or threatens public health or safety;

(2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk-management planning, or risk audit; or

(3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(c) CII Act means the Critical Infrastructure Information Act of 2002 in 6 U.S.C. 671-674; Sections 2222-2225 of the Homeland Security Act of 2002, Pub. L. 107–296, 116 Stat. 2135, as amended by Subtitle B of the Cybersecurity and Infrastructure Security Act of 2018, Pub. L. 115-278, 132 Stat. 4168.

(d) CISA means the Cybersecurity and Infrastructure Security Agency.

(e) Department or DHS means the Department of Homeland Security.

(f) Director means the Director of the CISA, any successors to that position within the Department, or any designee.

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

(g) Executive Assistant Director means the Executive Assistant Director for the Infrastructure Security Division of the CISA, any successors to that position within the Department, or any designee.

(h) Information Sharing and Analysis Organization, or ISAO, has the same meaning as is established ~~stated~~ in ~~section 212 of the CII Act of 2002~~ 6 U.S.C. 671(5) and means any formal or informal entity or collaboration created or employed by public or private sector organizations for purposes of:

(1) Gathering and analyzing CII ~~in~~, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(2) Communicating or disclosing CII including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to critical infrastructure or protected systems; and

(3) Voluntarily disseminating CII including cybersecurity risks and incidents, to its members, Federal, State, and ~~local~~ Local governments, or any other entities that may be of assistance in carrying out the purposes specified in paragraphs (e)(1) and (2) of this section.

(d)

(i) In the public domain means information lawfully, properly, and regularly disclosed generally or broadly to the public.

Information regarding system, facility, or operational security is not “in the public domain.”

Information submitted with CII that is proprietary or business sensitive, or which might be used to identify a submitting person or entity will not be considered “in the public domain.” Information may be “business sensitive” for this purpose whether or not it is

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

commercial in nature, and even if its release could not demonstrably cause substantial harm to the competitive position of the submitting person or entity.

(e)

(j) *Local government* has the same meaning ~~as is established~~stated in ~~section 2 of the Homeland Security Act of 2002~~6 U.S.C. 101(13) and means:-

- (1) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a ~~local~~Local government;
- (2) An Indian tribe or authorized tribal organization, or in Alaska, a Native village or Alaska Regional Native Corporation; and
- (3) A rural community, unincorporated town or village, or other public entity.

(f)

(k) *Protected Critical Infrastructure Information or PCII* means validated CII, including information covered by § 29.6(b) and (h), including the identity of the submitting person or entity and any person or entity on whose behalf the submitting person or entity submits the CII, that is voluntarily submitted, directly or indirectly, to CISA, for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate purpose. PCII also includes any information, statements, compilations or other materials reasonably necessary to explain the CII, put the CII in context, or describe the importance or use of the CII when accompanied by an express statement as described in § 29.5.

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

(l) PCII Program Manager means the federal employee within the Infrastructure Security Division of CISA appointed as responsible for the administration of the PCII Program pursuant to this part, any successors to that position within the Department, or any designee.

(m) PCII Program Manager’s Designee- means a ~~Federal~~federal employee outside of ~~the~~ PCII Program Office, whether ~~employed by~~ DHSCISA or another ~~Federal~~federal agency, to whom certain functions of ~~the~~ PCII Program Office are delegated by ~~the~~ PCII Program Manager, as determined on ~~a~~ case-by-case basis.

~~(g) Protected Critical Infrastructure Information, or PCII, means validated CII, including information covered by 6 CFR 29.6(b) and (f), including the identity of the submitting person or entity and any person or entity on whose behalf the submitting person or entity submits the CII, that is voluntarily submitted, directly or indirectly, to DHS, for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate purpose, and any information, statements, compilations or other materials reasonably necessary to explain the CII, put the CII in context, describe the importance or use of the CII, when accompanied by an express statement as described in 6 CFR 29.5.~~

~~(h) Protected Critical Infrastructure Information Program, or PCII Program,~~

(n) Protected Critical Infrastructure Information Program Office or PCII Program Office means the personnel organized within the Infrastructure Security Division of CISA who carry out the operational and administrative functions of the PCII Program pursuant to the direction of the PCII Program Manager.

(o) PCII Program Officer means a Federal, State, or Local government employee appointed by their respective agency or entity and, upon approval of the PCII Program Manager, carries out

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

the responsibilities described in 6 CFR 29.4(d) to ensure the proper use, storage, and handling of PCII within their respective agency or entity.

(p) Protected Critical Infrastructure Information Program or PCII Program means the program implementing the CII Act within the Infrastructure Security Division of the CISA, including the maintenance, management, and review of the information provided in furtherance of the protections provided by the CII Act.

†

(q) Protected Critical Infrastructure Information Management System or PCIIMS means the electronic database and platform used to record the receipt, acknowledgement, validation, storage, dissemination, and destruction of PCII. PCIIMS also enables CISA to manage and train individuals authorized to view, handle, and access PCII.

(r) Protected system has the same meaning ~~set forth in section 212(6) of the CII Act, stated in 6 U.S.C. 671(6)~~ and means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

†

(s) Purposes of the CII Act has the meaning set forth in ~~section 214(a)(1) of the CII Act~~ and includes the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational ~~purpose.~~

(k) purposes.



**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

~~(t)~~ *Regulatory proceeding*, as used in ~~Section 212(7) of the CII Act~~ 6 U.S.C. 671(7) and these rules, means administrative proceedings in which DHS is the adjudicating entity, and does not include any form or type of regulatory proceeding or other matter outside of DHS.

~~(t)~~

~~(u)~~ *State* has the same meaning ~~set forth~~stated in ~~section 2 of the Homeland Security Act of 2002~~ 6 U.S.C. 101(17) and means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

~~(m)~~

~~(v)~~ *Submission* as referenced in these procedures means any transmittal, either directly or indirectly, of CII to the ~~DHS CISA~~ PCII Program ~~Manager~~Office or the PCII Program Manager's ~~designee~~Designee, as set forth herein.

~~(n)~~

~~(w)~~ *Submitted in good faith* means any submission of information that could reasonably be defined as CII or PCII under this section.

Upon validation of a submission as PCII, ~~DHSCISA~~ has conclusively established the good faith of the submission.

Any information qualifying as PCII by virtue of a categorical inclusion identified by the PCII Program Manager pursuant to ~~section 214 of the CII Act~~ and this ~~Part~~part is submitted in good faith.

~~(e)~~

~~(x)~~ *Voluntary or voluntarily*, when used in reference to any submission of CII, means the submittal thereof in the absence of an exercise of legal authority by DHS to compel access to or submission of such information.

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

Voluntary submission of CII may be accomplished by (i.e., come from) a single ~~state~~State or ~~local~~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 section ~~3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))~~—of title 15 of the United States Code—the term “voluntary” or “voluntarily” does not include ~~information:~~ (i) Information or statements contained in any documents or materials filed, pursuant to section ~~12781(i) of the Securities Exchange Act of 1934 (title 15 U.S.C. 781(i))~~, of the United States Code with the U.S. Securities and Exchange Commission or with ~~Federal~~federal banking regulators; or a

(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~~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 or SAFETY Act Designation or Certification under 6 CFR ~~Part~~part 25 will also be considered a voluntary submission.

~~(p) The term used~~

~~(y) Used directly by such agency, any other Federal, State, or local Local authority, or any third party, in any civil action arising under Federal or State law in section 2146 U.S.C.~~

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

673(a)(1)(C) of the CII Act 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 Effect of provisions.**

**FOIA Exemptions and Restrictions on Regulatory 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, ~~local~~, or ~~tribal~~ 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~~ 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~~ Designee shall not share PCII with Federal, State, or ~~local~~ Local government agencies without instituting

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

appropriate measures to ensure that PCII is used only for appropriate purposes.

**§ 29.4 ~~Protected Critical~~ PCII Program Administration.**

~~(a) Cybersecurity and Infrastructure Information Program administration.~~

~~(a) Preparedness Directorate Program Management.~~

~~Security Agency.~~ The Secretary of ~~the~~ Department of Homeland Security hereby designates ~~the~~ Under Secretary for Preparedness Director as the senior DHS official responsible for the direction and administration of the PCII Program.

~~He~~ The Director shall administer this program through the Executive Assistant ~~Secretary for~~ Infrastructure Protection.

Director.

~~(b) Appointment of a PCII Program Manager.~~

~~The~~ Under Secretary for Preparedness Director shall:

(1) Appoint a PCII Program Manager serving under the Executive Assistant ~~Secretary for Infrastructure Protection~~ 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 ~~such~~ detailees or assignees from other ~~Federal~~ federal national security, homeland security, or law enforcement entities, as the ~~Under Secretary~~ Director deems appropriate, are assigned to the PCII Program to facilitate secure information sharing with appropriate authorities; and

(4) Promulgate implementing directives and prepare training materials, as

~~ppropriate~~ appropriate, for the proper treatment of PCII.

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

(c) *Appointment of PCII Program Officers.*

The PCII Program Manager shall establish procedures to ensure that each DHS component and each Federal, State, or ~~local~~ Local agency or entity that works with PCII ~~appoint~~ appoints one or more employees to serve as a PCII Program Officer in order to carry out the responsibilities stated in paragraph (d) of this section. Persons appointed to serve as PCII Program Officers shall be fully familiar with these procedures.

(d) *Responsibilities of PCII Program Officers.*

PCII Program Officers shall:-

- (1) Oversee the handling, use, and storage of PCII;-
- (2) Ensure the secure sharing of PCII with appropriate authorities and individuals, as set forth in ~~6 CFR §~~ 29.1(a), and paragraph (b)(3) of this section;-
- (3) Establish and maintain an ongoing self-inspection program, ~~to include~~ including periodic review and assessment of ~~the~~ compliance with handling, use, and storage of PCII;-
- (4) Establish additional procedures, measures, and penalties, as necessary, to prevent unauthorized access to PCII;- and-
- (5) Ensure prompt and appropriate coordination with the PCII Program Manager regarding any request, challenge, or complaint arising out of the implementation of these regulations.

(e) *Protected Critical Infrastructure Information Management System ~~(or PCIIMS)~~.*

The PCII Program Manager shall develop, for use by the PCII Program Manager Office and the PCII Manager's ~~designees~~ Designees, an electronic database, to be known as ~~the~~ “Protected Critical Infrastructure Information Management System” (PCIIMS), to record the receipt, acknowledgement, validation, storage, dissemination, and destruction of PCII.

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

~~This compilation of PCII shall be safeguarded and protected in accordance with the provisions of the CII Act.~~

~~The PCII Program Manager may require the completion of appropriate background investigations of an individual before granting that individual access to any PCII.~~

**§ 29.5 Requirements for ~~protection~~ Protection.**

(a) CII shall receive the protections of ~~section 214 of~~ the CII Act when:-

(1) Such information is voluntarily ~~submitted, directly or indirectly, to the PCII Program Manager~~ Office or ~~the~~ PCII Program Manager's ~~designee~~ Designee;

(2) The information is submitted for ~~protected use regarding the security of critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate purposes including, without limitation, for the identification, analysis, prevention, preemption, disruption, defense against and/or mitigation of terrorist threats to the homeland;~~

(3) The information is labeled with an ~~express statement as follows~~:-

(i) Documentary submissions. In the case of documentary ~~submissions, a~~ written marking on the ~~information or records substantially similar to the following: “This information is voluntarily submitted to the Federal federal government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002”; or 2002, as amended by the Cybersecurity and Infrastructure Security Act of 2018”;~~

(ii) Oral submissions. In the case of oral ~~information~~ submissions:

(A) Through an oral statement, made ~~at the time of the oral submission or within a reasonable period of time~~ thereafter, ~~indicating an expectation of protection from disclosure as provided by the provisions of the CII Act; and~~

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

(B) Through a written statement ~~substantially similar to the one specified above~~ in paragraph (a)(3)(i) of this section accompanied by a document that ~~memorializes the nature of the~~ oral information submission initially provided ~~received by~~ to the PCII Program ~~Manager~~ Office or the PCII Program Manager's ~~designee~~ Designee within a ~~reasonable period of time~~ after using making the oral ~~submission~~; ~~and or~~

(iii) Electronic submissions. In the case of electronic ~~information~~ submissions:

(A) Through an electronically ~~submitted~~ statement ~~made~~ within a reasonable period of time ~~after making~~ the electronic submission, ~~indicating an expectation of protection from disclosure as provided by the provisions of the CII Act~~; ~~and or~~

(B) Through a non-electronically ~~submitted~~ written statement ~~substantially similar to the one specified above~~ in paragraph (a)(3)(i) of this section accompanied by a document that ~~memorializes the nature of e-mailed information~~ the electronic submission initially provided; ~~to be received by~~ the PCII Program ~~Manager~~ Office or the PCII Program Manager's ~~designee~~ Designee within a reasonable period after ~~using email~~ making the electronic ~~submission~~; ~~and~~

(4) The ~~submitted information additionally~~ documentary, electronic, or oral submission is accompanied by a ~~statement~~, signed by the submitting ~~person~~ or an authorized person ~~on behalf~~ of an entity identifying the ~~submitting person or entity~~, containing ~~such contact information as is considered necessary by the PCII Program Manager Office~~, and certifying that ~~the information being submitted is not customarily in the public domain~~;

(b) Information that is not submitted ~~to the PCII Program Manager Office~~ or the PCII Program Manager's ~~designees~~ Designees will not ~~qualify for protection under the CII Act~~.

~~Only the PCII Program Manager Office~~ or ~~the a~~ PCII Program Manager's ~~designees~~ Designee

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

are  ~~authorized~~ to acknowledge receipt of  ~~information~~  ~~being~~ submitted for  ~~consideration~~ of protection under the  ~~CII~~ Act.

(c) All Federal, State, and  ~~local~~ Local government entities shall protect and  ~~maintain~~ information as required by  ~~these~~ rules  ~~or~~ and by the provisions of the  ~~CII~~ Act when that information is  ~~provided~~ to the entity by the PCII  ~~Program~~ Manager or  ~~the~~ a PCII Program  ~~Manager's~~  ~~designee~~ Designee and is marked as  ~~required~~ in  ~~6 CFR §~~ 29.6(c).

(d) All submissions seeking PCII  ~~status~~ shall be presumed to have been  ~~submitted~~ in good faith until validation  ~~or a determination not to validate~~  is made pursuant to  ~~these rules.~~ this part.

**§ 29.6 Acknowledgment of  ~~receipt, validation~~ Receipt, Validation, and  ~~marking.~~ Marking.**

(a) *Authorized officials.*

~~Only the~~  ~~DHS~~ PCII Program Manager is authorized to  ~~validate,~~ and mark information  ~~as PCII.~~ submitted for protection outside of a categorical inclusion as PCII. The PCII Program Manager or  ~~the~~ a Program Manager's  ~~designees,~~ Designee may mark  ~~information~~ qualifying for protection under categorical  ~~inclusions~~ pursuant to  ~~6 CFR 29.6(f).~~ paragraph (f) of this section as PCII.

(b) *Presumption of protection.*

~~All~~  ~~information~~ submitted in accordance  ~~with~~ the procedures set forth  ~~hereby in~~  § 29.5 of this part will be presumed to be and will be  ~~treated~~ as PCII, enjoying the protections  ~~of section 214~~ of the CII Act, from the  ~~time~~ the information is received by the  ~~PCII~~ Program Office or  ~~the~~ a PCII Program  ~~Manager's~~  ~~designee.~~ Designee. The information  ~~shall~~ remain protected unless and until  ~~the~~ PCII Program Office renders a final  ~~decision~~ that the information is not  ~~PCII.~~

~~The~~ PCII Program Office will, with  ~~respect~~ to information that is not  ~~properly~~ submitted,



**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

inform the submitting person or entity within thirty calendar days of receipt, by a means of communication to be prescribed by the PCII Program Manager, that the submittal was procedurally defective.

The submitter will then have an additional ~~30~~ thirty calendar days to remedy the deficiency from the date of receipt of such ~~notice~~.

notification by the PCII Program Office. If the submitting person or entity does not cure the deficiency within thirty calendar days ~~or after~~ the date of receipt of the notification provided by the PCII Program Office in this paragraph, the PCII Program Office may determine that the presumption of protection is terminated.

Under such circumstances, the PCII Program Office may cure the deficiency by labeling the submission with the information required in ~~6 CFR~~ § 29.5 or may notify the applicant that the submission does not qualify as PCII.

No CII submission will lose its presumptive status as PCII except as provided in ~~6 CFR~~ 29.6 paragraph (g) of this section.

*(c) Marking of information.*

All PCII shall be clearly identified through markings made by the PCII Program Office.

The PCII Program Office shall mark PCII materials as follows: “This document contains PCII.

In accordance with the provisions of 6 CFR ~~Part~~ part 29, this document is exempt from release under the Freedom of Information Act (5 U.S.C. 552(b)(3)) and similar laws requiring public disclosure. Unauthorized release may result in criminal and administrative penalties.

This document is to be safeguarded and disseminated in accordance with the CII Act and ~~the~~ PCII Program requirements.” When distributing PCII, the distributing person shall ensure that the distributed information contains this marking.

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

(d) *Acknowledgement of receipt of information.*

The PCII Program Office or ~~the~~ a PCII Program Manager's ~~designees~~ Designee shall acknowledge receipt of information submitted as CII and accompanied by an express statement, and in so doing shall:-

(1) Contact the submitting person or entity, within thirty calendar days of receipt of the submission of CII, by the means of delivery prescribed in procedures developed by the PCII Program Manager.

In the case of oral submissions, receipt will be acknowledged in writing within thirty calendar days after receipt by the PCII Program Office or ~~the~~ a PCII Program Manager's ~~designee~~ Designee of a written statement, certification, and documents that memorialize the oral submission, as referenced in ~~6 CFR~~ § 29.5(a)(3)(ii);-

(2) Enter the appropriate data into the PCIIMS as required in ~~6 CFR~~ § 29.4(e);- and-

(3) Provide the submitting person or entity with a unique tracking number that will accompany the information from the time it is received by the PCII Program Office or ~~the~~ a PCII Program Manager's ~~designees~~ Designee.

(e) *Validation of information.*

(1) The PCII Program Manager shall be responsible for reviewing all submissions that request protection under the CII Act.

The PCII Program Manager shall review the submitted information as soon as practicable.

If a final determination is made that the submitted information meets the requirements for protection, the PCII Program Manager shall ensure that the information has been marked as required in paragraph (c) of this section, notify the submitting person or entity of the determination, and disclose it only pursuant to ~~6 CFR~~ § 29.8.

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

(2) If the PCII Program Office makes an initial determination that the information submitted does not meet the requirements for protection under the CII Act, the PCII Program Office shall:-

(i) Notify the submitting person or entity of the initial determination that the information is not considered to be PCII.

This notification also shall, as necessary:-

(A) Request that the submitting person or entity complete the requirements of ~~6 CFR~~ § 29.5(a)(4) or further explain the nature of the information and the submitting person or entity's basis for believing the information qualifies for protection under the CII Act;-

(B) Advise the submitting person or entity that the PCII Program Office will review any further information provided before rendering a final determination;-

(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 submitting person or entity, or destroyed.

If a request for withdrawal-return is made, all such information shall be returned to the submitting person or entity.

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

(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 shall return~~ the information ~~is not PCII,~~ to the ~~PCII Program Office, submitter~~ in accordance with the submitting person or entity's written preference, ~~shall, and the procedures set forth in paragraph (e)(2)(i) of this section~~ within thirty calendar days of making a final determination, ~~return the that the information submitted is not eligible for protections under the CII Act. If the submitting person or entity cannot be notified or the submitting person or entity's response is not received within thirty calendar days of the date of the notification as provided in paragraph (e)(2)(i) of this section, the PCII Program Office shall make the initial determination final and return the~~ information to the submitter.

If return to the submitter is impractical, the PCII Program Office shall destroy the information within ~~30~~thirty calendar days. This process is consistent with the appropriate National Archives and Records Administration-approved records disposition schedule.

~~If the submitting person or entity cannot be notified or the submitting person or entity's response is not received within thirty calendar days of the date of the notification as provided in paragraph (e)(2)(i) of this section, the PCII Program Office shall make the initial determination final and return the information to the submitter.~~

(f) *Categorical Inclusions of Certain Types of Infrastructure CII as PCII.*

The PCII Program Manager has discretion to declare certain subject matter or types of information categorically protected as PCII and to set procedures for receipt and processing of such information.

Information within a categorical inclusion will be considered validated upon receipt by the PCII Program Office Manager or any of the PCII Program Manager's designees without further review, provided that the submitter provides the express statement required by

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

~~section 214(a)(1). Designees~~ § 29.5(a)(3). The PCII Program Manager's designees shall provide to the PCII Program ~~Manager~~ Office information submitted under a categorical inclusion.

(g) *Changing the status of PCII to non-PCII.*

Once information is validated, only the PCII Program ~~Office~~ Manager 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 received under ~~6 CFR~~ § 29.8.

**§ 29.7 Safeguarding of Protected Critical Infrastructure Information. (a) Safeguarding of PCII.**

*(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, ~~DHSCISA~~ will, to the extent practicable and consistent with the purposes of the CII Act, undertake appropriate background checks to ensure that individuals with access to PCII do not pose a threat to national security.

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

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 **and** 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 **CII** Act, for Automated Information Systems that contain PCII.

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

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~~. PCII.**

(a) *Authorization of access.*

The ~~Under Secretary for Preparedness Director~~, the ~~Executive Assistant Secretary for Infrastructure Protection Director~~, or either's designee may choose to provide or authorize access to PCII under one or more of the ~~subsections below~~ paragraphs in this section 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 Office~~ or ~~the~~ PCII Program Manager's ~~designees~~ Designee may provide PCII to an employee of the ~~Federal~~ federal government, provided, subject to ~~subsection~~ paragraph (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~~ Local government entity for the purpose of protecting critical infrastructure or protected systems, or in furtherance of ~~an~~ the investigation or ~~the~~ prosecution of a criminal act. The provision of PCII to a State or ~~local~~ 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

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

acknowledging the understanding and responsibilities of the recipient. State and ~~local~~ 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~~ 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 applicable criminal code or ~~to the applicable~~ employee code of conduct for the jurisdiction.

~~(e) Disclosure of information to Federal, State and local government contractors.~~

~~(c) Disclosure of **PCII** information to Federal, State, and ~~local~~ Local government contractors.~~

Disclosure of PCII to Federal, State, and Local government contractors may be made when necessary for an appropriate purpose under the CII Act, and only after the PCII Program Manager or a PCII Program 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 a~~ PCII Program Manager's ~~designee, Designee,~~ communicate with a submitting person ~~or an authorized 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 a PCII Program Manager's Designee, without the prior written approval of the PCII Program Manager or ~~the a~~ PCII Program Manager's ~~designee, Designee.~~



**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

(d) *Further use or disclosure of information by State, and local governments.*

~~(1) State and local~~ 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 a PCII Program Manager’s ~~designee~~ 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 a~~ a PCII Program Manager’s ~~designees~~ Designee, who shall be responsible for requesting and obtaining written consent from the submitter of the information.

(2) State and ~~local~~ 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, of the Department of Homeland Security, the Director, the Executive Assistant Secretary for Cyber Security and Telecommunications, or Assistant Secretary Director~~ for Infrastructure Protection Security of CISA, or the Executive Assistant Director for Cybersecurity of CISA. Such exigent circumstances exist only when approval of the Secretary, the ~~Under Secretary for Preparedness, Director, the Executive Assistant Secretary Director~~ for Cyber Infrastructure

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

Security ~~and Telecommunications~~ for CISA, or the ~~Executive~~ Assistant ~~Secretary~~ Director for ~~Infrastructure Protection~~ Cybersecurity for CISA 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, alert, 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.* ~~(f)~~

(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~~ the investigation or ~~the~~ prosecution of a criminal act by the ~~Federal~~ federal government, or by a State, ~~local~~ Local, or foreign government, when such disclosure is coordinated by a ~~Federal~~ 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 a~~ PCII Program Manager's ~~designee~~ Designee; or

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

(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 DHSCISA 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 Office of Inspector General.

(g) *Responding to requests made under the Freedom of Information Act or State, local, and tribal Local government information access laws.*

PCII shall be treated as exempt from disclosure under the Freedom of Information Act and any State or local Local government law requiring disclosure of records or information.

Any Federal, State, local, or tribal Local government agency with questions regarding the protection of PCII from public disclosure shall contact the PCII Program Manager Office, who shall in turn consult with the DHS-CISA Office of the General Chief Counsel.

(h) *Ex parte communications with decisionmaking decision-making officials.*

Pursuant to ~~section 214.6 U.S.C. 673(a)(1)(B) of the Homeland Security Act of 2002,~~ PCII is

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

not subject to any agency rules or judicial doctrine regarding ex parte communications with a ~~decisionmaking~~ decision-making official.

(i) *Restriction on use of PCII in civil actions.*

Pursuant to ~~section 2146 U.S.C. 673(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~~ Local authority, or by any third party, in any civil action arising under Federal, State, ~~local~~, or ~~tribal~~ Local law.

**§ 29.9 Investigation and ~~reporting~~ Reporting of violation Violation of PCII ~~procedures.~~**

**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~~ a PCII Program Manager's ~~designees.~~

Designee. Suspected violations may also be reported to the DHS Office of Inspector General.

The PCII Program Manager or ~~the~~ a PCII Program Manager's ~~designees~~ Designee shall in turn report the incident to the appropriate ~~Security Officer~~ security officer and to the DHS Office of Inspector General.

(b) *Review and investigation of written report.*

The PCII Program Manager, or the appropriate ~~Security Officer~~ security officer shall notify the DHS Office of 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 United States Department of Justice,

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

Criminal-~~Division~~, through the DHSCISA Office of the ~~General~~ Chief Counsel.

~~The~~ DHS Office of Inspector-~~General~~ also has authority to conduct-~~such~~ investigations, and shall report any-~~evidence~~ of wrongdoing to the- United States 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~~security officer~~ determines-~~that~~ a loss of information or an-~~unauthorized~~ disclosure of PCII has occurred,-~~the~~ PCII Program Manager or ~~thea~~ PCII-~~Program~~ Manager's ~~designees~~Designee 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,~~ 6 U.S.C. 673(f), 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~~ law, any information protected from-~~disclosure~~ by the CII Act coming to the-~~officer~~ or employee in the course of his-~~or~~ her employment or official duties or-~~by~~ reason of any examination or-~~investigation~~ made by, or return, report,-~~or~~ record made to or filed with, such-~~department~~ or agency or officer or-~~employee~~ thereof, shall be fined under-~~title~~ 18 of the United States Code,-~~imprisoned~~ not more than one year, or-~~both~~, and shall be removed from office-~~or~~ employment.

(2) In addition to the penalties set-~~forth~~ in paragraph (d)(1) of this section,-~~if~~ the PCII Program Manager determines-~~that~~ an entity or person who has-~~received~~ PCII has violated the-~~provisions~~

**DRAFT – PRE-DECISIONAL – FOR OFFICIAL USE ONLY**

**UNOFFICIAL REDLINE OF PCII TECHNICAL FINAL RULE**

of this ~~Part~~part or used PCII for ~~an~~ inappropriate purpose, the PCII ~~Program~~ Manager may disqualify that ~~entity~~ or person from future receipt of ~~any~~ PCII or future receipt of any ~~sensitive~~ homeland security information ~~under section 892 of the Homeland Security Act~~ under 6 U.S.C. 482, provided, however, that ~~any~~ such decision by the PCII Program ~~Manager~~ may be appealed to the ~~Office of the Under~~ Director.

DRAFT