Billing Code: 9110-9P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 29

RIN: 1601-AA77

Updates to Protected Critical Infrastructure Information Program

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Advance notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security (DHS) proposes to update its procedures for accepting Critical Infrastructure Information (CII) as a step towards meeting the challenges of evolving technology and identifying ways to make the PCII Program's protective measures more effective for information-sharing partnerships between the government and the private sector. The Critical Infrastructure Information Act of 2002 authorizes DHS to establish a program to accept information relating to critical infrastructure voluntarily submitted from the public, owners and operators of critical infrastructure, and State, local, tribal, and territorial governmental entities, while limiting public disclosure of that sensitive information under the Freedom of Information Act and other laws, rules, and processes. To implement this authority, DHS issued the "Procedures for Handling Critical Infrastructure Information" Final Rule in 2006. This Advance Notice of Proposed Rulemaking (ANPRM) provides an opportunity for DHS to hear and consider, during the development of new regulations to update DHS's PCII program, the views of the private and public sector, and other interested members of the public on their recommendations for program modifications, particularly subject matter

areas that have developed significantly since the issuance of the initial rule, such as automated information sharing.

DATES: Written comments must be submitted on or before **[INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by one of the following methods:

- Federal eRulemaking Portal: -- http://www.regulations.gov. Follow the instructions for submitting comments.
- Mail: -- U.S. Department of Homeland Security, National Protection and Programs Directorate, Office of Infrastructure Protection, Infrastructure Information Collection Division, 245 Murray Lane, SW, Mail Stop 0602, Washington, DC 20528-0602.

FOR FURTHER INFORMATION CONTACT: Emily R. Hickey, Deputy Program Manager, by phone at (703) 235-9522 or by mail at Protected Critical Infrastructure Information Program, Office of Infrastructure Protection, Infrastructure Information Collection Division, 245 Murray Lane, SW, Mail Stop 0602, Washington, DC 20528-0602.

SUPPLEMENTARY INFORMATION:

Abbreviations and Terms Used in This Document

ANPRM – Advance Notice of Proposed Rulemaking

CFR – Code of Federal Regulations

CII – Critical Infrastructure Information

CII Act of 2002 – Critical Infrastructure Information Act of 2002

DHS – Department of Homeland Security

PCII – Protected Critical Infrastructure Information

I. Background

The Department of Homeland Security receives sensitive information about the nation's critical infrastructure through its congressionally-mandated PCII Program. The PCII Program provides a secure environment for the private sector, government analysts, and other subject matter experts to share information that is vital to addressing concerns across all critical infrastructure sectors. The Critical Infrastructure Information Act of 2002 (Sections 211-215, Title II, Subtitle B of the Homeland Security Act of 2002, Public Law 107-296) (CII Act of 2002) established the PCII Program, which assures owners and operators that the information they voluntarily submit is protected from public disclosure. Only trained PCII Authorized Users, with a specific "need-to-know", can access PCII and use it only for homeland security purposes. In accordance with the CII Act of 2002, on September 1, 2006, DHS issued the PCII Program Final Rule (71 FR 52271, codified at 6 CFR part 29). This rule established procedures that govern the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to DHS. The procedures are applicable to all Federal, State, local, tribal, and territorial government agencies and contractors that have access to, handle, use, or store critical infrastructure information that enjoys protection under the CII Act of 2002.

After 10 years of operation, changes are needed to transition the managing of submissions, access, use, dissemination and safeguarding of PCII to state of the art technology that operates within an electronic environment. Throughout this ANPRM DHS discusses and seeks comment on the economic impact of transitioning the PCII

Program to a preferred electronic environment that: (1) Enhances the submission and validation process for critical infrastructure information, (2) uses state of the art technology for an automated interface for quicker access and dissemination of PCII, (3) modifies requirements for the express and certification statements; (4) expands the use of categorical inclusions; (5) requires portion marking of PCII; and (6) implements specific methods to capture and deliver metadata to the PCII Program.

This ANPRM also seeks comment on proposals to revise the overall approach for: (1) Automated submissions and an expansion of categorical inclusions, (2) marking PCII, (3) sharing PCII with foreign governments, (4) regulatory access, (5) safeguarding, (6) oversight and compliance, (7) alignment with other information protection programs, and (8) the administration of PCII at the State, local, tribal, and territorial level.

The CII Act of 2002 requires that all voluntary submissions (physical and electronic) of CII, for which protection is requested, are submitted to DHS, directly or indirectly, include an "express statement" and a "certification statement" with each submission. The "express statement" informs the PCII Program Office that the information in question is being voluntarily submitted to the Federal government in expectation of protection from disclosure as provided by the provisions of the CII Act of 2002. The "certification statement" includes the submitter's contact information and certifies that the information in question is not customarily in the public domain and is not being submitted in lieu of complying with a regulatory requirement. This ANPRM seeks comments on automating the submission process so that the transition to a preferred electronic environment captures the "express statement" and "certification statement" in an efficient manner.

Additionally, the ANPRM seeks comments on expanding submissions of CII through categorical inclusions and developing a consistent method for collecting the metadata on those categorical inclusions. "Categorical inclusions" are a means of creating a class of presumptively valid information, thus expediting the process of acceptance as PCII. The PCII Program Manager has the discretion to declare certain subject matter or types of information categorically protected as PCII and to set procedures for the receipt and processing of that information. CII submitted within a categorical inclusion will be considered validated upon receipt by the PCII Program Office or any of the Designees without further review, provided the submitter includes an "express statement" and the PCII Program Manager has pre-validated that type of information as PCII. The PCII Program Manager must appoint a Designee before an entity can establish a categorical inclusion. Currently, only Federal entities or systems or programs managed and overseen by a Federal employee can make use of the categorical inclusion.

The regulations at 6 CFR part 29 also authorize DHS (or the PCII Program Manager) to establish procedures to ensure that any DHS component or other Federal, State, local, tribal, or territorial entity that works with PCII understands and implements the policy and procedural requirements necessary to appropriately receive, use, disseminate, and safeguard PCII in compliance with the requirements of the CII Act and the associated regulations. Since the publication of the PCII Final Rule, the program has met several significant milestones and receives ongoing nationwide participation from Federal, State, local, tribal, and territorial partners. To date, the PCII Program has

received submissions from owners and operators across all 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or cyber, are considered so vital to the United States that their degradation, incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

As the PCII Program continues to expand throughout the nation, the PCII Program Office has to extend its efforts to perform effective oversight and compliance, accurate identification of PCII in a variety of materials, access and safeguarding of PCII, statistical reporting, and the tracking of PCII shared and disseminated within the critical infrastructure community.

II. Written Comments

A. In General

This ANPRM provides an opportunity for DHS to hear and consider the views of owners and operators of critical infrastructure and other interested members of the public on their recommendations for PCII Program modifications and improvements.

DHS invites interested persons to submit written comments, data, or views on how the current PCII Program regulations, codified at 6 CFR part 29, "Procedures for Handling Critical Infrastructure Information," might be improved. Comments that would be most helpful to DHS include the questions and answers identified in Part III of this document. Please explain the reason for any comments with available data, and include other information or authority that supports such comments. DHS encourages interested parties to provide specific data that documents the potential costs of modifying the existing rule requirements pursuant to the commenter's suggestions; the potential

quantifiable benefits including security and societal benefits of modifying the existing regulatory requirements; and the potential impacts on small entities of modifying the existing regulatory requirements.

DHS requests that commenters discuss potential economic impacts, whenever possible, in terms of quantitative benefits and costs when providing feedback on this ANPRM. DHS also requests that commenters provide any special circumstances related to small entities or uniquely high costs that small entities may bear.

DHS requests that commenters discuss economic impacts in as specific terms as possible. For example, if a policy change would necessitate additional employee training, then helpful information would include the following: the training courses necessary; the types of employees or contractors who would receive the training; topics covered; any retraining necessary; and the training costs if conducted by a third-party vendor or in-house trainer. DHS invites comment on the time and level of expertise required to implement commenter suggestions, even if dollar-cost estimates are not available.

DHS requests that commenters discuss economic impacts concerning the transition of the PCII Program to a preferred electronic environment. In addressing the transition from the paper environment to the electronic environment, DHS encourages interested parties to provide specific data that documents the potential costs of transforming the PCII Program to an electronic environment. DHS is seeking information on potential quantifiable benefits including security and societal benefits of the transition and cost data on the potential impact of the transition and how a preferred electronic environment could impact the number of voluntary submittals. In particular,

DHS is seeking comment on how many potential submitters would not have access to the internet and any costs relating to expenses associated with obtaining internet access for those entities without such access. This could include internet fees and any costs for applicable software and training that would be necessary to facilitate electronic submission of critical infrastructure information for protection as PCII or travel costs (time and mileage costs) needed to acquire a location with internet access. Commenters might also address how DHS can best obtain and consider accurate, objective information and data about the costs, burdens, and benefits of automating the PCII Program and whether there are lower cost alternatives that would allow DHS to achieve its goal of automating the PCII Program.

Feedback that simply states a stakeholder feels strongly that DHS should modify the PCII Program, without including actionable data, including how the proposed change would impact the costs and benefits of the PCII Program, is much less useful to DHS. To help DHS organize and review all comments, please identify the relevant provision of 6 CFR part 29 that relates to the specific comment provided (e.g., 6 CFR 29.9 (d) Criminal and administrative penalties). Commenters may comment on topics related to the current 6 CFR part 29 not included in this ANPRM as well as those questions posed in this ANPRM.

Written comments may be submitted electronically or by mail, as explained previously in the **ADDRESSES** section of this ANPRM. To avoid duplication, please use only one of these methods to submit written comments.

Except as provided below, all comments received, as well as pertinent background documents, will be posted without change to http://www.regulations.gov, including any personal information provided.

B. Handling of Proprietary or Business Sensitive Information

Interested parties are encouraged to submit comments in a manner that avoids discussion of trade secrets, confidential commercial or financial information, CII or PCII, or any other category of sensitive information that should not be disclosed to the general public. If it is not possible to avoid such discussion, however, please specifically identify any confidential or sensitive information contained in the comments with appropriate warning language (e.g., any PCII must be marked and handled in accordance with the requirements of 6 CFR 29.5 through 29.7) and submit them by mail to the PCII Program Manager listed in the **FOR FURTHER INFORMATION CONTACT** section.

DHS will not place any confidential or sensitive comments in the public docket; rather, DHS will handle them in accordance with applicable safeguards and restrictions on access. See, e.g., 6 CFR 29.5 through 29.7. See also the DHS PCII Procedures Manual ("Protected Critical Infrastructure Information Program," April 2009, located on the DHS website at www.dhs.gov/protected-critical-infrastructure-information-pcii-program). DHS will hold any such comments in a separate file to which the public does not have access, and place a note in the public docket that DHS has received such materials from the commenter. DHS will provide appropriate access to such comments upon request to individuals who meet the applicable legal requirements for access to such information.

III. Questions for Commenters

The transition from a paper-based PCII Program to a preferred electronic PCII Program must be addressed and managed on many different and complex levels: administratively, financially, culturally, technologically, and institutionally. This ANPRM seeks comments on making the transition to a preferred electronic PCII Program that is practicable. This ANPRM's goal is to adopt solutions that streamline workflow performance rather than continuing existing processes that are becoming outdated.

To help DHS identify ways, if any, to improve the manner in which it administers PCII, DHS seeks public comments on any and all aspects of 6 CFR part 29. This ANPRM seeks comments from all interested parties and subject matter experts and other private and public organizations associated within the Information Technology and cyber security fields. Areas that DHS is most interested in receiving comments on include, but are not limited to, the following:

a. Automated Submissions. Currently, all submitters are required to include an "express statement" and a "certification statement" with each CII submission (physical and electronic). This ANPRM seeks comments on modifying this requirement to allow multiple associated CII submissions under one "express statement" and "certification statement." Comments 1 through 3 concern the automated submissions of express and certification statements, comments 4 through 5 concern internal and external statistical reporting, and comments 6 through 9 concern the expansion of categorical inclusions. Specifically, we are requesting:

    1) Comments on how to enhance the submission methods for critical infrastructure information and automate sharing via structured information expression profiles and electronic exchange protocols

such as the Structured Threat Information eXpression (STIX) and the Trusted Automated eXchange of Indicator Information (TAXII);

2) Comments on whether an updated PCII rule should permit multiple submissions of information under one express statement and certification statement enabling the submission of multiple documents by an organization over the course of several weeks or months, all relating to an identified incident, and whether such submission should be treated and tracked as one submission;

3) Comments on whether an updated PCII rule should allow submissions in a purely electronic format that includes an electronic express statement and certification statement in order to simplify the submission of large data sets in particular, such as electronic submissions with a large volume of data potentially indicating a compromise of a critical information system;

4) Currently, the PCII Program does not have an automated process for collecting statistical information on each submission. For this reason, this ANPRM seeks comments outlining whether and to what extent an automated submission process should incorporate auditing and statistical reporting requirements to increase transparency of the frequency and types of data being submitted to the program;

5) Currently, the PCII Program does not facilitate the submitter's ability to request and receive audits or access data relating to the submission. This ANPRM seeks comments addressing any process amendments or

program enhancements to effectively implement automated submission processing in order to facilitate the submitter's ability to request and receive timely audits of access to the submissions and to withdraw the data submitted to the program via an automated process;

6) Comments about what effect, if any, an updated PCII Program would have on enabling broader sharing and analysis among other trusted recipients of cyber threat and risk data, including potential concerns related to protecting sources and methods;

7) Comments on the extent to which specific programmatic-submission use cases that define data collection needs should be developed and established as categorical inclusions in specific data exchange activities in order to increase the submitters' community use and ease of submission in the PCII submission process, and to foster broader use of the PCII Program; and

8) Categorical inclusions enjoy a presumption of protection for CII relating to certain subject matters that the PCII Program Manager declares as PCII. Additionally, the PCII Program Manager sets procedures for receipt and processing of such information. This ANPRM seeks comments on the extent to which specific programmatic-submission use cases should be developed and established as categorical inclusions in order to normalize a range of permissible and impermissible uses for specific types of data shared as PCII; and

9) Currently, categorical inclusions exist in Federal governmental entities. This ANPRM seeks comments on expanding categorical inclusions to the State governmental level to increase the range of submissions, enhance the efficiency of information sharing, and make the protection of critical infrastructure information more effective.

b. Marking/Portion Marking – The purpose of the portion marking process is to identify what information within a submission of critical infrastructure information should be protected. Presently, submitters are not required to portion mark the submitted information. The PCII Program Office does not currently mark portions of submitted information as PCII or non-PCII within the steps of the validation process. If the submitted information is validated as PCII, the entire submission is given protection as PCII. Additionally, metadata practices are not streamlined so that it is received in a uniform process. This ANPRM seeks comments regarding the marking of PCII as it relates to the Controlled Unclassified Information (CUI) framework, to include comments on portion marking of original PCII, and the marking of PCII metadata.

c. Sharing PCII with Foreign Governments – To date the PCII Program does not share PCII with foreign governments, however it is possible to do so through sharing agreements. This ANPRM seeks comments regarding the sharing of PCII with trusted international partners identified through sharing agreements to support the critical infrastructure protection and resilience efforts of the United States and partner governments.

d. Regulatory Purposes – Comments on whether the current information in 6 CFR part 29 is sufficient to describe the restriction on regulatory access to PCII. See sections 29.2(k) and 29.3 of 6 CFR part 29.

e. Safeguarding – Comments on all aspects of PCII safeguarding, including comments on storage, violations of unauthorized disclosure, dissemination, tracking and use of PCII, and destruction of same.

f. Oversight and Compliance – Currently, oversight and compliance within the PCII Program ensures that all critical infrastructure activities are in accordance with the CII Act of 2002 and 6 CFR part 29. This ANPRM seeks comments relating to broadening the oversight and compliance of the PCII Program to enhance assessment and measure the effectiveness of compliance with PCII Program policies, procedures and practices.

g. Alignment with other information protection programs – Comments regarding how DHS may be able to better align the PCII Program with other existing information protection and sharing programs, such as the Transportation Security Administration's Sensitive Security Information program, the Department of Homeland Security's Chemical-Terrorism Vulnerability Information program, and the National Archives and Records Administration Controlled Unclassified Information Program, including comments on any duplication or overlap that may exist between the PCII Program and another information protection programs. When providing comments on this topic, DHS encourages commenters to provide the specific citations to any information protection programs that may duplicate or

overlap with the PCII requirements as well as a specific description of the duplicative or overlapping requirement.

h. Administration of PCII Program in States – Comments on streamlining the administration of the PCII Program within State, local, tribal, and territorial entities by including State, local, tribal, and territorial Homeland Security Advisors in the management of the PCII Program so that states are accredited in their entirety and aligned with the requirements of the PCII Program.

In each of the above cases, DHS also requests that the commenter provide, in as much detail as possible, an explanation why the procedures should be modified, streamlined, expanded, or removed, as well as specific suggestions of the ways DHS can better achieve its protective objectives for sharing information about the nation's critical infrastructure.

In addressing these topics, DHS encourages interested parties to provide specific data that documents the potential costs of modifying the existing regulatory requirements pursuant to the commenter's suggestions; the potential quantifiable benefits including security and societal benefits of modifying the existing procedures; and the potential impacts on small businesses of modifying the existing regulatory requirements. Commenters might also address how DHS can best obtain and consider accurate, objective information and data about the costs, burdens, and benefits of the PCII Program and whether there are lower cost alternatives that would allow DHS to continue to achieve its goal of protecting sensitive security information on the nation's critical infrastructure consistent with the CII Act of 2002.

Jeh Charles Johnson,

Secretary

[FR Doc. 2016-09186 Filed: 4/20/2016 8:45 am; Publication Date: 4/21/2016]