U.S. Communications
Sector Coordinating Council

July 20, 2016

VIA ELECTRONIC FILING
Attn: 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

Re: Updates to Protected Critical Infrastructure Information Program

This letter is submitted by the Communications Sector Coordinating Council (CSCC) in response to the U.S. Department of Homeland Security's (DHS) Advance Notice of Proposed Rulemaking (ANPRM) issued on April 21, 2016, to update DHS procedures for accepting Critical Infrastructure Information (CII) and identifying ways to make the Protected Critical Infrastructure Information (PCII) Program's protective measures more effective for information-sharing partnerships between the government and the private sector.

The CSCC is comprised of five segments including broadcast, cable, wireless, wireline, and satellite, and represents over 33 U.S. companies and trade associations. Our sector is one of 16 Critical Infrastructure/ Key Resource (CI/KR) sectors. Council members have participated in the PCII Program, and have been actively following developments and issues related to the Program.

To continue to encourage participation from industry, and to enable the long-term success of the PCII Program, DHS should preserve or expand all existing protections for participants in the PCII Program. The CSCC is appreciative of the PCII Program's robust protections, and believes that these protections have been mutually beneficial to the government and the private sector in promoting transparency, visibility, and dialogue around cybersecurity. Any modifications that reduce protections for program participants, or create an undue burden on participants, could undermine the Program's success. Accordingly, DHS should weigh any proposed changes with an eye toward avoiding unintended consequences.

Among the critical protections that enable private sector participation and advance the Program's viability, the language of the Critical Infrastructure Information Act of 2002 ("the CII Act") is clear that the Congress' goal was to facilitate the exchange of sensitive, propriety information through the use of voluntarily shared information with specific protections against a government agency using the information in regulatory proceedings and enforcement actions. According to the statute, the voluntary submission of CII to a covered Federal agency "does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory

proceedings."[1] Further, without written consent of the person or entity submitting the CII, the CII Act prohibits Federal agencies, any other Federal, State, or local authority, or any third party from using such information in a civil action arising under Federal or State law if the information is submitted in good faith.[2]

DHS seeks comments on whether the current language in 6 CFR 29 is sufficient to describe the protections and clear restrictions on access to PCII for regulatory and enforcement purposes. The current rules restrict the use of PCII by Federal, State, and local agencies, specifying that agencies that receive PCII may utilize the PCII only for purposes appropriate under the Act, and are prohibited from using the PCII for any other collateral regulatory purposes without the written consent of the PCII Program Manager and the submitting person or entity.[3] The Council supports this limited access to PCII and believes that the current rules on this issue should not change, for they strike the appropriate balance between agencies' legitimate interests in PCII, and the submitting person or entity's interest in protecting such information.

The current rules allow a person or entity submitting CII to withdraw the CII either before DHS completes its validation that the CII should be deemed PCII,[4] or after DHS changes the status of a submission from PCII to non-PCII.[5] This important protection should be expanded to allow a person or entity to withdraw a submittal that has been deemed PCII by categorical inclusion pursuant to 6 CFR 29.6(f), or validated as PCII pursuant to 6 CFR 29.6(e). This change will afford the person or entity a meaningful degree of additional protection should the party determine that DHS or a third party with access to the PCII under the rules is not itself protecting the PCII in accordance with the statute, the rules, or the person or entity's expert opinion; or a third party is likely to misuse or misinterpret the PCII.

The current rules also call for DHS to, among other things, oversee the handling, use, and storage of PCII;[6] and ensure the secure sharing of PCII with appropriate authorities and individuals. More specifically, "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."[7] To develop greater trust in the relationship between DHS and submitting persons or entities, and thus encourage voluntary participation in the PCII program, a person or entity planning to submit PCII to DHS should have the right to review the procedures established pursuant to 6 CFR § 29.7 before the submission of information.

Further, to the extent that DHS seeks to streamline the administration of the PCII Program within State, local, tribal, and territorial entities, these entities should adhere strictly to the existing requirements of the PCII program to protect the information voluntarily shared by participating entities. The more information is shared with entities that are not in a position to support the PCII protections, the greater the risk that the information will be compromised.

---

[1] *Critical Infrastructure Information Act of 2002*, § 212 (7), available at https://www.dhs.gov/sites/default/files/publications/CII-Act-508.pdf.
[2] *Id.*, at § 214 (a)(1)(c).
[3] 6 CFR § 29.3 (b), § 29.8 (f).
[4] 6 CFR § 29.6 (e)(2)(i)(C).
[5] 6 CFR § 29.6 (g).
[6] 6 CFR §29.4.
[7] 6 CFR § 29.7.

States and localities are not immune to having data compromised. In recent years, government-maintained databases in multiple states have been breached, compromising the sensitive personal data of millions of Americans nationwide.[8] Thus, DHS should work with parties that may submit CII to develop a questionnaire about security of information held at the state and local levels, including, but not limited to, who will be able to access the information; and how will it be stored. That questionnaire, and/or answers to it, should be updated with some frequency (e.g., annually) to account for the ever-changing nature of threats and best practices for securing data. Finally, a person or entity should have the right to review the procedures for the handling, use, and storage of PCII put in place by a third party that has access to the party's PCII under this program.

To achieve the stated goal of adopting solutions that streamline workflow performance for PCII, DHS should refrain from incorporating into the automated submission process auditing and statistical reporting requirements and should automate sharing using protocols other than TAXII and formats other than STIX.

DHS has asked whether and to what extent an automated submission process should incorporate auditing and statistical reporting requirements in order to increase the transparency of the frequency and types of data being submitted to the program. While transparency is a laudable goal in most circumstances, in this instance, it could undermine the goals of the PCII program, as information created from these requirements could be used as a *de facto* metric, which could lead to problematic behaviors. The requirements could discourage private sector entities from sharing information through the PCII program. For instance, if that the information shows that Sector A had fewer PCII submissions than Sector B, Sector B could respond by reducing its number of future submissions in order to create the appearance of increased security. Further, he ANPRM is not clear on what the overall goal and purpose would be for auditing or statistical purposes, what the information would ultimately be used for, and who would have access to it.

To the extent that any such requirements are enacted, the information gleaned from these requirements should be used for internal agency purposes only.

DHS also asked how it could enhance and automate sharing. Threat information should be available to consumers in an automated fashion using protocols other than TAXII and formats other than STIX. Specifically, the Comma Separated Value (CSV) format data should be made available over HTTPS using the same authentication mechanisms as the current DHS TAXII server. The inordinate complexity of STIX and TAXII and the lack of open source tools available to retrieve that data and extract it into a useful form create a nearly insurmountable barrier to participation for any company that cannot afford an expensive commercial solution.

---

[8] *See, e.g.,* Kristina Torres, "Georgia tries to contain fallout from data breach," Atlanta Constitution Journal (Nov. 19, 2015), available at http://www.myajc.com/news/news/state-regional-govt-politics/georgia-tries-to-contain-fallout-from-data-breach/npRSJ/; Jaikumar Vijayan, "Texas comptroller takes blame for major breach," Computer World (Apr. 29, 2011), available at http://www.computerworld.com/article/2508352/security0/texas-comptroller-takes-blame-for-major-breach.html; News 4 Jax, "DCF suffers major security breach" (Apr. 17, 2015), available at http://www.news4jax.com/news/local/dcf-suffers-major-security-breach-; and Molly Young, "Data breach, manager resignation point to more Employment Department woes," The Oregonian/Oregon Live (Oct. 10, 2014), available at http://www.computerworld.com/article/2508352/security0/texas-comptroller-takes-blame-for-major-breach.html.

DHS sought comments on whether PCII should be shared with trusted international partners. Sharing PCII with foreign entities raises unique considerations. In general, the more information shared with entities that are not in a position to support the PCII protections, the greater the risk that the information will be compromised. While sharing agreements that protect PCII and the limitations on its use would be critical in such circumstances, the U.S. may not have the means to enforce these agreements with foreign entities. This could ultimately compromise any PCII shared with foreign entities. In addition to these concerns, certain threshold questions, such as who are "trusted international parties," what is the purpose of sharing, and how would these trusted parties use the information – should be answered.

To the extent that DHS recommends sharing PCII with foreign entities, DHS should ensure that the circumstances for sharing such information are narrowly tailored, limited to partners with an established level of trust, include formal assurances that information will be appropriately handled and protected, and allow the person or entity submitting the PCII to withdraw it before it is shared with a foreign entity.

On behalf of the Communications Sector Coordinating Council members, we are grateful to DHS for undertaking updates to the PCII Program, and look forward to continuing to engage on this matter.

Sincerely,

Nneka Chiazor	Kathryn Condello	Rudy Brioché
Verizon	CenturyLink	Comcast Corporation
Chair, CSCC	Vice Chair, CSCC	Secretary, CSCC