CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

R. BRUCE JOSTEN
EXECUTIVE VICE PRESIDENT
GOVERNMENT AFFAIRS

1615 H STREET, N.W.
WASHINGTON, D.C. 20062-2000
202/463-5310

May 20, 2004

Ms. Janice Pesyna
Office of the General Counsel
Department of Homeland Security
Washington, DC 20528

Re: Comments to Procedures for Handling Critical Infrastructure Information; Interim Rule

The United States Chamber of Commerce (the "Chamber") appreciates the opportunity to comment on the Procedures for Handling Critical Infrastructure Information, Interim Rule.

The Chamber is the world's largest business federation, representing more than three million businesses and organizations of every size, sector and region. We provide the following comments on behalf of the Chamber's Homeland Security Policy Task Force.

Specific Comments on the Interim Rule

We believe that the interim rule matches closely with the intent, spirit, and letter of the Critical Infrastructure Information Act of 2002. We support the goal of the interim rule, which is to increase the level of information sharing between the public and private sectors, and believe that the Act and the interim rule are a necessary first step in meeting this goal.

Specifically, the Chamber believes the following sections are especially important in enhancing information sharing:

- Section 29.2 *Definitions*: We support the clarification that submissions from Information Sharing Organizations such as industry specific Information Sharing and Analysis Centers do qualify for protection under the Critical Infrastructure Information Program.

- Section 29.3 (b) *FOIA Disclosure Exemptions*: We support the language clarifying that the FOIA exemption [provided in Section 214(a)(1)(A) of the CII statute] is a separate exemption [under 5 USC 552(b)(3)], and that any inapplicability of that exemption will not affect the applicability of other FOIA exemptions [e.g., under 5 USC 552(b)(4) for confidential business information]. Note, however, that adding references, such as we have done here, would provide even greater clarity.

- Section 29.6 (b) *Presumption of Protection*: We support the language that presumes that submitted information is protected. Having this presumption is necessary to encourage companies to share information.

- Section 29.8 *Disclosure of Protected Critical Infrastructure Information*. We support the language that sets conditions on when protected information is shared with state and local governments, and federal contractors, and the language that limits the use of the information. In addition, we support the protections of subsection (g) (1), which states that protected information that is shared by the Program Manager or designee with state and local governments is protected from disclosure under state FOIA laws.

- Section 29.8 (i) *Restrictions on Use of Protected CII in Civil Actions*. Companies that voluntarily share their critical, sensitive data to enhance homeland security should be free to do so without fear that DHS will turn such information over to other authorities so that this information can subsequently be used against the companies in civil actions. Therefore, we strongly support the protections reiterated in this section.

While recognizing the positive aspects of the interim rule, we must also raise several areas that need clarification or amendment.

- A general concern with the CII Program as established by the interim regulations is that the regulations and/or Program will discourage the private sector from continuing to provide DHS with CII directly and rapidly through existing time-sensitive initiatives and offices including the Indications Analysis and Warnings (IAW) program and the Homeland Security Operations Center

(HSOC). Because both of these efforts function effectively only when they are provided information on a rapid, "as-occurring" basis, they cannot work in a system where CII determinations do not occur instantly. Thus, we believe that the regulations should specify that CII material will be afforded fully protected status when provided to DHS through any such time-sensitive program or office. The regulations could be written to specify by name each such eligible program or office, as well as a mechanism for said programs and offices to convey that CII material to the CII program for further appropriate handling. As well, note the suggestion below at Section 29.5(a)(3)(ii) regarding the need to facilitate rapid, ongoing oral communications during major incidents.

- In addition, the interim regulations as worded give the reader the impression that all prior-submitted CII will not be given Protected CII status, even though at least some was submitted specifically pursuant to assurances that it would be so protected. In order to further assure the private sector that CII will be completely afforded all available protections, and thus encourage the private sector to continue providing CII to DHS, the regulations must clarify that information already provided to DHS pursuant to a written or verbal assurance of confidentiality under the CII Act and other applicable provisions, even though submitted prior to the inception of the CII Program established in the interim regulations, will be fully afforded status as Protected CII.

- A further general concern relates to the ability of DHS to protect information shared with other entities. There have been incidents recently where sensitive information was broadly released to the public after having been shared with other governmental entities. In order to give private owners and operators of critical infrastructure assurance that sensitive information will remain confidential if provided to the government voluntarily, we urge DHS to pay particular attention to creating procedures, incentives, and disincentives assuring that all CII will remain confidential once shared by DHS. Note in particular the suggestion below relating to Section 29.8(j) – Disclosure to Foreign Governments.

- Section 29.3 *Effect of Provisions.* This section would be enhanced by adding a provision mirroring the provision in Section 214 (a)(1)(F) of the CII statute,

which indicates that submissions will "not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection." It is important to repeat this phrase in the rule to assure that this intent is carried forward to DHS contracts with states, local governments, and contractors implementing these rules. It should also recognize that this applies regardless of whether the information is ultimately deemed to be Protected CII.

- Section 29.4(e) *Protected Critical Infrastructure Information Management System (PCIIMS).* This section states that an electronic tracking system will be developed to track submitted information. We recommend that this section be clarified to state that the actual protected information itself will not be part of this system.

- Section 29.5 (a) (3ii) *Requirements for Protection.* This section states that in cases of oral submissions, a submitter has 15 days to request CII classification. The interim rule does not clarify the status of orally submitted information during those 15 days. We therefore request that this section be clarified to state that during that 15 day window, orally submitted information will be fully protected from disclosure in order to give an incentive to companies to engage in oral communications. Also, we request that "writing" be clarified to include e-mail or facsimile transmissions.

- Additionally, during incidents that disrupt the operations of a critical infrastructure sector (or sectors), it is expected that the federal government and the private sector will be in near-constant communication to discuss recovery and reconstitution efforts. At such times, it is unrealistic to expect either government officials or private sector representatives to keep detailed records on conversations. Therefore, we propose that the requirement to follow up in writing be waived during Catastrophic Incidents, Incidents of National Significance and Major Disasters or Emergencies, as defined in the National Response Plan. At such times, all conversations between the DHS or other regulatory agencies, and the owners and operators of critical infrastructure facilities related to such incidents, should receive Protected Critical Infrastructure Information status.

- Section 29.5 (a)(4) *Requirements for Protection.* We question the need for the requirement that submitted information be accompanied by a certifying statement. This requirement raises potential criminal liability and acquisition issues for federal contractors in case of a misstep. Furthermore, we note that no certification is required by the CII statute. Rather, the only statutory requirement is for the "express statement" specified in CII Section 214(a)(2) and reiterated in Section 29.5(a)(3) of the rules. Moreover, the text of the certification requires in (iii) the submission of details that are neither critical to determining whether CII is protected, nor implicitly or explicitly required by the CII statute. This is a substantial disincentive to participation which appears unnecessary.

- Section 29.5 (b) *Requirements for Protection.* We recommend that this section be clarified to state that when information is inadvertently submitted to someone other than the Protected CII Program Manager, the person or agency that received the information shall treat it as protected and not copy or release it. This is, of course, prior to the existing obligation to turn this information over to the CII Program Manager.

- Section 29.6 (d)(3) *Acknowledgement of Receipt of Information.* This section states that submitters will be given a tracking number so that they can review the status of their CII request. This raises two questions: 1) will the PCIIMS be a public database? and 2) can a reviewer check the status of another submitter? We recommend that this section make clear that PCIIMS is not a public database and that appropriate security steps will be taken so that reviewers cannot check the status of any submissions other than his or her own.

- Computer-based management of PCII requests is important, given the approach taken by DHS generally presuming that submissions are not protected until so designated. Likewise, PCII itself must be protected once received, and in many instances such PCII will be maintained in IT systems and systems of records. Therefore, both PCII and PCII requests should be secured at a high level as required by the Federal Information Security Management Act (FISMA) and defined in NIST Federal Information Processing Standard 199 (FIPS-199), "Standards for Security Categorization of Federal Information and

Information Systems," and in related FIPS special publications. Our recommendation here is likewise applicable to Section 29.7 (b) *Use and Storage*, *Section* 29.7 (d) *Disposal of Information*, and Section 29.7 (e) *Transmission of Information*.

- Section 29.6 (e) (2)(E)(ii) *Acknowledgement of Receipt, Validation, and Marking*. This section concerns the use of submitted information that is determined to not meet the protected requirements. We support the language that provides the submitter with the option of having the information destroyed or held by DHS without protection. However, we are concerned with the language that enables the Program Manager to override the choice of the submitter. In this section of the interim rule, the Program Manager can independently determine that the information is of law enforcement importance and, therefore, not only keep it, but also share it with law enforcement— all without informing the submitter. We request that the Program Manager be granted no such discretion and that it be deleted from the rule. If DHS insists on keeping this discretion in the rule, then we request this section include guidelines on how the Program Manager should determine how such information might have law enforcement value, and immediately notify the submitter that the information was shared with law enforcement and not destroyed. Furthermore, we believe any such guidelines should also be subject to public comment before this section of the PCII rule becomes effective.

- We would also recommend that DHS add a requirement to store information determined not to be Protected CII in the same manner as Protected CII, pending destruction, if the submitter has asked that it be destroyed (or in a more stringent manner, based on the nature of the information and separately applicable legal protections). This is particularly important for CII that may be covered by another FOIA exemption (e.g., confidential business information).

- Section 29.7 (b) *Use and Storage*. This section states that "reasonable steps" shall be taken to secure protected information and that it shall be stored "in a secure environment that affords it the protection commensurate with its vulnerability and sensitivity." This appears to permit the Program Manager to provide tiered

levels of security measures and determine what information falls into which tier. We believe that all Protected CII should be stored in the same secure manner, and that the rule should provide further guidance to the Program Manager as to what methods are appropriate for securing the information. See also our comment above regarding information held for destruction.

- Section 29.7 (d) *Disposal of Information.* This section should clarify that the information will be disposed of in accordance with the Federal Records Act. This will ensure consistency with Section 29.6 (e)(2)(E), which states that information must be disposed of in accordance with the Federal Records Act. Further clarity would also be helpful so that submitting parties are aware of the processes used by DHS to comply with those general statutory requirements.

- Section 29.7 (e) *Transmission of Information.* We recommend that this section be changed to state that the Program Manager or designee will use only secret or encrypted communication protocols to transmit Protected CII documents.

- Section 29.8 (a)(2) *Disclosure; Authorization of Access.* Further clarity, and an opportunity for public comment, would be appreciated regarding how DHS will determine whether and how CII is "proprietary" or "business sensitive." Will the submitter need to assure that such claims are detailed with the submission, and that a FOIA exemption under 5 USC 552 (b)(4) is claimed with the submission?

- Section 29.8 (j) *Disclosure to Foreign Governments.* This section states that Protected CII documents can be disclosed to foreign governments without the written consent of the submitter. We believe that neither the Homeland Security Act or the Critical Infrastructure Information Act authorizes the release of Protected CII to foreign governments. Furthermore, we contend that there are obvious problems with such releases created by the sometimes dramatic differences among the world's legal systems. Therefore, we request that this section be deleted in its entirety. If DHS believes transmitting this information to foreign governments is absolutely essential, we especially ask that his section be reworded to clarify that only "warnings" based on Protected CII, but not actually including any Protected CII itself, are covered, as

contemplated under Sections 214(g) and 214(e)(2)(D) of the CII Act.

- Section 29.9 (c) *Notification to Originator of Protected CII.* This section states that the Program Manager will notify the submitter if information is lost or an unauthorized access has occurred. We recommend that this section be changed so that the submitter is notified every time there is a disclosure of CII documents, including to law enforcement.

- Additionally, if an individual identifier will be established for information submitted seeking PCII status, and if such identifier will link to personally identifiable information regarding the submitter, then the information submitted may be protected under the Privacy Act of 1974. That is, protections under the Privacy Act such as individual access, ability to protect records, and requirements for federal Register publication of routine disclosures may be afforded to individuals involved in submitting PCII. This issue should be examined to determine applicability of the Privacy Act to any part of the submissions process, including retained and transmitted data.

- Finally, we would encourage further efforts on two matters mentioned in the preamble but not addressed in the rules, i.e., the additional exploration of how to facilitate protection of indirect submittals through other federal agencies (e.g., the FCC), and how to address potential overlap with rules of other agencies protecting sensitive information (e.g., the Transportation Security Administration). The draft rules had an acceptable proposal for indirect submissions that would adequately address the first issue. Regarding the second issue, DHS could clarify that otherwise protected information [such as "SSI" designated by TSA or the Coast Guard, or "CEII" designated by the Federal Energy Regulatory Commission] will remain subject to those protections when obtained and used by DHS for critical infrastructure protection purposes. See 44 U.S. Code Sec. 3510(b).

Thank you for your consideration. We would be pleased to provide you with further comments or clarifications upon request.

Sincerely,

R. Bruce Josten