

American Petroleum Institute.txt

Subject: Comments on DHS CII Proposed Rule
Date: Sun, 15 Jun 2003 21:58:00 -0400
From: "Kendra Martin" <Martink@api.org>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Please find attached comments from the American Petroleum Institute on the Department of Homeland Security's proposed Rulemaking on "Procedures for Handling Critical Infrastructure Information."

API Oil & Gas Security Seminars
& Vulnerability Assessment Workshops
August 6-8, Los Angeles, CA

Visit www.api.org/events for details!

Kendra L. Martin
CIO & Security Team Leader
American Petroleum Institute
1220 L Street, NW
Washington, DC 20005-4070
USA
Phone: 202-682-8517
Fax: 202-682-8207
E-mail: martink@api.org

View the New www.api.org

DHS CII Final Comments.doc Name: DHS CII Final Comments.doc
 Type: WINWORD File (application/msword)
 Encoding: base64
 Description: DHS CII Final Comments.doc

June 15, 2003

Office of the Secretary
Department of Homeland Security
“Procedures for Handling Critical Infrastructure Information”
6 CFR Part 29
RIN 1601-AA14

The American Petroleum Institute (API) is pleased to provide comments on the April 15, 2003 Federal Register Notice of Proposed Rulemaking on “Procedures for Handling Critical Infrastructure Information” (68 Fed. Reg. 18524 – 29) to implement Section 214 of the Homeland Security Act of 2002. The American Petroleum Institute is a national trade organization representing over 400 companies involved in all aspects of the oil and natural gas industry including exploration, production, refining, marketing, distribution and marine activities. API members are owners/operators of critical infrastructure and, as such, have a direct interest in the procedures for handling critical infrastructure information.

API believes that this proposed regulation for protecting critical infrastructure information (CII) provided to DHS will provide most of the necessary protections desired by industry. However, API is very concerned that the exception to these protections for information “not submitted in good faith” is a major flaw which could potentially undermine the overall protection intended by this regulatory effort, and thereby undermine security enhancement.

Therefore, API recommends that this provision (Section 29.6(f)) of the regulations be deleted, as it contradicts the intent of the Homeland Security Act of 2003, and will place a chill on the ongoing cooperation of critical infrastructure facilities to share critical information. Moreover, as drafted the exception is based on a subjective determination of “bad faith” and contains no provisions for safe keeping of the information. If the exception is retained, it needs objective criteria and strict procedures for notifying the submitter and careful return or disposal of the information.

General

Nearly 90 percent of the nation’s critical infrastructure – physical and computer networks for production and delivery of energy, food, water, telecommunications, financial services, health care, chemicals and other raw materials, essential products and services –

are owned and controlled by the private sector. Furthermore, they are largely interconnected with, and interdependent upon, each other.

Many of these companies may want to share critical infrastructure threat and vulnerability information with the government but have been concerned about the security risks that would result from its public disclosure under the Freedom of Information Act (FOIA) or similar requirements. API understands that an effective partnership between government and industry to protect the nation's critical infrastructure must be built on a foundation of trust and cooperation. One of the most important elements for a successful partnership will be for industry to have the assurance that CII provided to DHS will be properly protected and that, if issues with that information do arise, the relationship will be in place that will enable matters to be resolved in a way that continues to protect the information. For the most part, the proposed regulations would enable DHS to develop a program to provide such assurances.

Specific Comments on the Proposed Rule

- Section 29.6(f) would allow the CII Program Manager to determine that information was not submitted in good faith in accordance with the CII Act of 2002. In addition, the CII Program Manager would **NOT** be required to notify the submitter that the information does not qualify as Protected CII. API has concerns with this provision for the following reasons:
 - API believes the proposed exemption from protection against disclosure for information submitted in "bad faith" was never intended by the statute. Rather, the statutory provision in the CII Act of 2002 is quite narrowly drawn and is clearly intended to protect information voluntarily submitted from, among other protections, use in civil litigation if submitted in good faith.
 - The proposed rule acknowledges that this provision is the only exception to the notice requirement of the procedures. The notion that a determination could be made that information was submitted in bad faith and the submitter would not necessarily be made aware of this determination is contrary to the intent of the statute, the rest of the proposed rule and is inconsistent with the spirit of cooperation.
 - If the CII Program Manager makes a determination that information voluntarily provided to DHS was not done so in good faith, then that information would not have the CII protection. Does that mean that DHS would then disclose, if asked? If this is the case, API strongly opposes this provision, especially if this could occur and the submitter would not be aware since there is no obligation for DHS to notify the submitter in the first place.

- There is no description of the criteria the CII Program Manager would use to make a determination that information was not provided in good faith. Objective criteria, such as a *material* failure to submit information in accordance with the procedures as outlined in § 29.5, must be developed.

API Recommendations for provision 29.6(f):

- Delete this provision
 - If retained, revise the provision to include a requirement that the CII Program Manager must notify the submitter that it has been determined that the information was not submitted in good faith
 - Revise the provision to incorporate the same wording as in 29.6(e) which describes the procedures that CII Program Manager would use if information was determined not to qualify for CII protection.
- Section 29.6(g) states that the CII Program Manager or his designee may change the status of protected CII to non-protected CII and remove the protected CII markings. However, the provision does not describe the situations contemplated for this to take place nor does it describe the notification process if it does occur. API recommends that this section be clarified to state that the submitter must request, in writing, that the information be changed from protected to non-protected CII or, if that determination is made by DHS based on particular circumstances, that the procedures in 29.6(e) will be used.
 - Section 29.7(f) mentions the use of “secure electronic means” as a method of transmission of protected CII. API suggests that this phrase be explained or clarified so it is clear to the submitter what the options are. DHS should provide a variety of electronic means based on current and widely used transmission mechanisms.
 - Section 29.8(b) permits the CII Program Manager to share protected CII with employees of the federal government or of a state or local government provided that such information is shared for the purposes of securing critical infrastructure. API recommends that this provision be clarified to indicate that the CII Program Manager will make a judgment on the validity of the request to ensure that the requesting agency/organization has a clearly defined statutory role in homeland security or critical infrastructure protection.

API appreciates the opportunity to comment on this proposed rule to protect CII. With the resolution of our above comments, we think the proposal is largely consistent with the intent of CII Act of 2002 and will serve as a solid foundation for a government-industry partnership that will protect our nation’s critical infrastructure.