American Petroleum Institute

1220 L Street, Northwest
Washington, DC 20005-4070
Tel 202-682-8517
Fax 202-682-8207
E-Mail martink@api.org

Kendra L. Martin
Chief Information Officer & Security Team Leader

May 20, 2004

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

RE: "Procedures for Handling Critical Infrastructure Information" (2/20/04; 69 FR 8074); 6 CFR Part 29; RIN 1601-AA14

Ms. Pesyna:

The American Petroleum Institute (API) is pleased to provide comments on the February 20, 2004 Federal Register notice on the interim rule for "Procedures for Handling Critical Infrastructure Information" (69 FR 8074) to implement Section 214 of the Homeland Security Act of 2002. API 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 that are established for handling Protected critical infrastructure information (CII).

API generally supports this interim rule on the protection of CII because it should provide adequate protection of voluntarily submitted information to protect critical infrastructure. In addition, API is pleased that the majority of our comments submitted on the June 15, 2003 proposed rule (attached) have been addressed in this interim rule. However, in an effort to make the program more effective and better protect critical infrastructure, additional provisions should be incorporated into the rule stating that anytime Protected CII is shared outside DHS, the submitter should be notified as such.

The comments below seek further explanation or clarification of certain provisions of the interim rule that will help API members better understand the CII Program.

One of the most important elements for a successful public-private partnership will be for the critical infrastructure facilities to have the assurance that any CII provided to DHS (which can then be shared with other government agencies and even foreign governments) will be properly protected. If issues with that information do arise, a relationship will be in place, enabling matters to be resolved while continuing to protect

the information. For the most part, this rule should enable DHS to implement a program to provide such assurances.

Specific Comments on the Interim Rule

- The section on *Protected CII Program Management and Administration* in the preamble discusses a phased approach that will eventually expand the points of entry for Protected CII within DHS. Consistent with this approach and as described in Homeland Security Presidential Directive – 7, "Critical Infrastructure Identification, Prioritization and Protection", API encourages DHS to expand the Protected CII Program to allow the Sector-Specific Federal Agencies to also become points of entry for Protected CII.

- Section 29.7(e) *Transmission of Information* has been revised to state that Protected CII shall be submitted by secure means of delivery, as determined by the Protected CII Program Manager or the designees. While API understands that this wording is meant to provide flexibility, it would be useful for DHS to provide some examples of what type of secure delivery may be determined to be appropriate.

- Section 29.8(b) has clarified how Protected CII may be shared with other Federal, State, and local government agencies. API believes it is imperative that the Protected CII Program Manager takes necessary steps to ensure that the requesting agency/organization has a clearly defined statutory role in homeland security or critical infrastructure protection and thereby is likely to have a need for such information.

- Section 29.8(j) *Disclosure to Foreign Governments* permits the sharing of Protected CII with foreign governments without the written consent of the submitter. As stated above, API believes the submitter should be notified prior to the release of Protected CII outside DHS. Moreover, API remains very concerned about the release of Protected CII to foreign governments, as it is not clear what criteria would be used to determine if the foreign government has a legitimate need for such information, nor how such governments would be able to protect the information consistent with this interim rule. Finally, if the information is not protected consistent with the rule, neither DHS nor the submitter has any specified recourse with the foreign government.

  API suggests that Protected CII not be shared with foreign governments and, thus, this section be deleted. If this is not acceptable, API suggests, at a minimum, that the submitter be notified that Protected CII is being shared with a foreign government and that DHS has taken the necessary steps to ensure that the foreign government has procedures in place to properly protect the Protected CII from public disclosure. In addition, DHS should more clearly define the potential circumstances under which this information may be shared with the foreign governments.

API appreciates the opportunity to comment on this rule. With the resolution of the above comments, the interim rule is largely consistent with the intent of the Critical Infrastructure Information Act of 2002 and will serve as a solid foundation for government-industry information sharing that will help protect our nation's critical infrastructure.

Sincerely,

Kendra L. Martin