

Chevron Texaco.txt
Subject: ChevronTexaco Comments to DHS: Procedures for Handling CII
Date: Fri, 13 Jun 2003 11:39:18 -0400
From: "Diaz, Katlyn (Katlyn)" <Katlyn@chevrontexaco.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Please accept these comments from ChevronTexaco on Procedures for Handling
Critical Infrastructure Information - 6CFR Part 29, RIN 1601-AA14.

<<6CFRPart29.pdf>>
Katlyn Diaz CIH, CSP

Chevrontexaco
Public and Government Affairs, Policy and Political Affairs
6001 Bollinger Canyon Rd. (A-2140), San Ramon, CA 94583
Tel 925 842 3427 Fax 925 842 3618 Mobile 925 765 2606

mailto:katlyn@chevrontexaco.com

6CFRPart29.pdf Name: 6CFRPart29.pdf
 Type: Acrobat (application/pdf)
 Encoding: base64
 Description: 6CFRPart29.pdf

ChevronTexaco
Washington, DC Office
1401 Eye Street, NW, Suite 1200
Washington, DC 20005
Tel 202 408 5800
Fax 202 408 5845

Philip T. Cavanaugh
Vice President Federal and
International Government Relations

ChevronTexaco

June 12, 2003

Associate General Counsel (General Law)
Department of Homeland Security
Washington, DC 20528

**Re: Procedures for Handling Critical Infrastructure Information
6 CFR Part 29
RIN 1601-AA14**

Dear Madam or Sir:

ChevronTexaco appreciates this opportunity to provide comments on DHS's April 15, 2003 Federal Register Notice of Proposed Rulemaking concerning Procedures for Handling Critical Infrastructure Information (68 Federal Register 18524-18529).

ChevronTexaco is an integrated energy company, involved in every aspect of the energy industry. Our operations range from oil and gas exploration and production to transportation, refining and retail marketing, as well as chemicals manufacturing and sales and power production. We are committed to protecting our personnel and assets around the world.

We offer the following comments:

1. The proposal makes reference to "protecting Critical Infrastructure Information (CII) from being disseminated to the general public". We would like see clear language in the final rulemaking that security-related, company-confidential information submitted to the Government is protected from Freedom of Information Acts (FOIA).
2. The proposed rule for protecting CII applies only to information that is voluntarily provided to local, State, and Federal governments. The scope should be extended to protect security-related, company confidential information (e.g. vulnerability assessments, security plans, and other E&HS information) that is required to be submitted to local, State and Federal governments if disclosure may increase a facility's security vulnerability or compromise the company's competitive position. Information that is independently obtained per section 29.3(d) should also be protected if disclosure may increase a facility's vulnerability.

3. The logistics for transmitting information to the Government are not clear. We recommend that this be clarified in the final rulemaking.
4. We are concerned that these procedures do not offer adequate protection against unauthorized access. One can deduce in 29.7(b) that protected CII has no provision to ensure confidential information be secured in a locked desk or file cabinet during working hours, as long as "reasonable" steps are taken to minimize the risk of access by unauthorized personnel. This omission contradicts certain basic and universal tenets of good security practices. We recommend that the final rulemaking specify protection against unauthorized access that is consistent with recognized security practices.
5. The FBI and DOE have been marking voluntarily submitted information as "secret" and as such are required to follow procedures for its handling. The proposed rule says that voluntarily submitted information should be marked with "This information is voluntarily submitted to the Federal Government *in expectation of protection from disclosure* ..." We recommend that the marking have a stronger statement that is consistent with existing U.S. information protection classification systems. This would be in line with 29.6(b) which states there is a presumption of protection.
6. It is not clear what level of screening or background clearance an authorized individual must have to receive, handle or store CII information. The DHS needs to clarify this issue in the final rulemaking.
7. If the CII Program Manager determines that information is not submitted in good faith, then the information does not qualify as Protected CII. Under this condition, there is no requirement to notify the submitter. First, the criteria for determining "good faith" should be defined in the rule. Second, the CII Program Manager should be required to notify the submitter such as that required in 29.6(e)(1)(ii). Because of the sensitive nature of material supplied, the Program Manager should protect information submitted until the issue is resolved with the submitter.
8. Foreign governments are included in the scope of the proposed regulation, however they are not mentioned in section 29.9(d), criminal and administrative penalties. It is not defined how the U.S. Government will verify that foreign governments are following the CII protection process. Further, the DHS needs to define how the U.S. Government will enforce criminal and administrative penalties if the process is not being followed.
9. There are two sections that may increase a facility's vulnerability, and in so doing, would discourage voluntary reporting. For this reason, we believe the following two sections should be deleted:
 - Section 29.8(a) states that the Under Secretary of IAIP may choose to authorize access to protected CII when it supports a lawful and authorized Government purpose as enumerated in the CII Act of 2002, *other law, regulation, or legal authority*. This appears to be contradictory with section 29.3(c) which states that

"Federal agencies shall not utilize CII for regulatory purposes without the written consent of the submitter."

- Section 29.8(j) says that the CII Program Manager may provide protected CII to foreign governments without the consent of the submitter . . . "in furtherance of an investigation or the prosecution of a criminal act."

If these sections are deemed necessary, then they should be revised to provide, at a minimum, advance notification to the submitter that such disclosure will be made and assurances that any such disclosure will be narrowly tailored to fit the necessity and protect the identity and security of the submitter or facility to the fullest extent possible.

10. We agree that persons who work with protected CII should be personally responsible for following the procedures and there should be criminal and administrative penalties if they violate the rule as noted in section 29.9(d).

Thank you for the opportunity to comment on this rule. If you have any questions please contact Katlyn Diaz at 925-842-3427.

Sincerely,

A handwritten signature in cursive script, appearing to read "Philip T. Cavanaugh for".

Philip T. Cavanaugh