

American Chemistry Council.txt
Subject: Comments of American Chemistry Council on CIIA Proposed Rules
Date: Fri, 13 Jun 2003 16:38:22 -0400
From: <James_Conrad@americanchemistry.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

(See attached file: CIIA comments.doc)

* * * * *

James W. Conrad, Jr.
Counsel
American Chemistry Council
1300 Wilson Blvd.
Arlington, VA 22209

703-741-5166
703-741-6092 (fax)
703-405-1660 (cell; not always on)
james_conrad@americanchemistry.com

CIIA comments.doc Name: CIIA comments.doc
 Type: WINWORD File (application/msword)
 Encoding: base64
 Description: CIIA comments.doc

June 16, 2003

Associate General Counsel (General Law)
Department of Homeland Security
Washington, D.C. 20528

Re: Comments on Proposed Procedures for Handling Critical Infrastructure
Information, 68 Fed. Reg. 18524 (April 15, 2003)

Dear Sir or Madam:

The American Chemistry Council (the Council or ACC) appreciates this opportunity to provide these comments on the Department of Homeland Security's (DHS's) proposed rules implementing the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131-34 (CIIA or the Act). The Council represents the leading companies engaged in the business of chemistry. Council members apply the science of chemistry to make innovative products and services that make people's lives better, healthier and safer. The Council is committed to improved environmental, health and safety performance through Responsible Care[®], common sense advocacy designed to address major public policy issues, and health and environmental research and product testing. The business of chemistry is a \$460 billion enterprise and a key element of the nation's economy. It is the nation's largest exporter, accounting for ten cents out of every dollar in U.S. exports. Chemistry companies invest more in research and development than any other business sector.

The business of chemistry is part of the nation's critical infrastructure, a fact recognized by the President's *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Feb. 2003) (at 65-66). It is a critical sector both in its own right and because it provides resources essential to the functioning of most other critical sectors, including national defense, health care and information technology.

The Council actively supported the CIIA, as its members and other representatives of critical infrastructure sectors had been unable to most effectively share and analyze information about threats, vulnerabilities and responses, either among themselves or



with government, due to concerns about release of information under the Freedom of Information Act and state open records laws, antitrust liability, application of the Federal Advisory Committee Act to industry/government meetings, and possible tort or compliance liability. Fortunately, the CIIA speaks to all of those concerns.

The Council is pleased that DHS has proposed these regulations to implement the CIIA. In the main, the Council strongly supports the proposal and commends DHS for hewing to the spirit of the CIIA. *Of particular urgency, ACC requests DHS to promptly confirm that CIIA Section 214(a) is effective now.* The following pages address that point, as well as (i) a series of provisions that the Council particularly supports, (ii) areas where the Council has concerns or requests clarification, and (iii) additional steps that DHS should take promptly to complete the CIIA implementation process.

Discussion

I. DHS Should Promptly Confirm that CIIA Section 214(a) is Effective Now

At this writing, Council member companies are expressing concern that critical infrastructure information (CII) they may submit to DHS might not be protected by the CIIA since this rulemaking has not been finalized. This concern is an obstacle to our members assisting with current DHS projects.

The Council supports DHS's issuance of these proposed rules. Nonetheless, in our view the existence of final implementing rules is not a condition precedent to effectiveness of Section 214(a) of the CIIA. We believe that provision is self-implementing and became effective on November 25, 2002. While Section 214(e) calls on DHS to "establish procedures" for handling CII, DHS correctly notes that this provision does not require DHS to promulgate those procedures by rule (68 Fed. Reg. 18524), and the statute does not provide any reason believe that DHS must do so before Section 214(a) can become effective. We ask DHS to confirm this position in writing at its earliest opportunity, to eliminate any concerns that submitters may have before this proposed rule is finalized.

II. Submission to Other Federal Agencies

The Council supports DHS's position that, in addition to being submitted to DHS, CII may also be submitted "indirectly" to DHS via another federal agency (§ 29.2(i)).¹ We also support the proposals that agencies must forward CII to DHS for acknowledgement and validation (§ 29.5(c), second sentence), and that such agencies may not otherwise distribute or release the information until DHS instructs (§ 29.5(d)(2)). We suggest that these latter two provisions be included in some sort of direction from the Executive Office of the President (e.g., an Executive Order or Presidential memorandum) to confirm that all executive agencies will be expected to comply with them.

¹ All section symbol (§) references are to the proposed sections of 6 C.F.R.

III. Scope and Degree of Protection Afforded

Several aspects of the proposal reveal DHS's dedication to protecting CII broadly, all of which ACC strongly supports. These kinds of categorical assurances are crucial to enabling a free flow of information:

A. Fulllest Extent of the Law. Above all, the Council strongly supports DHS's statement that it will protect CII to the fullest extent permitted by law (§ 29.1(a)). Such a clear statement will go a long way to reducing uncertainty on the part of submitters.

B. Presumption of Protection. Similarly, the Council endorses DHS's presumption of protection unless and until the CII Program Manager finally determines that it is not (§ 29.6(b)).

C. Reliance on Submitter Discretion. ACC is pleased that DHS has not attempted to develop a definition of CII that is more detailed than the statute's definition, instead "rel[ying] on the discretion of the submitter as to whether the volunteered information meets the definition" 68 Fed. Reg. 18524. This approach recognizes the very diverse forms that CII can take across sectors.

D. Destruction of "Orphan" Information. ACC supports DHS's proposal to automatically destroy information that it has determined does not constitute CII if it has not heard back from the submitter within thirty days (§ 29.6(e)(1)(ii)).

E. Retention of Otherwise Applicable FOIA Exclusions. The Council agrees with DHS that a determination that information does not constitute CII does not thereby deprive it of any otherwise applicable exemptions from the Freedom of Information Act for which it may qualify (§29.3(b)).

IV. Points on Which the Council Has Concerns

A. Good Faith Determinations. The Council is very troubled by the provision authorizing the CII Program Manager to determine that information has not been submitted in good faith, and to do so without informing the submitter (§ 29.6(f)). We support the comments of the Coalition Supporting Confidentiality for Critical Infrastructure Information on this issue (and the other issues discussed there).

B. Effect of the CIIA and Regulations on State and Local Governments. The proposal states that protected CII will only be made available to federal government contractors and to foreign, state and local governments pursuant to express agreements (§ 29.8(b), (c) & (j)). The Council supports the ability of state and local governments to have access to CII, since these governments are the first line of defense for, and need to work closely with, CI facilities. We urge DHS to confirm, however that the Act's bar on use of CII in civil proceedings and its preemption of state and local open records laws

(CIIA Sections 214(a)(1)(C) & (E)) are automatic and not dependent upon agreement with the relevant jurisdiction.

C. Interaction of §§ 29.6(g) and 29.6(e)(ii). Proposed § 29.6(g) says only the CII Program Manager can remove the protected status that attaches to CII. The final rules should clarify that when this happens, the CII Program Manager then must contact the submitter pursuant to proposed § 29.6(e)(ii) to determine the submitter's preference.

V. Recommendations for Completing CIIA Implementation

A. DHS Should Announce Where Exactly the Critical Infrastructure Information Program (CIPP) Will Be Located. The proposed procedures state that the Secretary "shall" designate the Under Secretary for IAIP as the senior DHS official in charge of the CII Program (§ 29.4(a)), and that the Under Secretary "shall . . . [a]ppoint a CII Program Manager within the IAIP Directorate to direct and administer the CII Program" (§ 29.4(b)(1)). ACC urges DHS, as soon as possible and in the final rules at the latest, to actually designate the Under Secretary for IAIP as the senior DHS official in charge of the CII Program, and to actually appoint someone within that office to be the CII Program Manager. Knowing the offices and persons running the program will greatly others in interacting with DHS on this subject.

Relatedly, the final rules should correct an inconsistency between § 29.5(b)(1), which says that CII should be submitted "to the IAIP Directorate," and § 29.5(c), which speaks of submission "to the CII Program Manager."

B. DHS Should Announce Where the ISAC Functions of the NIPC Will Be Located. Last year, ACC and the FBI's National Infrastructure Protection Center (NIPC) established a Chemical Sector Information Sharing and Analysis Center, one of over a half-dozen such ISACs. ACC has invested substantial resources in this ISAC, and has worked hard to make the ISAC the single, or at least predominant, point of contact between its members and the federal government. Other ISAC sponsors have done similarly.

ACC has been concerned that it has not been able to find out where within the IAIP Directorate the NIPC will land, or for that matter whether the NIPC will remain our counterparty under the ISAC Standard Operating Procedures. We urge DHS to reach out to its ISAC counterparties, like ACC, to discuss (i) where the ISACs will be housed within DHS; (ii) what roles ISACs may play now that their counterparty is DHS; and (iii) how the CII Program and other component parts of DHS will coordinate in sharing and analyzing information with critical infrastructure sectors.

C. DHS Should Implement its Defense Production Act Authorities Relevant to Critical Infrastructure Protection. As noted earlier, a key obstacle to sharing and analyzing CII within industry has been concern that such discussions could subject the participants to unfounded -- but nonetheless very costly -- antitrust lawsuits. To remedy

that concern, Section 213 of the CIIA provides that the President or the Secretary of DHS may designate a component of DHS as a “critical infrastructure protection program” (CIPP), and Section 214(h) adds that the President may delegate to that program the authority to enter, along with an ISAC or other representatives of the private sector, into a voluntary agreement or plan of action, as those terms are defined under Section 708 of the Defense Production Act of 1950 (DPA). Section 708 in turn provides a defense from claims under the antitrust laws for actions by industry representatives taken in the course of developing or carrying out an agreement or plan, so long as its procedural requirements are met.²

ACC is eager to see these designation and delegation steps taken, so that we could begin discussions with the appropriate DHS staff about the nature and scope of a possible DPA voluntary agreement addressing protection of chemical sector critical infrastructure. It is unclear to us whether DHS’s proposed CIIA rules accomplish the designation task. Presumably, § 29.4(a) designates the IAIP Directorate as the CIPP, but DHS should remove any doubt.³ It is also unclear to us whether the President has delegated his powers under DPA Section 708 to the CIPP.⁴ Again, this issue should be resolved clearly.

ACC urges DHS to work with the President to address these issues as soon as possible. ACC does not believe that any changes to the DPA are necessary for its provisions to apply in the context of critical infrastructure, a position shared by all the Administration witnesses who testified on June 6 before the Senate Banking Committee.⁵ This position is also consistent with the President’s recent revisions to the procedures for classifying information, which provide that “‘national security’ means the national defense or foreign relations of the United States” and “includes defense against transnational terrorism.”⁶ Nonetheless, if the Administration believes any such changes are warranted, the Council urges it to include them in the reauthorization of the DPA this year, currently pending in both houses of Congress.

² 50 U.S.C. § 2158(j).

³ The preamble refers generically to the Act establishing a “critical infrastructure protection program,” *see* 68 Fed. Reg. 18524, and the only reference to this phrase in Section 214 of the CIIA is in Section 214(h). However, the balance of the proposal -- including § 29.4(a) -- speaks of a “critical infrastructure information program,” a phrase not found in the CIIA. Also, the preamble makes no reference to the DPA or to CIIA Section 214(h).

⁴ Section 24 of Executive Order 13286 puts the Secretary of Homeland Security in charge of administering the DPA. Section 501 of E.O. 12919 (which it amends) states that the President’s authority under DPA § 708 is delegated to the heads of all federal departments and agencies, but Section 902(c) of that same E.O. appears to say that this delegation cannot be redelegated to lower level officers.

⁵ BNA Homeland Security Briefing, “Senate Panel Explores Use of DPA for Homeland Security, Cybersecurity” (June 6, 2003).

⁶ E.O. 13292, preamble and §§ 1.1(a)(4) & 6.1(y).

D. DHS Should Begin Implementing the Homeland Security Information Sharing Act. Council members often express frustration at the inability (or perceived unwillingness) of federal officials to share detailed threat information. To address that problem, Title VIII, Subtitle I of the Homeland Security Act created the “Homeland Security Information Sharing Act” (HSISA), a free-standing law intended to promote the distribution of information that is classified or sensitive but unclassified. While the HSISA speaks of sharing such information with “State and local personnel,” that term is defined to include “employees of private sector entities that affect critical infrastructure, cyber, economic or public health security, as designated by the Federal government in procedures developed pursuant to [the HSISA].”⁷

Overall, the HSISA declares the sense of Congress that federal agencies should share, to the maximum extent practicable, information that:

- Relates to terrorist threats;
- Relates to the ability to prevent or disrupt terrorist activity;
- Would improve the identification or investigation of suspected terrorists; and
- Would improve response to terrorist attacks.⁸

Essentially, the HSISA instructs the President to develop homeland security information sharing systems to promote the sharing of both classified and sensitive but unclassified information. These systems are to have the capability to limit distribution to specific subgroups of people based on geographic location, type of organization, position of recipient within an organization, and need to know.⁹ They may also condition distribution on limitations on redistribution.¹⁰ The procedures can include issuing additional security clearances for classified information or entering into nondisclosure agreements for sensitive but unclassified information.¹¹ The law clarifies that information distributed through these procedures remains under the control of the federal government and may not be released under state open records laws.¹²

ACC believes that the HSISA provides a tremendous opportunity for critical infrastructure sectors like the chemical industry to work with the federal government to increase preparedness. The HSISA also is consistent with the President’s *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, which emphasizes the crucial need for “meaningful information sharing” between the federal government and the private sector owners and operators of critical infrastructure. (*Id.* at

⁷ 6 U.S.C. § 482(f)(3)(F).

⁸ *Id.* §§ 481(c), 482(f)(1). The bill specifically refers to the FBI’s Terrorist Threat Warning System, the National Law Enforcement Telecommunications System and the Regional Information Sharing System. *Id.* § 482(b)(4).

⁹ *Id.* § 482(b).

¹⁰ *Id.*

¹¹ *Id.* § 482(c).

¹² *Id.* § 482(e).

ix.) Yet ACC has not become aware of any steps on the part of the Administration to implement this statute.

ACC requests DHS to contact it and other critical infrastructure representatives to explain its intentions in this regard. In that connection, ACC proposes that DHS create a "Facility Security Officer" (FSO) program, in which the chief security officers of critical infrastructure companies would become "designated private sector employees" under HSISA and given enhanced access to classified or sensitive but unclassified information. An FSO program would promote a consistent level of competence, and consistent use of terminology, between government and industry and across industry sectors. It would also serve to establish a public/private network of professionals to promote benchmarking and coordination. Conceptually, this program would resemble the Industrial Security Management course run by the Defense Security Service's Defense Security Institute. However, instead of a one-week course like the ISM, the FSO program should consist of one week of generic training and another week of training in issues associated with particular industry sectors. The FSO program could be created by building on the existing training now available to private sector officials from the Security Specialties Division of the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. Ideally under this proposal, FSOs would be given secret clearances. As a second choice, they would be given special access to sensitive but unclassified information.

We look forward to discussing our FSO idea and other ways in which the HSISA can be implemented.

* * *

In conclusion, the Council once again commends DHS for this proposal and appreciates the opportunity to present these comments. To follow up on any of the issues discussed here, please contact the undersigned.

Sincerely,

James W. Conrad, Jr.
Counsel
703-741-5166
james_conrad@americanchemistry.com