May 20, 2004

Janice Pesyna
Office of the General Counsel
Department of Homeland Security
Washington, D.C. 20528

Re: Comments on Interim Procedures for Handling Critical Infrastructure Information, 69 Fed. Reg. 80774 (Feb. 20, 2004)

Dear Ms. Pesyna:

The American Chemistry Council (the Council or ACC) appreciates this opportunity to provide these comments on the Department of Homeland Security's (DHS's) interim 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,[1] a part of the nation's critical infrastructure, as recognized by *Homeland Security Presidential Directive (HSPD) - 7*, among other documents. Chemistry 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, and we filed significant comments on DHS' April 2003 proposed rules.

ACC is very pleased that DHS has issued these regulations to implement the CIIA. An effective system for sharing critical infrastructure information is crucial to the public/private partnership that this nation needs to protect that infrastructure. ACC has

[1] 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.

submitted information under the new rules several times already and we have found the submission process workable. Indeed, we have been very pleased with the promptness and responsiveness to questions we have received from Mr. Herr and his staff.

In the balance of these comments, we focus first on particular steps that DHS can and should take to complete the implementation process and make the most of its CIIA authority. We then list specific technical corrections that DHS should make. Finally, we reemphasize the need for DHS to clarify how it will implement the Homeland Security Information Sharing Act, particularly as it affects private critical infrastructure.

I. Major Comments

A. Need to expedite implementation. ACC urges DHS to proceed as quickly as possible to implement subsequent phases:

- *Allowing electronic submission*. It is ironic that ACC established the Chemical ISAC in 2002 to create a secure, encrypted means for submitting threat information to the federal government, and yet those communications are not now covered by the very statute that was enacted to promote these kinds of CII exchanges between business and government. As a result, the ISAC cannot perform the function it was principally meant to serve, and sensitive information must be routed through ACC staff.[2] DHS should move as quickly as possible to enable CII to be submitted electronically. As discussed in Part I.C below, DHS may also want to issue a "class determination" that such communications, when time-sensitive, are PCII.

- *Within DHS*. The interim rules require information to go to the PCII Program in order to be protected.[3] But other parts of DHS routinely ask for CII, particularly Protective Security Division staff, and often when they are in the field. It is cumbersome and slow for information to have to be sent to PCII Program, and then be forwarded to the relevant DHS office. It is better, but still clumsy, for information to have to be sent simultaneously to PCII Program and the requesting DHS office. It would be best if all or selected DHS offices and personnel were authorized to accept CII , which they then would forward to the PCII Program office for validation. Such a system would not require field or other offices to develop expertise or make judgments regarding eligibility; the PCII Program could retain exclusive authority to validate CII. The other offices would simply have to follow the safeguarding requirements of 6 C.F.R. § 29.7 and

[2] A cynic has commented that this situation is like the "Cone of Silence" in *Get Smart*, the ineffective communications protection device that forced users to bypass it by shouting in order to hear each other.

[3] *See* 6 C.F.R. § 29.5. DHS should clarify the intent of the first sentence of § 29.5(b) by adding at the end "until such time as it is provided to one of them." This change would confirm that CII does not *lose* its ability to become protected by being given first to somebody besides the PCII Program Manager or his designees, it just doesn't *gain* that protection until one of those entities receives it.

agree to forward the information promptly to the PCII Program. (Obviously, the presumption of protection provided by § 29.6(b) would need to apply in these cases as well.)

DHS could explore the prospect of issuing "class determinations" (discussed further below) that would allow DHS staff outside the PCII Program in effect to validate -- upon receipt -- certain classes or types of information. An example would be facility vulnerability assessments or security plans, which are categorically protected under the Coast Guard's Maritime Transportation Security Act (MTSA) rules.[4] ACC is uncertain, however, whether this process would be superior to one where the PCII Program validates the information – it still would have to be safeguarded upon receipt and forwarded quickly to the PCII Program.

- *Other federal agencies*. ACC is pleased that DHS intends to provide other federal agencies access to PCII, under written agreements, for purposes of protecting critical infrastructure. ACC urge DHS and those other agencies to quickly conclude those agreements so that PCII can be shared universally among all federal agencies that, under HSPD-7, have responsibilities for critical infrastructure protection.

- *State and local governments*. These entities were a prime intended beneficiary of the CIIA. ACC and its member companies would like to share more information with them, but have been concerned about their ability to protect it. We thus welcomed the CIIA's provisions regarding access by state and local governments.[5] We interpret those provisions as being self-implementing and effective now. We understand DHS's desire to enter into written agreements with states and local governments to confirm those provisions. Again, however, we urge DHS to move with dispatch. In particular, we recommend that, to the maximum extent permitted by state law, DHS enter into agreements with state governments that bind all the political subdivisions of that state, so that DHS does not unnecessarily have to negotiate additional agreements with those subdivisions.

B. Allow indirect submissions. DHS's proposed rule properly envisioned allowing persons to submit CII to DHS indirectly through other federal agencies. While the interim rule does not authorize this, ACC is pleased that DHS intends to do so ultimately, and that the final rule encourages comments on the issue.

ACC supports allowing indirect submissions, and believes that allowing them is a reasonable interpretation of the CIIA. The act does not explicitly (or, for that matter, implicitly) prohibit them. The statute only says that DHS must "receive" CII.[6] But it does not state (or suggest) that DHS must receive it directly from the submitter. At various places, it speaks of "submittal to" or "communication of" CII to "a covered

[4] *See* 33 C.F.R. § 105.400(c).
[5] 6 U.S.C. § 133(a)(1)(E).
[6] *Id*. § 131(4).

Federal agency," elsewhere defined as DHS, but this should not lead to a conclusion that CII may only go to DHS directly, for at least two reasons:

- First, the statute clearly allows DHS to receive CII indirectly from intermediaries *outside* the federal government -- namely, Information Sharing and Analysis Organizations.[7] It is certainly consistent with this authority for DHS to be able to receive CII indirectly from intermediaries *within* government as well.
- Second, the bill that became the CIIA (S. 1456) originally authorized the submission of critical infrastructure information to any of a long list of "covered federal agencies."[8] When the bill was folded into the House's version of the Homeland Security Act (H.R. 5005) during the Government Reform Committee's markup of that bill, the Committee deleted the list of agencies in favor of the new Department being created by that bill.[9] Having been close to this process, ACC understands that the legislators' rationale was to avoid having multiple agencies running separate CII programs, potentially developing different policies and interpretations, and thus increasing the risk that some CII might be released improperly or otherwise mismanaged. They were not concerned about other agencies simply receiving CII and passing it along to DHS for ultimate validation. The CIIA's legislative history thus supports allowing indirect submissions.

As the agency charged with implementing the statute, DHS clearly has discretion to interpret it as allowing indirect submissions, and courts are likely to defer to that reasonable interpretation. DHS had previously proposed that agencies must forward CII to DHS for acknowledgement and validation,[10] and that such agencies may not otherwise distribute or release the information until DHS instructs.[11] DHS should restore these proposed provisions. ACC also suggests that the 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.

C. Class determinations. Several federal agencies (e.g., EPA) have made advance determinations that any record falling within a certain class is either protected or exempt under FOIA.[12] DHS should explore a similar approach under the CIIA, so

---

[7] *Id*. § 131(7)(A).
[8] *See* S. 1456, § 5(a)(2) (the "Bennett/Kyl" bill, introduced Sept. 24, 2001, available at http://thomas.loc.gov). The closest house bill similarly authorized submission of CII to "any Federal agency." See H.R. 2435, § 4(a) (the "Davis/Moran" bill, introduced July 10, 2001).
[9] *See* H.R. 5005, § 722(2) (as reported July 12, 2002). This explains the odd syntax of 6 U.S.C. 131(2), "Covered Federal agency": "The term 'covered Federal agency' means the Department of Homeland Security."
[10] Proposed 6 C.F.R. § 29.5(c), second sentence.
[11] Proposed § 29.5(d)(2).
[12] *See, e.g*., EPA, *Freedom of Information Act Manual* 8-6 (1992), available at http://www.epa.gov/foia/docs/foiamanual.pdf.

that particular kinds or classes of information could be validated once, and, subsequently, anyone with information falling within that class could submit it to DHS (or its designees) which in turn could accept it without having to make a separate validation decision. An example would be time-sensitive information submitted by ISACs or Sector Coordinators to the Homeland Security Operations Center. ACC's concerns in this connection are shared by the U.S. Chamber of Commerce, whose comments recommend that the revised rules deem such communications to be protected. The class determination approach would accomplish the same goal.

D. Coverage of transmittal letters and the like. ACC requests DHS to clarify that CIIA applies not only to documents for which protection is requested, but also to transmittal or cover letters and any other documents that substantiate the original request. While the interim rules – quite properly -- do not require substantiations, cover letters and similar documents may well contain some substantiation beyond the express statement required by the rules. These substantiations may well contain CII themselves and need to be protected.

E. Relationship between CII and SSI. ACC had several concerns regarding the preamble's discussion of "sensitive security information." The SSI regulations are especially important to ACC, as they authorize the provision of SSI to trade associations representing covered persons and, on a need-to-know basis, to members of the private sector besides the submitter -- thus enabling some limited amount of information sharing between government and industry.[13]

TSA and DOT have just published a new interim final rule on SSI[14] that addresses some of our original concerns but also raises new ones. ACC will reserve a full discussion of its concerns to the comments that it will file on that new rule. Nonetheless, we believe it is important to flag at least one issue now: voluntary submissions. The preamble claims that SSI "ordinarily will not be voluntarily submitted,[15] a statement echoed in the new preamble to the interim rule.[16] In fact, ACC and others have voluntarily submitted a significant amount of maritime, rail and motor vehicle-related security information to DOT, its Research and Special Projects Administration (RSPA),[17] and the Coast Guard under those agencies' assurances that it would be protected as SSI. A prime example is the Responsible Care® Alternative Security Program Plan submitted to the Coast Guard by ACC and approved by it last December. It will be important for DHS to allow such

[13] *See* 49 C.F.R. §§ 1520.7(g) & (j), 1520.11(a)(1).
[14] 69 Fed. Reg. 28066 (May 18, 2004).
[15] *Id*. at 8076.
[16] *Id*. at 28069 ("information constituting SSI generally is not voluntarily submitted to the government"). It does go on to note that "[t]here may be cases, however, where the owner or operator of a critical transportation asset voluntarily submits information, such as a vulnerability assessment, to TSA or the Coast Guard." *Id.*
[17] RSPA administers the Hazardous Materials Transportation Act.

voluntary submissions -- when not accompanied by a request for protection under the CIIA -- to be managed under the SSI rules and the practical flexibility they offer.

II. Technical comments:

- § 29.3(d) (independently obtained information). The first and third sentences of this subsection logically belong together. The second is really a proviso applicable to both. DHS should put the first and third together and place the second before them.

- § 29.8(a) (authorization of access). DHS should insert, after "CII" in the first sentence, ", under one or more of the subsections below," to clarify that subsection (a) is not a separate or catch-all authorization for disclosure, but only an introductory statement . All (and the only) permissible bases for providing access to CII are enumerated in subsections (b) through (k).

- § 29.8(a)(2) (ditto). DHS should change "and" to "or" in this subparagraph. Information need only meet one of these four criteria to be protected from disclosure. This change is required to track the statutory language -- see 6 U.S.C. § 133(g)(2).

- § 29.8(e) (disclosure of information to appropriate entities or to the general public). Make same change in last sentence for same reason.

III. DHS Should Take Concrete Steps to Implement the Homeland Security Information Sharing Act.

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* emphasizes the importance of "partnering" between federal, state and local government, and the private organizations owning "the lion's share" of the nation's critical infrastructure.[18] It frankly acknowledges that "[f]orging this unprecedented level of cooperation will require dramatic changes in the institutional mindsets honed and shaped by Cold War-era regimes."[19] Nowhere is this more true than in the area of information affecting security, which since Cold War days has been classified or at least tightly held by the government.

To drive this fundamental change, Congress included within the Homeland Security Act the "Homeland Security Information Sharing Act" (HSISA), a free-standing law intended to promote the distribution to state and local governments of security- related information that is classified or sensitive but unclassified.[20] While the HSISA speaks of

---

[18] *National Strategy* (Feb. 2003) at 15-20.

[19] *Id*. at 3.

[20] 6 U.S.C. §§ 481-84. 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;

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]."[21]

ACC believes this law has tremendous promise as a mechanism for providing vitally needed threat and related information to representatives of critical infrastructures, and more generally for enabling these representatives to partner directly with federal, state and local entities in both the design and implementation of security initiatives. To date, however, such sharing has generally not been occurring.

In its comments on the proposed CIIA rules filed last June, ACC called upon DHS to implement its HSISA authority. Since then, the President has issued Executive Order 13311, which assigns most functions under the HSISA to the Secretary of DHS, including the ability to designate private sector entity employees as noted above.[22] Yet ACC has received no further concrete information regarding this important statute. ACC understands that DHS is fleshing out a concept of "sensitive homeland security information" (SHSI) that may be the new name for information distributed under this law. ACC also understands that DHS is developing a "Homeland Security Information Network" that will utilize the Joint Regional Information Exchange (JRIES) to share information with state and local personnel and the private sector. But ACC has no real confirmation of these understandings, and is unclear as to how and when these mechanisms will be established.

The GAO has repeatedly called on DHS to implement effective information sharing among states and local governments[23] and among critical infrastructures.[24] The Director of the federal Information Security Oversight Office has also emphasized the need for "a seamless and congruous system for protecting and sharing all types of information, both classified and unclassified," including information about potential threats to critical infrastructures.[25] He adds that the decentralized program he envisions "is about as significant a cultural change as there is possible."[26] As stated earlier, ACC believes that this change is needed, and that the HSISA provides a tremendous opportunity to

---

- Would improve the identification or investigation of suspected terrorists; and
- Would improve response to terrorist attacks.

Id. § 482(f)(1).

[21] *Id*. § 482(f)(3)(F).

[22] 68 Fed. Reg. 45149 (July 31, 2003). *See esp*. § 1(f).

[23] *E.g*., GAO, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened* (GAO-03-760, Aug. 2003) at 3, 13.

[24] *E.g*., GAO, *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors* (GAO-04-699T, April 21, 2002) at 32-34.

[25] Remarks of J. William Leonard, "Information Sharing and Protection: A Seamless Framework or Patchwork Quilt?" (June 12, 2003) at 1, 6, available at www.fas.org/sgp/isoo/ncms061203.html.

[26] *Id*. at 6.

accomplish these goals, to enable critical infrastructure sectors like the chemical industry to work with federal, state and local government to increase preparedness. We again urge DHS to let us know how its plans to implement the law. ACC will be in touch to pursue this important issue.

* * *

In conclusion, the Council once again commends DHS for issuing these interim rules 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.
Assistant General Counsel
703-741-5166
james_conrad@americanchemistry.com

cc: J. Caverly
T. Connelly
J. Mares