

Federal Bar Association.txt

Subject: CII Regulation Comments
Date: Mon, 16 Jun 2003 13:49:09 -0400
From: "Joseph Beach" <JBEACH@skadden.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Please accept the attached comments from the Federal Bar Association.

Thank you,

Joseph W. Beach
Skadden, Arps, Slate, Meagher & Flom LLP
1440 New York Avenue, NW
Washington, DC 20005-211
Telephone: +1-202-371-7879
Fax: +1-202-661-9079

This e-mail and any attachments thereto, is intended only for use by the addressee(s) named herein and may contain legally privileged and/or confidential information. If you are not the intended recipient of this e-mail, you are hereby notified any dissemination, distribution or copying of this email, and any attachments thereto, is strictly prohibited. If you receive this email in error please immediately notify me at (212) 735-3000 and permanently delete the original copy and any copy of any e-mail, and any printout thereof.

Further information about the firm, a list of the Partners and their professional qualifications will be provided upon request.

was2_437852_1.pdf	Name: was2_437852_1.pdf
	Type: Acrobat (application/pdf)
	Encoding: base64
	Description: was2_437852_1.pdf



Federal Bar Association

June 16, 2003

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

RE: Proposed Procedures for Handling Critical Infrastructure Information, 68 F.R.
18524 – 529 (Apr. 15, 2003)

Dear Sir or Madam:

On behalf of the Government Contracts Section (the "Section") of the Federal Bar Association ("FBA"), we respectfully submit comments on the above referenced Proposed Procedures for Handling Critical Infrastructure Information (hereafter the "Proposed Rule").¹ The Section consists of attorneys and associated professionals in government service, private practice, and industry. We seek to improve the relationship between the government, industry, and the public with respect to the procurement of goods and services by the federal government. If you have

1. Comment: Proposed Section 29.6(f) does not define "good faith" or offer sufficient opportunities to avoid misunderstandings.

Section 29.6(f) of the proposed rules states, "In the event the CII Program Manager determines that any information is not submitted in *good faith* accordance [sic] with the CII Act of 2002 and these procedures, the Program Manager is not required to notify the submitter that the information does not qualify as Protected CII. This is the only exception to the notice requirement of these procedures." (emphasis added). We believe that the Department may wish

¹ The Federal Bar Association ("FBA") is an association of attorneys who practice in various areas of law relating to the Federal Government. The Government Contracts Section, FBA, which consists of attorneys engaged in the practice of all aspects of government procurement, is authorized by the Constitution of the Federal Bar Association to submit public comments on pending legislation, regulations, and procedures relating to the procurement of goods and services by the federal government. These comments have been prepared by the Homeland Security Committee of the Government Contracts Section, with the direction and approval of Section leadership. The views expressed in these comments reflect the position of the Homeland Security Committee. They have not been considered or ratified by the FBA as a whole, or by any Federal agency or other organization with which Section members are associated through their employment or otherwise.

to consider adding further clarification to the term "good faith" and afford notice to the submitter of any adverse decision under this provision.

There are several troubling aspects of the current language of 29.6(f). First, neither the Act nor the proposed rules define the words "good faith." Without knowledge of this standard, the submitter will face great uncertainty in any situation that they might consider "good faith" to be an issue. Such uncertainty will likely lead them to choose to not submit the questionable information rather than take a risk. In this case, the current version of the rules will work to defeat the fundamental purpose of the Act. Refusing to set forth this standard can also lead to misunderstandings with submitters, who could believe that they are acting in good faith.

Second, the lack of notification back to the submitter does not seem consistent with the other provisions of the proposed rules. Section 29.6(e) requires the Program Manager to tell the submitter that the information does not qualify as protected CII. Section 29.6(e) also gives the entity submitting information the opportunity to "further explain the nature of the information and the submitter's basis for believing the information qualifies for protection under the CII Act of 2002." The current version of 29.6(f) makes DHS the sole and final arbiter of what is "good faith" and excludes the submitter from even the knowledge that their submission has been deemed unprotected.

We recommend that the notice and further explanation provisions of Section 29.6(e) should also be included in 29.6(f). If the submitter has made an honest mistake, it will only aid the Department's attempts to foster public/private cooperation by allowing the submitter to answer for its actions. The CII Program Manager should mark the information as presumed protected, and it can be put to use by the Department pending the final determination of its status. The CII Program Manager can easily remove the information's protection at a later date if he or she does not receive an adequate answer from the submitter. We believe that the interest of fostering an effective spirit of public/private cooperation on Homeland Security justifies taking extra steps here to minimize misunderstandings. Finally, we strongly urge the Department to develop guidance on the definition of "good faith" and include it in the rules. The Act is structured to encourage voluntary participation by the private sector. In order to make reasoned decisions, they will need a complete understanding of the standards by which their actions will be judged.

2. Comment: The proposed Rules should be amended to include the submitter in the decision process when determining whether to release protected information to foreign, state or local governments.

The proposed rules to the Critical Infrastructure Information Act ("CIIA" or "the Act") of 2002, allow the Department of Homeland Security ("the Department" or "DHS") to share protected critical infrastructure information with foreign governments. Section 29.8(j) states, "The CII Program Manager, or the Program Manager's designee, may provide Protected CII to a Foreign Government without the written consent of the person . . . " Procedures for Handling

Critical Infrastructure Information, 68 Fed. Reg. 18, 524 (proposed Apr. 15, 2003)(to be codified at 6 C.F.R. pt. 29). Further, the CIIA and the proposed rules allow DHS to share CII with state and local governments. Section 29.8(b) of the proposed rules states, "The CII Program Manager may provide Protected CII to an employee of the Federal Government or of a State or local government, provided that such information is shared for purposes of securing the critical infrastructure . . . "

We believe this potential information sharing regime does not possess sufficient safeguards in favor of the submitter. According to statements made by both DHS and the Department of Justice, the federal government will have no mechanism to ensure that these other entities observe the full legal protections granted to CII under the Act and these proposed rules. We view this shortcoming in the rules as a serious impediment to private sector cooperation, especially in the electric utility, telecommunications and banking and finance sectors.

6 U.S.C. § 133(f) criminalizes the unauthorized release of CII by "an officer or employee of the United States or of any department or agency thereof," but no provision in the Act or these rules addresses unauthorized disclosure by state and local employees. Section 29.8(d) of the proposed rules forbids state and local governments from disclosing shared information without obtaining the CII Program Manager's authorization or using the information for any other purpose (except for criminal investigations). The proposed rules do not, however, contain any sanctions against anyone who violates these standards. Without any explicit penalty or enforcement provisions, these rules do not provide the necessary assurance to private sector entities that their information will remain protected once it is handed over to state and local governments.

Likewise, these rules contain no assurances that foreign governments will maintain the confidentiality of CII. While it can be argued that cooperation with DHS is in their best interest to maintain a good relationship with the US and to continue to receive this important information, such a general concept does not provide the necessary assurance that CII will be protected in every instance. In *Xerox Corp. v. United States*, 12 Cl.Ct. 93 (1987), the United States demonstrated its willingness to go to great lengths to protect foreign information shared under confidence with the US government. Such examples, however, do not provide any assurance to US submitters that foreign governments will exhibit the same zeal.

While the root of some of these concerns may be founded in gaps in the Act, we believe the Department can alleviate our concerns through minor additions to the proposed rules. We understand that the Department will be called upon to make judgments about what information must be shared with other governments in order to best protect America from future terrorist threats. Rather than attempt to limit or forestall DHS's ability to share necessary CII, we request that the rules be amended to include consultation with the submitter in this process. We propose a new Section 29.8(l) to read as follows:

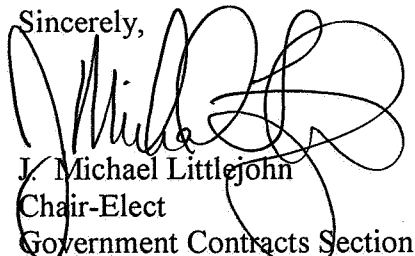
(l) *Consultation with submitter prior to disclosure of information to Foreign, State or Local governments.* The CII Program Manager, or the Program Manager's designee, will consult with the submitter prior to releasing any information that has been marked "Protected Critical Infrastructure Information" to a Foreign, State or Local government. The purpose of this consultation shall be to identify any potential harm that could come to the submitter should the receiving government engage in any unauthorized use of the information. The CII Program Manager, or the Program Manager's designee, shall give careful consideration to the submitter's request to withhold or redact non-essential parts of the information.

The purpose of this proposed change is to give to submitter a chance to inform DHS of any potential harm that could befall the submitter if the receiving government misuses that information. In many situations, it may be possible to disclose the information that DHS needs to disclose without threatening any harm to the submitter through the careful redaction of non-essential information.

Conclusion

We believe these comments will aid the Department address these two areas of serious concern. We appreciate this opportunity to discuss the Department's proposed rules. If you or anyone else at the Department has a question concerning these comments or if we can be of any further assistance to you, please do not hesitate to contact me at (703) 790-8750 or at mlittlejohn@wickwire.com.

Sincerely,



J. Michael Littlejohn
Chair-Elect
Government Contracts Section
Federal Bar Association