

Natural Resources Defense Council.txt

Subject: Comments on Proposed 6 CFR part 29
Date: Mon, 16 Jun 2003 16:35:02 -0400
From: "Devine, Jon" <jdevine@nrdc.org>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

To Whom It May Concern:

Attached (to be sent in hard copy as well) are comments of the Natural Resources Defense Council on the proposed regulations concerning the Department of Homeland Security's implementation of the Critical Infrastructure Information provisions of the Homeland Security Act of 2002.

Please feel free to contact me with any questions regarding these comments, or if there is any problem with this transmission. Thank you in advance for considering our views.

<<CII Comments NRDC.doc>>

Jon Devine
Senior Attorney
Natural Resources Defense Council
> 1200 New York Ave., NW, Suite 400
> Washington, DC 20005
> ph: 202-289-6868
> fax: 202-289-1060
>

PRIVILEGE AND CONFIDENTIALITY NOTICE

This message is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable law as attorney client and work-product confidential or otherwise confidential communications. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication or other use of a transmission received in error is strictly prohibited. If you have received this transmission in error, immediately notify sender at the telephone number above.

CII Comments NRDC.doc Name: CII Comments NRDC.doc
 Type: WINWORD File (application/msword)
 Encoding: base64
 Description: CII Comments NRDC.doc



June 16, 2003

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

<mailto:cii.regcomments@DHS.gov>

To Whom It May Concern:

On behalf of the Natural Resources Defense Council (NRDC), thank you for the opportunity to provide comment upon the notice of proposed rulemaking located at 68 Fed. Reg. 18,523 (Apr. 15, 2003). This proposal outlines procedures for handling critical infrastructure information (CII) that is voluntarily submitted to the government pursuant to section 214 of the Homeland Security Act (HSA) of 2002. Although NRDC remains troubled by the scope of the enacted provision, and although these comments outline a number of areas in which we believe the rule should be improved, elements of the proposed rule represent serious and well-intentioned efforts to address some of the problems that the bill created.

Attached is a section-by-section description of our concerns with the proposed rule, along with specific suggested improvements. If NRDC can provide additional information or clarify any of the enclosed comments, please do not hesitate to contact me at (202) 289-6868.

Sincerely,

Jon P. Devine, Jr.
Senior Attorney

SECTION-BY-SECTION ANALYSIS OF PROPOSED CRITICAL INFRASTRUCTURE INFORMATION REGULATIONS

1. *Section 29.2(b) -- Definition of "Critical Infrastructure Information"*

Plainly, this definition plays a central role in the operation of these regulations. Having maximum clarity about what kinds of records will qualify as CII thus is vital to the successful implementation of the rules. Unfortunately, two key elements of the definition are ambiguous, as neither "customarily" nor "public domain" have obvious meanings. We encourage DHS to clarify what these terms include.

First, the term "public domain" should be defined to include any method in which the document has been made available -- or could be made available -- to a member of the public. If a kind of document has been previously released by a state or federal entity, or by the submitter, it should be considered in the "public domain." Similarly, "customarily" should not be interpreted to require that a certain kind of record be made public with any specific frequency; instead, if it would be a company's or an agency's practice to release the information upon request, such release should be considered "customary."¹

2. *Section 29.2(i) -- Definition of "Submission to DHS"*

The proposed regulations permit a submitter to gain "protected CII" status for a record by submitting it through another agency to DHS. This option seems likely to engender confusion at recipient agencies, delay in determining whether a document legitimately qualifies as "protected CII," and unnecessary administrative burdens. The proposal reveals no reason for permitting this unorthodox method of submission, and we strongly urge the Department to abandon it.

We perceive multiple problems in implementing a provision that allows companies to submit CII through one agency to DHS. First, the regulations require conduit agencies to safeguard information they receive seeking CII protection, but do not provide a mechanism by which such agencies will be informed of the CII Program Manager's conclusion about whether the document is protected CII. Accordingly, an agency which maintains a copy of the record (which one would expect, since submitters hopefully will have some reason for sending the document to the non-DHS agency in the first place), but which does not learn of the CII Program Manager's decision, will treat the material as protected CII even if it should be released in response to a request.

Second, allowing a company to submit information through a conduit agency will result in a longer time passing between submission and DHS's evaluation of the company's claim of protected CII. A recipient agency, though obliged to send

¹ In addition, something should be considered "customarily" disclosed information if the type of material requested is customarily available, even if the identical information requested is not publicly available. See Center for Auto Safety v. NHSTA, 244 F.3d 144, 151-52 (D.C. Cir. 2001).

information claimed to be protected to DHS, see proposed 6 C.F.R. §§ 29.2(i); 29.5(b)(1), will necessarily take time to do so. Agency information administration is famously slow, so it may be a significant time before someone in the recipient agency realizes what is supposed to be done with the submission and then actually takes the steps to forward it to DHS. Because submitted information with a claim of protected CII must be treated as protected unless and until the DHS CII Program Manager rejects such a claim, see id. § 29.2(f), any delay in DHS's receipt of the information means a longer period of unquestioned protected status. Given this dynamic, the ability to submit information to DHS through another agency would seem to encourage companies to do so, if for no other reason than to gain additional time during which their assertion of protected status will be honored.

Third, allowing submitters to deliver information via a non-DHS agency to DHS adds administrative burden to a government information regime that is already taxed. Last year, a General Accounting Office (GAO) study of the implementation of the Freedom of Information Act (FOIA) concluded that "agency backlogs of pending requests are substantial, and growing, indicating that agencies are falling behind in processing requests." See GAO, Information Management: Update on Implementation of the 1996 Electronic Freedom of Information Act Amendments, at 12 (Aug. 2002). Requiring agencies to develop mechanisms to identify, handle, and forward information claimed as protected CII could divert resources and staff from processing already-delayed FOIA requests. Absent a compelling reason for creating these additional delays, we urge DHS not to move forward with the proposal to enlist other agencies in the processing of information claimed to be protected CII.

Finally, permitting submitters to channel their information to DHS through another agency is inconsistent with the expectation of those who enacted the HSA. Section 214(a)(1) of the HSA limited the scope of the Act's protection to CII "that is voluntarily submitted to a covered Federal agency for use by that agency," 6 U.S.C. § 133(a)(1), and the Act elsewhere defines "covered Federal agency" to mean DHS alone, not any other agency. Id. § 131(2). Indeed, a legislative attempt to add other agencies to the definition of "covered Federal agency" failed in the House of Representatives, despite supporters' protests that the bill's provisions "should not be artificially limited to the Department of Homeland Security exclusively when the President may want other existing Departments to be recipients of infrastructure vulnerability information." 148 Cong. Rec. H5,850 (daily ed. July 26, 2002) (text of amendment and statement of Rep. Cannon); see also id. at H5,869-70 (roll call vote).

3. Sections 29.2(j) and 29.3(a) -- "Voluntary" Submission of Materials Required by Other Agencies

The proposed regulations mirror an internal tension in the HSA by defining "voluntary" to include material that is mandated by a non-DHS agency, but then

denying CII protection to such materials. Proposed section 29.2(j) makes a submission "voluntary" if it is "submitted in the absence of DHS's exercise of authority to compel access to or submission of such information. . . ." However, quite a bit of information submitted to the government -- from tax returns to pollution reports -- is not provided to DHS or pursuant to DHS authority, but instead is submitted pursuant to some other agency's authority. Indeed, it is unclear to us what information collection authorities DHS has, if any. Consequently, we expect that a great deal of company information will qualify as "voluntarily" submitted under this definition.

By contrast, section 29.3(a) of the proposed rules states that "the CII Act of 2002 and these procedures do not apply to any information that is submitted to a Federal agency pursuant to any legal requirement." Likewise, that section says that "when information is required to be submitted to a Federal agency to satisfy a provision of law, it is not to be marked by the submitter, by DHS, or by any other party, as submitted or protected under the CII Act of 2002 or to be otherwise afforded the protections of the CII Act of 2002."

We recognize that these provisions are not literally incompatible; all "voluntary" information might not be afforded "protected CII" status. However, we believe that any confusion about the status of material submitted under compulsion to one agency but not under DHS compulsion could be alleviated simply by defining "voluntary" to exclude such a submission. Doing so is also needed because these provisions operate against a preexisting legal framework that gives protection -- quite apart from the CII requirements -- to "voluntarily" submitted information. Exemption 4 of FOIA has been interpreted to prohibit federal agencies from disclosing "voluntarily" submitted financial and commercial information in response to a FOIA request, see Critical Mass Energy Project v. Nuclear Regulatory Comm'n, 975 F.2d 871 (D.C. Cir. 1992), cert. denied, 507 U.S. 984 (1993), and the proposed regulations expressly preserve preexisting FOIA exemptions. See proposed § 29.3(b). Consequently, when one considers the interaction of these provisions and the existing law, companies which are required to submit commercial or financial information to a non-DHS agency may be able to submit the information to DHS, claim it as "voluntarily" submitted, and invoke the protections of Critical Mass, even while being ineligible for protection under these rules.²

² Indeed, this example raises a related issue -- whether Critical Mass-style submissions should be permitted at DHS at all. The CII provisions, for all of their flaws, at least introduce some procedural rigor in how submitters could claim the FOIA protection for information that is "voluntarily" submitted to DHS. If a company chooses to share information voluntarily with DHS, but neglects to make the "express statement" called for by the HSA and by section 29.5(b)(3) of the proposed regulations, we do not understand whether DHS intends to protect such information pursuant to Exemption 4 of FOIA, or whether it will be released because it is unprotected under the CII provisions.

4. *Section 29.2(j) – Definition of Term “Regulatory Proceedings”*

As it should, the proposed regulation prohibits material submitted during “regulatory proceedings” from being considered “voluntarily” submitted. It strikes us as common sense that a company that submits information to receive a regulatory benefit or avoid a penalty does so in a less than voluntary way. It is therefore important for the rules to define all of the circumstances that are encompassed by the term “regulatory proceedings.” DHS should not limit the term to formal agency actions – such as rulemakings and adjudications.

For instance, the rules should not exempt material required as part of a government contract bidding process from FOIA, and should declare such material unprotected under the CII provisions. Several judicial decisions recognize that such records are not “voluntarily” submitted. See McDonnell Douglas Corp. v. USAF, 215 F.Supp. 2d 200, 205 & n.3 (D.D.C. 2002) (collecting cases).

Likewise, information submitted by companies in an effort to deflect formal regulatory action should be publicly available. Take a hypothetical example. After DHS is given authority to promulgate regulations regarding terrorism vulnerabilities at chemical plants (as pending legislation would do), chemical companies decide it is in their interest to convince the Department to require very little of facilities that participate in a voluntary industry program. Industry representatives therefore meet several times with DHS officials and present information about their program, prior to DHS’s issuance of a notice of proposed rulemaking. Because the proposal could ultimately be influenced to a great degree by such information, it needs to be subject to public scrutiny; nevertheless, defining “regulatory proceedings” to exclude such pre-proposal meetings might allow the company to label their lobbying material as “protected CII.”

5. *Section 29.3(a) – Disclosure Under Non-FOIA Laws*

With regard to information required to be submitted to a Federal agency, the proposed rules rightly provide that the CII requirements do not affect agencies’ obligation to disclose the material under FOIA. The provision should be amended to say the same about disclosure pursuant to “any other laws.” Laws other than FOIA also mandate government information disclosure under certain circumstances, see, e.g., 42 U.S.C. § 7414(c) (Clean Air Act), and these rules should make clear that compliance with the CII provisions do not affect agencies’ independent duties to follow these disclosure obligations.

6. *Section 29.3(c) – Use of Protected CII*

There appears to be a drafting error in this section. The proposed rule states that “Federal agencies shall not utilize CII for regulatory purposes without the written consent of the submitter.” The term “protected” should be inserted in that

sentence prior to the term “CII.” Otherwise, the section could be interpreted to prohibit agencies from using any CII, whether or not it qualifies for protection under the HSA. Such a result is plainly not DHS’s intent, nor was it the intent of Congress.

We also suggest that the quoted sentence is too categorical insofar as it suggests that no regulatory use is permitted. There are several exceptions to the statutory prohibition on the use of this material (e.g., criminal investigations), as noted in section 29.8(f) of the proposal. To avoid confusion, section 29.3(c) should include a cross-reference to section 29.8(f).

7. *Section 29.5(b)(3)(ii) -- Information Communicated Verbally*

The regulations contain no real plan for handling “oral information.” This section requires that there be a written follow-up to a verbal communication of CII for which a submitter claims protection, but the rules otherwise do not explain how recipients of verbal information (especially ones who receive the information during the 15 days that can precede a company’s claim for protection) will be informed that they need to safeguard information they have been told. Given that draconian penalties apply to employees who mishandle protected CII, see proposed § 29.9(d), DHS employees should have a clear understanding of their legal obligations.

8. *Sections 29.6(c) and (d) – Marking and Tracking CII Received*

The proposed rules fail to ensure that recipients of material initially claimed as protected CII can later ascertain if its status has changed. As discussed above, conduit agencies (assuming DHS continues to allow such submission, despite our concerns) will have copies of records for which companies claim protection, but which have not yet been validated by the DHS CII Program Manager. Likewise, as discussed below, material initially validated as “protected CII” might lose its status depending upon later events, so there needs to be a mechanism for tracking the status of material marked “protected CII.” Specifically, if the CII Program Manager concludes that submitted records are not “protected CII,” whether during the initial validation determination or later, DHS should include this finding in the database contemplated by proposed section 29.6(d)(2).

The CII database also should be accessible by any federal employee who will have possession of records labeled “protected CII.” This is important both to allow employees to whom such records are disseminated to find out what the legal status of any given record is, and to enable them to better protect the public by letting them search the database for records related to their work.

9. *Section 29.6(e) – Validating Claims of Protected CII*

We perceive several problems with the Department’s plan to “validate” claims of protected CII.

First, although we support the idea that DHS will make an initial review of submitted CII to ensure that only eligible material is protected, doing so may be a significant effort, and we urge you to commit sufficient resources to the task. Adequately assessing the legal status of any given record will require the CII Program manager to know whether the same record is required to be submitted by another agency, has been submitted during a “regulatory proceeding,” and is otherwise “customarily in the public domain,” to name a few items.

Second, the procedures for validation do not make sense. The rules require an “initial validation determination” by the CII Program Manager, but do not require a final determination unless the initial determination is unfavorable to the submitter. Worse, during the initial determination, the Program Manager “shall give deference to the submitter’s expectation that the information qualifies for protection.” The term “deference” is highly ambiguous – how agreeable must the Program Manager be? Considering these problems, the first and last word on whether a record is protected from disclosure or use might be a cursory initial review in which DHS defers to an unspecified degree to the submitter. To address these concerns, DHS at least must remove the “deference” provision.

Third, the section needs to contain a provision that requires DHS to reevaluate the information’s status in response to a FOIA request that covers a record that has been marked “protected CII.” Records submitted today may not be responsive to a FOIA request for many years. By the time such a request is submitted, the record may have been demanded by another agency exercising independent authority, may have been submitted during a “regulatory proceeding,” or might have become customarily public. In other words, the CII provisions of the HSA may no longer apply to the information requested, and DHS will have no legal basis to withhold such records.

Fourth, we are concerned about sections (e)(i)(D) and (e)(ii), which give power to a submitter who requests protection for information that is determined to be non-protected to dictate what the government will do with the information. Upon a final determination that information is unprotected, the submitter gets to choose whether the records will be kept by DHS or “disposed of . . . in accordance with the Federal Records Act.” If such disposal occurs promptly in response to a submitter’s request,³ it would appear to create an incentive to make submissions

³ Given that the information is to be disposed of under the Federal Records Act, DHS will need to develop a schedule that provides for the retention and destruction of the documents. Therefore, the content of that schedule will explain specifically whether the records will be destroyed immediately upon request, or under some other circumstance. However, immediate destruction seems to us to be the intent of the proposed regulatory language (since it gives submitters the choice between retention without protection and disposal).

of vast volumes of extraneous information in the hopes of getting it declared protected. Companies seem to be able to submit the information to see if DHS treats it as protected (which, of course, DHS is likely to do, given the “deference” it owes to a submission) and, if DHS does not, simply request that the information be destroyed. Such an approach would be a risk-free way of gaining a suite of legal protections for company information, including heading off potential regulatory action based on the information. If this is indeed DHS’s intent, we think it is a seriously flawed policy, and if it is not, we urge DHS to clarify what it means.

Finally, the regulations should contain provisions that ensure a speedy and accurate review of the eligibility of submitted information for protection. In particular, the validation process (both the initial and final determinations) should include a step that requires the Program Manager to consult with any agencies that can assist in determining whether the submitted information is customarily public, required to be submitted under applicable law, related to homeland security, or otherwise meets the “protected CII” criteria. In addition, we urge DHS to include a required time in which the Program Manager will evaluate submitted information and determine its eligibility for protection.

10. Sections 29.6(f) and 29.8(i) – Definition of “Good Faith”

The regulations deny certain protections (notice of a determination of unprotected status and civil immunity) to companies who submit information without a “good faith” basis for seeking protection. Although we certainly agree that companies’ good faith will be essential to the proper functioning of these rules, we also believe that the regulations should spell out how a company can show its good faith. For instance, a submitter could be required to document that it diligently investigated whether the information met all of the prerequisites for being considered protected CII (e.g., it would explain the steps that it takes to make sure the material is not customarily made public). Having such a requirement would not only make these “good faith” provisions more enforceable; it would also make it more practicable for the CII Program Manager to substantively review company submissions.

11. Section 29.7(e) – Transmission of Protected CII

We read this section as prohibiting person-to-person transmission (e.g., giving the DHS employee in the adjacent office a copy of the document) of protected CII, and requiring instead that it be sent through the mail. We assume that is not DHS’s intent, and simply suggest that this provision be clarified.

12. Section 29.8(h) – “Ex Parte” Rules and Doctrine

One of the most opaque provisions of the HSA was the limitation in section 214 that protected CII would not be subject to “any agency rules or judicial doctrine regarding ex parte communications with a decision-making official.” Accordingly, we looked forward to these proposed rules giving some definition to the statutory

language. Unfortunately, the rules utterly fail to do so, and instead merely quote the language of the law. We urge DHS to explain to what situations this provision applies.

For instance, a simple legal database search turned up numerous circumstances in federal law where *ex parte* contacts are either discouraged or permitted, yet it is unclear from the proposed rules whether DHS believes that all, some, or none of them are negated with regard to protected CII. See, e.g., Fed. R. Bkrpcy. P. 9003 (generally barring *ex parte* contacts with the court); Fed. R. Crim. P. 6(e)(3)(F) (allowing government to petition *ex parte* to disclose grand jury proceedings); 12 C.F.R. § 263.9 (prohibiting *ex parte* communications with the Federal Reserve Board); 29 C.F.R. § 102.131 (same; National Labor Relations Board); 37 C.F.R. § 1.560 (concerning *ex parte* patent reexamination proceedings); 5 C.F.R. § 185.116 (Office of Personnel Management rules prohibiting *ex parte* contacts with administrative law judges); 7 C.F.R. § 1.173(c) (Department of Agriculture rules of practice prohibiting *ex parte* contacts by administrative judges during cease and desist proceedings under section 2 of the Capper-Volstead Act).

13. Section 29.8(i) -- Use of Protected CII In Civil Actions

The regulations essentially mirror the statutory language on the use of protected CII in civil lawsuits, but omit a key word. We hope that doing so was simply inadvertent, and that DHS will correct it in the final rules.

Section 214(a)(1)(C) of the HSA stated that protected CII “shall not, without the written consent of the person or entity submitting such information, be used directly . . . in any civil action arising under Federal or State law if such information is submitted in good faith.” The proposed regulations omit the word “directly” from this requirement, and effect a substantial change by doing so. As a Department of Justice witness testifying about this very topic stated:

If Congress chooses to include civil liability protections, the protections must be very carefully crafted so as not to hamper, or even eviscerate, law enforcement objectives. The bills already introduced include civil liability provisions. Some drafts of the liability provision have included so-called “indirect” use protections. We strongly believe that, at most, only “direct” use should be prohibited, since indirect or derivative use is extremely difficult to disprove. A similar issue frequently lurks in immunity proceedings in criminal cases, where the Federal government, in order to proceed with a criminal prosecution, may have to disprove derivative use of a defendant’s statements in a so-called Kastigar hearing. In the civil context, for example, should the government receive information about a vulnerability under an information-sharing bill that included indirect civil protection and then seek to sue the submitter, we would be required to prove that the submitted information was not used in any way in the

investigation, including developing leads. In essence, we have to prove that all of our evidence came from independent sources. Past experience clearly demonstrates that this is a very difficult burden to meet.

Testimony of John G. Malcolm, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, before the Senate Committee on Governmental Affairs (May 8, 2002). Clearly, then, the word “directly” should be inserted into this provision to give effect to Congress’s intent.