

Center for Progressive Regulation.txt

Subject: COMMENTS ON PROPOSED CII REGULATION, 68 FED. REG. 18524

Date: Mon, 16 Jun 2003 16:25:57 -0400

From: "Rena Steinzor" <rena.steinzor@verizon.net>

To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Attn: Frank Nolan

Please find attached, in word and RTF format, the comments of the Center for Progressive Regulation on the above-referenced regulations.

I would appreciate receiving an electronic mail acknowledgment of your receipt of these comments.

Thank you.

Rena Steinzor
Professor of Law
University of Maryland
School of Law
515 W. Lombard Street
Baltimore, MD 21221

(410) 706-0564 (phone)
(410) 706-2184 (telecopy)

rstein@law.umaryland.edu

cpr FINAL COMMENTS DHS REGS 061603.doc

Name: cpr FINAL COMMENTS
DHS REGS 061603.doc
Type: WINWORD File
(application/msword)
Encoding: base64
Description: cpr FINAL COMMENTS
DHS REGS 061603.doc

cpr FINAL COMMENTS DHS REGS 061603.rtf

Name: cpr FINAL COMMENTS
DHS REGS 061603.rtf
Type: WINWORD File
(application/msword)
Encoding: base64
Description: cpr FINAL COMMENTS
DHS REGS 061603.rtf



P.O. Box 76293
Washington, DC 20013-6293
www.progressiveregulation.org

June 16, 2003

FILED BY ELECTRONIC MAIL

mailto: cii.regcomments@DHS.gov

**Re: Department of Homeland Security Procedures for Handling
Critical Infrastructure Information;
Proposed Rule – published in 68 Fed. Reg. 18525**

Dear Sir/Madam:

These comments are submitted by the Center for Progressive Regulation (CPR), an organization of academics specializing in the legal, economic, and scientific issues that surround federal regulation. CPR's mission is to advance the public's understanding of the issues addressed by the country's regulatory laws. CPR is committed to developing and sharing knowledge and information, with the ultimate aim of preserving the fundamental value of the life and health of human beings and the natural environment. We seek to inform the public about scholarship that envisions government as an arena where members of society choose and preserve their collective values. CPR also seeks to provoke debate on how the government's authority and resources may best be used to preserve collective values and to hold accountable those who ignore or trivialize them. We reject the idea that government's only function is to increase the economic efficiency of private markets.

These comments concern the Department of Homeland Security's (DHS) Proposed Regulation to Implement the Critical Infrastructure Information Act (CIIA or Act) (Proposed Regulation).¹ Our basic message is simple: to avoid an administrative nightmare, at best, and, at worst, the fateful undermining of corporate accountability and open government, DHS needs to go back to the drawing board and revise the regulations implementing the CIIA to establish a workable "tag and track" system for covered documents.

¹ 68 Fed. Reg. 18524-29 (April 15, 2003).

Overview and Summary

The creation of DHS represents the most significant reorganization of the federal government in several decades. As the new Department struggles to its feet, it is plagued by a myriad of issues, as well as the worrisome possibility that the tragedies that inspired its creation could recur. DHS and the nation can ill afford the administrative and judicial nightmares that could be triggered by careless implementation of the CIIA. In sum, more is at stake in this rulemaking than abuse of the law by corporations with something to hide. As egregious as that outcome could prove, undermining the enforcement of the nation's environmental, civil rights, consumer protection, and even tax liability laws, it is overshadowed by the possibility that precious DHS resources will be wasted on efforts to administer the Act.

HYPOTHETICAL CASE STUDY

To illustrate these implications, consider the progress of a hypothetical document through the system contemplated by the Proposed Regulation:

A company that makes an acutely toxic chemical used to combat bioterrorism “voluntarily” submits a three-dimensional drawing of its manufacturing facility to EPA as part of a presentation by the American Chemistry Council on plant security. The diagram shows that the chemical is kept in an above-ground tank, under carefully controlled pressure and temperature. The diagram is stamped CII and accompanied by a request that it be forwarded to DHS. EPA complies with this request, keeping a copy for its own files. The diagram is reviewed by DHS and the CII claim is not disputed, although the reviewer makes no effort to determine whether it is “customarily in the public domain.” DHS does not communicate this determination to EPA because its regulation does not require that it track CII claims in any way, even where another agency has served as a conduit for submission.

Three years later, a company official requests an appointment with a senior EPA official, stating that the company seeks EPA endorsement of its product in order to increase its sales to local government “hazmat” teams. The company submits the same drawing as part of its sales package, this time not stamped CII.

The senior EPA official has a background in chemical engineering. As she reviews the drawing, she notices that the plant abuts a residential neighborhood and that there does not appear to be a redundant power source available onsite. She becomes quite alarmed because the quantity of the chemical stored at the site has a “kill zone” of two miles depending on prevailing winds. She visits the company's web site and discovers that the drawing is the centerpiece of its home page.

When the company representative appears for the appointment, he is greeted by a team of EPA experts requesting that the company immediately install the capacity to provide back-up electricity in order to prevent the tank from exploding in the event of a power failure. The company refuses. When EPA attempts to take action to force its hand, the company cites the CII status of the drawing, and all the “information” it contains – i.e., how the physical plant is configured.

With no mechanism for appealing the initial DHS determination that the diagram was CII, EPA officials spend months shuttling between the company and their counterparts at DHS attempting to get the document’s status changed. When EPA finally achieves a DHS decision withdrawing CII protection and prepares to bring an enforcement action, the company takes its case to court, claiming that DHS regulations do not provide for reconsideration of an initial CII decision on the basis of subsequent disclosure of the information in a public arena. It also notes that the diagram has been removed from its web site.

CORE RECOMMENDATIONS

To forestall scenarios like this one, DHS should modify the Proposed Regulation to provide that:

- 1. *CII status applies only during the time period when the information is “not customarily in the public domain.”***
- 2. *Information is “customarily” in the “public domain” when: (a) it has been disclosed to a random cross section of the public, with or without the submitter’s consent; (b) the submitter has not taken steps to protect its confidentiality; or (c) this type of information has been available to the public in the past.***
- 3. *Information that enters the public domain automatically loses its CII status, unless disclosure was accomplished by illegal means and all extant copies can be easily retrieved.***
- 4. *Information is “independently obtained” and therefore not subject to CII protection if the requester learned of its existence and sought access to it through a process or set of circumstances unrelated to DHS processing of a CII claim.***
- 5. *Federal, state, and local agencies and any third party can appeal an initial determination that information is CII to DHS at any time, and DHS will consider such appeals in a timely and attentive manner.***
- 6. *Companies requesting CII status should submit documents directly to DHS, and should not assert CII status in submissions to other agencies until DHS has upheld their claims.***
- 7. *Initial submissions of information claimed to be CII should be accompanied by a statement that the information is not “customarily in the public domain,” thereby triggering federal criminal penalties if such claims turn out to be false.***

8. *Documents determined to constitute CII should be assigned a tracking number that companies must use every time they assert that the information the document contains is entitled to CII status.*
9. *Tracking numbers should be kept in a national, publicly accessible, computerized database. In subsequent disputes over the status of a document and the information it contains, those tracking numbers shall be used by the submitter in responding to requests for access, allowing the third parties seeking the information to determine quickly how to approach DHS with requests that such claims be reconsidered.*
10. *Other federal agencies should not be required to serve as “conduits” for CII.*
11. *Companies that refuse to address their vulnerabilities when requested to do so by the government achieve a special status under the law that subjects all future CII claims to heightened scrutiny by DHS.*

The remainder of these comments explores the ambiguities inherent to the CIIA, forecasting best and worst case scenarios for how the Act could be interpreted by the private sector and the courts. We explain why implementation of the above recommendations is necessary to avoid the worst case scenario: the consumption of scarce resources by DHS and its constituencies in resolving intricate CII disputes.

Best and Worse Case Scenarios

The DHS authorizing statute is close to 200 pages long, and was cobbled together within a few months. It is not surprising, then, that the CII title got lost in the shuffle, and was barely mentioned as Congress debated the law. The title is not a model of clear and precise legislative language and its implications are very much in the eyes of the beholder.

During confirmation hearings for Governor Tom Ridge, appointed by President Bush to head the new Department, Senator Carl Levin engaged the nominee in a discussion of the CIIA, motivating the Governor to make the following pledge:

It certainly wasn't the intent, I'm sure, of those who advocated the Freedom of Information Act exemption to give wrongdoers protection or to protect illegal activity. And I'll certainly work with you to clarify that language.²

In response to follow up questions by the Committee, Governor Ridge promised to establish a “tag and track” system to ensure that CII claims sent to DHS would be labeled

² Senate Governmental Affairs Committee Hearing on the Nomination of Tom Ridge to Be Director of Homeland Security, 108th Cong. (Jan. 17, 2003) (statement of Tom Ridge), *available at* 2003 WL 133596; *see* 149 Cong. Rec. S1463-01 (daily ed. Jan. 23, 2003) (statement of Sen. Jeffords).

and processed correctly.³ Such a system is vital to ensure that false claims are not spread throughout government without any opportunity to question and refute them, thereby paralyzing routine functions. Unfortunately, the Proposed Regulation issued in April does not fulfill this commitment.

As DHS is obviously aware, the CIIA offers corporations the opportunity to win confidentiality and civil liability immunity with respect to “critical infrastructure information” that they submit “voluntarily” to the new Department. CII includes virtually any information about physical or cyber infrastructure that could prove useful to terrorists or others intent on causing damage to the facility. Unless they obtain the written consent of the company, *no one* may use CII in *any* civil action arising under federal or state law. These privileges and immunities provide a strong incentive for misuse of the statute’s protections by companies otherwise in trouble under the law. It is inevitable that some corporations, concerned not just about security but also about enforcement actions and other forms of civil liability, will work hard at the administrative level and in the courts to expand the scope and effect of this section.

For example, since “information” is covered, as opposed to specific “records” (the term used throughout the Freedom of Information Act), companies may assert that documents containing the same information are also covered, whether or not they submitted this particular paperwork to the government.⁴ This assertion will almost certainly spawn widespread litigation because the submission of a single piece of information could invalidate the use of the same information memorialized in countless other formats.

As another example, if information is available, but not widely available (e.g., it is not accessible through the worldwide Web), companies may argue that it is not “customarily” in the public domain. Further, information may have been made publicly available without a company’s consent, offering submitters the opportunity to argue that the owner of the information did not, as a matter of its own “custom,” disclose the material.

The CIIA contains an all-important savings clause designed to preserve the ability of all three levels of government and third parties to gain access to “independently obtained information” under “applicable law.” In an exercise of ambiguous drafting of the type that exasperates federal judges, such authority is preserved only to the extent that those entities seek to obtain the information “in a manner not covered by” the CIIA’s core provisions. This language could be read to allow access and use so long as the requester discovers the availability of the information through independent means. Or it

³ See Pre-hearing Questionnaire for the Nomination of Tom Ridge, Nominee for Secretary, Department of Homeland Security at 37-38 (answer to question 67 posed by the Committee).

⁴ FOIA defines “record” as “any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format.” 5 U.S.C. § 552(f)(2).

could be read to mean that once information is labeled CII, no one can obtain it again in any format.

A narrow reading of the statutory language would interpret the CIIA as consistent with *Critical Mass Energy Project v. Nuclear Regulatory Commission*,⁵ where the D.C. Circuit Court of Appeals held that voluntarily submitted information is only exempt from the Freedom of Information Act if the government could *not* obtain it through other legal means. On the other hand, an expansive reading would transform the CIIA into a radical reversal of common law tort liability and open government requirements. Under this scenario, the CIIA would immunize corporations and their employees from malfeasance in routine activities, from discrimination on the basis of race in the workplace, to embezzlement, to violations of environmental laws, to negligence that harms the general public financially or physically. Not incidentally, these interpretations would also immunize corporations that proved negligent in the face of terrorist threats, allowing them to avoid accountability for endangering their fellow citizens.

Commendably, the Proposed Regulation tries to discourage expansive claims by stating 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

See 68 Fed. Reg. 18526, 6 C.F.R. §29.3(a).

Without a mechanism to enforce this crucial injunction, however, it is likely to remain hortatory, honored only when DHS officials have the resources to intervene in escalating disputes regarding the legitimacy of CII claims.

Establishing a “Tag and Track” System

As Governor Ridge recognized in his response to the Senate Committee on Governmental Affairs, all of these shortcomings could be alleviated if the Proposed Regulation adopted a “tag and track” system allowing effective oversight of the continued legitimacy of CII claims. *A tag and track system has three essential components:*

1. *a procedure for continuously revisiting the CII status of information at the request of a governmental or private party seeking to obtain or use it;*

⁵ 975 F.2d 871 (D.C. Cir. 1992).

2. *a public, web-based system for tracking the status of CII by a non-descriptive number so that requesters can verify where the information stands in the review process; and*
3. *penalties for submitters who abuse the system.*

Continuous Opportunities for Review

Amazingly enough, DHS makes a commitment in the proposed rule to review *every* piece of information labeled CII when it is first submitted, whether or not anyone inside or outside of government has expressed either a need or a desire to use the information. Yet the system established by the Proposed Regulation does not appear to contemplate that DHS will ever revisit that initial determination, even though it provides that “[o]nly the CII Program Manager or the Program Manager’s designee may change the status of Protected CII to non-Protected CII and remove its Protected CII markings.”⁶

A crucial test of the validity of a CII claim is whether the information is “customarily in the public domain.”⁷ Since the status of information in this regard can change over time, it is especially important that DHS provide for a revisiting of its initial determination. To omit this crucial component of a workable rule is to ensure that a morass of litigation will be necessary to resolve these questions. The proposal would set up an unworkable, and arguably illegal, system conferring permanent CII status on pieces of information that do not meet the statutory definitions. These unacceptable results would occur unless DHS, in its sole discretion, decides to go outside established procedures and revisit its initial determination.

RECOMMENDATION: The Final Rule must establish a procedure for reviewing the validity of CII claims in response to efforts to obtain it by any government official or third party.

Opportunity to Be Heard

If the DHS “CII Program Manager” determines that the information is *not* CII, the submitter will be notified and given an opportunity to lobby for a reversal of this adverse decision.⁸ The Proposed Regulations instruct such officials to “give deference to the submitter’s expectation that the information qualifies for protection.”⁹ This provision virtually invites submitters to play fast and loose with the review process, stretching the law to the edge of its conceivable boundaries and causing unmanageable abuse of the system.

⁶ See 68 Fed. Reg. 18527, 6 C.F.R. §29.6(g).

⁷ See 68 Fed. Reg. 18325, 6 C.F.R. §29.2(b) (defining CII in conformance with the Homeland Security Act).

⁸ See 68 Fed. Reg. 18527, 6 C.F.R. §29.6(e).

⁹ *Id.*

Compounding this problem, the Proposed Regulation does not include any requirement that federal agencies serving as conduits for the information – and therefore presumably affected by the assertion that the information is CII – also be informed of this process and given an opportunity to participate in DHS reconsideration of a rejected claim. As indicated above, CPR would solve this problem by eliminating the provision that requires agencies to serve as conduits.

RECOMMENDATION: The Final Regulation must omit any provision giving deference to a submitter's CII claims. Instead, the Final Regulation should require that submitters sign a statement attesting to the validity of their CII claims under the law. Subsequent requesters should be given an opportunity to submit evidence challenging the validity of CII claims at appropriate points in the process.

Resource Commitment

We must await the next budget cycle to determine the resources DHS will commit to this potentially onerous and overwhelming task. However, in the absence of sufficient resources, it is likely that if companies take full advantage of the law's broad definitions, the flood of submissions will force DHS to convert this upfront process into a superficial, cursory review. Resource constraints will also make it very difficult to revisit initial decisions.

RECOMMENDATION: To avoid this unfortunate perversion of the process in its early years of application, DHS must commit significant resources to initial reviews that will forestall such abuses.

Barring Conduit Submissions

The implications of DHS's failure to establish a workable review procedure are compounded by its misguided and arguably illegal decision to encourage companies to use other agencies as conduits for CII, rather than requiring that all such information be submitted directly to DHS.¹⁰ Not only must agencies and departments act as conduits, they must establish procedures for protecting CII when it is given to them, presumably in response to the submitter's claim that it is CII, as opposed to any independent verification they might wish to conduct.¹¹ This obligation is a one-way street, however. The Proposed Regulation does not commit DHS to communicate back to the conduit agency when a CII claim is denied. Presumably then, improperly labeled CII could remain in the conduit agency's files indefinitely, chilling its use for enforcement and other purposes.

The CII provisions enacted as part of the Homeland Security Act limit the opportunity to submit CII, and the authority to protect CII, to the "covered federal

¹⁰ See 68 Fed. Reg. 18525, 6 C.F.R. §29.2(i).

¹¹ See 68 Fed. Reg. 18527, 6 C.F.R. §29(7).

agency,” a phrase defined by the statute as DHS.¹² Advocates of the legislation made an unsuccessful attempt to extend this opportunity and authority to all federal agencies and departments, but the amendment was soundly defeated on the House floor.¹³ For DHS to decide to use federal agencies and departments as conduits for CII violates the clear intent of the law.

DHS may be tempted to defend this provision by arguing that it does not give agencies and departments authority to “acknowledge and validate the receipt of Protected CII.”¹⁴ Rather, other agencies are merely instructed to forward CII to DHS when explicitly directed to do so by the submitter. Or, in other words, acting as a conduit for information does not violate the intent of the law because it does not confer authority to accept and protect CII, which was the purpose of the amendment rejected on the House floor.

Nevertheless, the provision allowing other agencies and departments to receive and forward CII compounds the problems with the confused and ineffective process that the Proposed Regulation establishes for reviewing such information. With protected information seeping into files government-wide, it is very difficult to imagine how DHS will keep up with its review, much less track its dispersal. In the free-for-all that follows, the lodging of CII claims will inevitably inhibit the daily operations of government, especially because there are criminal penalties for disclosing it improperly, but there are no penalties for making blatantly unsupported CII claims.¹⁵

Indeed, the conduit provision could chill use of a wide range of information for any purpose other than the protection of CII by DHS. This effort flouts the clear intent of the Act, which explicitly preserves the normal use of information that is customarily in the public domain. While the Proposed Regulation acknowledges these provisions, it sets up circumstances that, as a practical matter, are very likely to result in their routine violation.¹⁶

RECOMMENDATION: The proposed rule should eliminate provisions allowing other agencies and departments to act as conduits for CII.

Certification by Submitter

To qualify for confidential treatment, CII must be submitted to DHS “voluntarily,” a term the Act defines to mean “submittal thereof in the absence of such

¹² See Section 214(a), Title II, Subtitle B, of the Homeland Security Act of 2002, P.L. 107-296.

¹³ Congressional Record, H5850-53, H5869-70 (July 26, 2002).

¹⁴ See 68 Fed. Reg. 18526, 6 C.F.R. §29.5(a).

¹⁵ See 68 Fed. Reg. 18529, 6 C.F.R. §29.9(d).

¹⁶ See 68 Fed. Reg. 18525, 6 C.F.R. §29.2(b) (acknowledging that CII does not include information customarily in public domain), 6 C.F.R. §29(j) (defining which types of information cannot be deemed CII).

[covered] agency's exercise of legal authority to compel access to or submission of such information."¹⁷ Following this provision to the letter, the Proposed Regulation states that to qualify for protection, the CII must be submitted "*in the absence of DHS's exercise of legal authority to compel access to or submission of such information.*"¹⁸

This approach reflects a considerably more conservative, even crabbed, interpretation of the law than the liberal, arguably illegal interpretation that permits agencies and departments throughout the government to act as conduits for CII. When combined with the conduit provision, the definition of voluntary in the Proposed Regulation means that agencies and departments receiving CII claims cannot dissolve such claims simply by exercising their own authority to obtain the information independently. Rather, they must forward the claims to DHS, which may or may not have authority to obtain the information independently, and may or may not review the legality of the claims.

As the hypothetical presented at the outset of these comments indicates, if companies engage in widespread gaming of this distorted system, labeling as CII the information they formerly provided to agencies and departments to demonstrate compliance with applicable regulatory requirements, regulators will be hard-pressed to loosen the restrictions on this data unless and until DHS assists them. This daunting hurdle will place the entire burden of refuting CII claims on the question whether the information was customarily in the public domain.

Once again, to its credit, DHS has included a provision instructing companies *not to claim* CII treatment for information that "*is required to be submitted to a Federal agency to satisfy a provision of law.*"¹⁹ This provision correctly reflects the legislative intent not to cover information that was already available to the government. Unfortunately, however, since there is no enforcement mechanism available to agencies and departments or requesters wishing to invoke this prohibition, and the process for asserting CII claims through those same agencies and departments is so open and confusing, the prohibition may well prove meaningless as a practical matter.

RECOMMENDATION: DHS must rewrite its Proposed Regulation to state that information formerly provided to other agencies and departments throughout government is "customarily in the public domain" unless it is covered by other, existing Freedom of Information Act exemptions (e.g., protection of confidential business information). The Final Regulation should provide that submitters mislabeling information in violation of the rule's requirements will lose CII status for that information and will have all future claims scrutinized more carefully.

¹⁷ See Section 212(7), Title II, Subtitle B, of the Homeland Security Act of 2002, P.L. 107-296.

¹⁸ See 68 Fed. Reg. 18526-7, 6 C.F.R. §29(j) (emphasis added).

¹⁹ See 68 Fed. Reg. 18526, 6 C.F.R. §29.3(a).

For more information, please contact Rena Steinzor at (410) 706-0564,
rstein@law.umaryland.edu.

Respectfully Submitted,

Rena Steinzor,
Board Member and Member Scholar,
Center for Progressive Regulation