Center For Progressive Regulation
PO Box 218
Riderwood, MD 21139-0218
www.progressiveregulation.org

**May 20, 2004**

**FILED BY ELECTRONIC MAIL**
mail to: cii.regcomments@DHS.gov

**Re: Department of Homeland Security Procedures for Handling Critical Infrastructure Information; Interim Rule – published in 69 Fed. Reg. 8074**

Dear Sir/Madam:

The Center for Progressive Regulation submits the following comments concerning the Department of Homeland Security's (DHS) Interim Rule to Implement the Critical Infrastructure Information Act (CIIA or Act) (Interim Rule).[1] The Center for Progressive Regulation (CPR) is 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.

## OVERVIEW AND SUMMARY

Abuse of the law by corporations with something to hide is not all that is at stake in this rulemaking: DHS and the nation can ill afford the administrative and judicial fiascos that could be triggered by careless implementation of the CIIA. Two changes that DHS incorporated into the Interim Rule are particularly important steps in ensuring against realization of such fiascos; namely, the elimination of the requirements that other federal agencies act as conduits for CII[2] and that the CII Program Manager "give deference to the submitter's expectation that the information qualifies for protection" in

[1] 69 Fed. Reg. 8074-89 (Feb. 20, 2004) (to be codified at 6 C.F.R. pt. 29).
[2] Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 18523, 18526, 6 C.F.R. § 29.5(b)(1) (proposed Apr. 15, 2003).

determining whether the information is entitled to protection.[3] However, these positive revisions are effectively neutralized by other changes elsewhere in the Interim Rule.

One of the principal drawbacks of the conduit requirement was that it could have resulted in information receiving CIIA protections even though it was legally required to be submitted to the federal government, thereby significantly impeding the ability of federal agencies to carry out their mandates. In our previous comments on the Proposed Regulation, CPR applauded DHS's effort to make clear that information that must be submitted to the federal government by law is not entitled to CIIA protections. Changes incorporated into the Interim Rule, however, appear to allow for the possibility of such information being accorded protected CII status. Similarly, although the Program Manager is no longer instructed to give deference to the submitter's belief that the information is entitled to protected-CII status, the Interim Rule now dictates that all submissions "shall be regarded as submitted with the presumption of good faith on the part of the submitter."[4]

These changes in the Interim Rule, along with DHS's failure to incorporate the other modifications urged by CPR in our previous comments (i.e., other than the elimination of the conduit and deference requirements), make the destructive and burdensome implementation of the CIIA even more probable, increasing the risk that the CIIA system will be abused and that, ironically, the nation will be less secure.

Our core recommendations fall into two main categories: the definition of protected CII and the process of determining whether information is entitled to protection—both at the time of submission to DHS and thereafter.

## DEFINITION OF PROTECTED CII

In establishing rules that implement the CIIA, it is imperative to bear in mind the sweeping nature of this legislation and the concomitant potential for manipulation. The Act 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 Act'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 press for an overly-broad definition of protected CII.

[3] *Id.* at 18527, 6 C.F.R. § 29.6(e)(1).
[4] 69 Fed. Reg. at 8085, 6 C.F.R. § 29.5(d).

Congress placed three principal limitations on the type of information that is entitled to protection under the Act: (1) the information must be "voluntarily submitted,"[5] (2) the information cannot be "customarily in the public domain,"[6] and (3) even if (1) and (2) are satisfied, CII is not protected if it is "independently obtained" by anyone through lawful means.[7]

## The 'Independently Obtained' Limitation

This limitation is embodied in the CIIA's all-important savings clause, which is 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. By itself, this language could be accorded the narrow interpretation that access and use are allowed so long as the requester discovers the availability of the information through independent means, or the much more expansive interpretation that access to the information in any format is prohibited once information is labeled CII. Reading the "independently obtained" provision in conjunction with the CIIA's definition of "voluntary," however, makes clear that the narrow reading is the better one.[8] Congress specifically provided that a party cannot "voluntarily" submit (and thus cannot receive CII protection for) "information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings."[9]

Further support for the narrow interpretation is provided by the House Select Committee on Homeland Security's explication of "voluntary" in its report accompanying the bill containing the provisions ultimately enacted as the CIIA: "The Select Committee intends that (the CIIA) only protects private, security-related information that is voluntarily shared with the government in order to assist in increasing homeland security. *This subtitle does not protect information required under any health, safety, or environmental law*."[10] Congress's desire to clarify that it did not intend to extend CIIA protection to such required information makes sense in light of the potential disastrous consequences of expansive interpretations; namely, immunization of 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

---

[5] Homeland Security Act of 2002, Pub. L. No. 107-296, § 212(7) (hereinafter "HSA").
[6] *Id.* § 212(3).
[7] *Id.* § 214(c).
[8] This narrow reading is also consistent with the 1992 decision in *Critical Mass Energy Project v. Nuclear Regulatory Comm'n*, 975 F.2d 871, in which the D.C. Circuit Court of Appeals held that voluntarily submitted information is exempt from the Freedom of Information Act only if the government could *not* obtain it through other legal means.
[9] HSA, *supra* note 5, § 212(7)(B)(ii).
[10] H. Rep. No. 107-609, at 116 (emphasis added).

negligent in the face of terrorist threats, allowing them to avoid accountability for endangering their fellow citizens.

Emphasizing that the broad reading would effect a radical reversal of common law tort liability and open government requirements in our comments on the Proposed Regulation, we applauded DHS's effort to discourage expansive claims by providing in section 29.3 that:

> Information submitted to any other Federal agency pursuant to a Federal legal requirement is not to be marked as submitted or protected under the CII Act of 2002 or be otherwise afforded the protection of the CII Act of 2002.[11]

However, the Interim Rule achieves the opposite effect, suggesting an expansive interpretation of "independently obtained" by adding to the end of this statement in section 29.3 the following qualification:

> provided, however, that such information, if it is separately submitted to DHS pursuant to these procedures, may upon submission to DHS be marked as Protected CII or otherwise afforded the protections of the CII Act of 2002.[12]

This caveat appears to allow a company to attain protected-CII status for information that the company is legally required to submit to another federal agency simply by also "voluntarily" submitting the information to DHS (presumably before, after, or simultaneous with the submission to the other federal agency). Given the "independently obtained" savings clause of the CIIA, particularly when read in light of the statutory definition of "voluntary" discussed above, there is a strong argument that according such information protection is illegal. DHS had apparently reached a similar conclusion: the Proposed Regulation not only included the statement quoted above, without the unwarranted "provided that" qualifier, it also stated clearly, in the same section, 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."[13] As this second statement contradicts the new "provided that" language, it is not surprising that this provision was deleted from the Interim Rule. Other changes indicate that DHS has adopted this arguably illegal interpretation of the definition of protected CII in the Interim Rule.[14]

---

[11] 68 Fed. Reg. at 18526, 6 C.F.R. § 29.3(a).
[12] 69 Fed. Reg. at 8084, 6 C.F.R. § 29.3(a).
[13] 68 Fed. Reg. at 18526, 6 C.F.R. § 29.3(a).
[14] In particular, the Interim Rule requires the submitter to include with the information a statement certifying, *inter alia*, that "[t]he information is or is not required to be submitted to a Federal agency," and "[i]f the information is required to be submitted to a Federal agency," to "identify the Federal agency . . . and the legal authority that mandates submission." 69 Fed. Reg. at 8085, 6 C.F.R. § 29.5(a)(4)(iii). This requirement apparently contemplates the possibility that a submitter could attain CII protection for

In its preamble to the Interim Rule, DHS notes that the rule "do[es] not apply to or affect any obligation of any Federal agency to disclose mandatorily submitted information (even where it is identical to information voluntarily submitted pursuant to the CII Act of 2002)."[15] While this language is heartening, its legal effect is arguably undermined by the language of the Interim Rule provision it purportedly describes, section 29.5(a)(4), which only requires submitters to include statements in the submission that the information is not being submitted in lieu of other federal requirements and that the information "is not" required to be submitted to a Federal agency.[16] In sum, while we are not entirely sure whether DHS intends the outcome we posit—that information, once submitted to DHS will forevermore be protected, whether or not it is required to be submitted to another agency—we think the point is far too important to remain ambiguous. To avoid draining litigation to resolve these ambiguities, DHS must make a clear statement regarding how it will view and process information in these circumstances.

***RECOMMENDATIONS:***

- ***The Final Rule should clearly provide that information is "independently obtained" and therefore not within the definition of protected CII if the information is required to be submitted to another federal agency to satisfy a provision of law and omit all provisions suggesting otherwise.***
- ***The Final Rule must provide that 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.***

## The 'Not Customarily in the Public Domain' Limitation

Unlike the "independently obtained" limitation of the CIIA, which excludes certain CII from protection, the "not customarily in the public domain" limitation is part of the definition of CII. Although the Interim Rule provides that CII "means information not customarily in the public domain,"[17] the Rule neither defines "customarily in the public domain" nor makes sufficient provision for the possibility that information not customarily in the public domain at the time of its initial submission could subsequently enter the public domain and thus no longer meet the statutory definition of CII. Consequently, there is a risk that determinations whether information is customarily in the public domain will be arbitrary and that non-CII will be protected, both of which provide opportunities for exploitation of the CIIA system.

---

information legally required by another agency, as there would be no point in making the submission to DHS otherwise.

[15] 69 Fed. Reg. at 8076.

[16] *Id.* at 8085, 6 C.F.R. § 29.5(a)(4).

[17] *Id.* at 8083, 6 C.F.R. § 29.2.

***RECOMMENDATIONS:***

- ***The Final Rule should define information as being "customarily" in the "public domain" when: (a) it has been disclosed to members 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.***
- ***The Final Rule should state that 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.***
- ***DHS must rewrite its Interim Rule 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 Rule 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.***

## PROCESS FOR DETERMINING WHETHER CII IS ENTITLED TO PROTECTION

### Unreasonable Deference to Submitters

As noted above, we welcome DHS's well-considered decision to delete the provision requiring the CII Program manager to "give deference to the submitter's expectation that the information qualifies for protection."[18] As we explained in our earlier comments, which we incorporate herein by reference, this provision virtually invited 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. DHS recognized this concern, noting that a number of comments expressed a fear that the deference provision "provide[d] too much discretion to the submitter."[19] Unfortunately, the new provision in the Interim Rule presuming good faith on the part of the submitter has essentially the same effect on the CII Program Manager's decision-making process as the deference provision. In fact, this presumption would appear to provide the submitter with even greater leeway than deference.

Compounding the problem of undue power accorded to the submitter by the good-faith presumption is the complete absence in the Interim Rule of any provision allowing requesters of information to challenge the claim that the information is protected CII, even though procedures are established for submitters to appeal the determination that information is *not* entitled to protection.[20] In fact, the only clearly-established trigger for DHS to revisit its initial determination that information *is* protected is the provision permitting the submitter to "request[] in writing that [protected] information no longer be

[18] 68 Fed. Reg. at 18527, 6 C.F.R. § 29.6(e)(1).
[19] 69 Fed. Reg. at 8080.
[20] *See id.* at 8086, 6 C.F.R. § 29.6(e)(2).

protected."[21] Otherwise, the Interim Rule states merely that protected "[s]tatus changes may take place . . . when the Protected CII Program Manager or the Protected CII Program Manager's designee determines that the information was customarily in the public domain, is publicly available through legal means, or is required to be submitted to DHS by Federal law or regulation."[22] Without more specific procedures that trigger review of protected status, however, this recognition that the status of information can change over time is of little practical import. Because it lacks such procedures, the Interim Rule establishes 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.

In order to provide governmental entities and third parties with a meaningful opportunity to challenge the protected status of information, a "tag-and-track" system allowing effective oversight of the continued legitimacy of CII claims must be established. Such a 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;***
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.***

More specifically, 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. These 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, the submitter should be required to use the tracking numbers in responding to requests for access, so the third parties seeking the information could quickly determine how to approach DHS with requests that such claims be reconsidered.

***RECOMMENDATIONS:***

- ***The Final Rule must omit the presumption of good faith on the part of the submitter.***
- ***The Final Rule should provide that federal, state, and local agencies and any third party may appeal an initial determination that information is CII to DHS at any time, and that DHS must consider such appeals in a timely and attentive manner.***
- ***The Final Rule must establish a procedure for reviewing the validity of CII claims in response to efforts to obtain such information by any government official or***

[21] *Id.* at 8086, 6 C.F.R. § 29.6(f).
[22] *Id.*

***third party. Subsequent requesters should be given an opportunity to submit evidence challenging the validity of CII claims at appropriate points in the process.***

- ***The Final Rule must establish a "tag and track" system with the three essential components enumerated above.***
- ***The Final Rule should provide that if a company refuses to address its vulnerabilities when requested to do so by the government, DHS will review any of that company's future CII claims with heightened scrutiny.***

## Implementation Resources 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

Because DHS indicated its intention to include in the final rule provisions allowing submitters to use other agencies as conduits for CII,[23] we reiterate our objections to such a system as misguided and arguably illegal. 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 agency," a phrase defined by the statute as DHS.[24] 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.[25] 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."[26] 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

---

[23] *See id.* at 8075.
[24] *See* HSA, *supra* note 5, § 214(a).
[25] Congressional Record, H5850-53, H5869-70 (July 26, 2002).
[26] 68 Fed. Reg. at 18526, 6 C.F.R. § 29.5(a).

floor. Nevertheless, with protected information seeping into files government-wide, it is 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.[27] Indeed, a conduit provision could chill use of a wide range of information for any purpose other than the protection of CII by DHS. This result flouts the clear intent of the Act, which explicitly preserves the normal use of information that is customarily in the public domain.

***RECOMMENDATION:***

***The Final Rule should not permit other agencies and departments to act as conduits for CII.***

For more information, please contact Rena Steinzor at 410-706-0564, rstein@law.umaryland.edu or Karen Sokol at 713-528-0901, kcsokol@yahoo.com.

Respectfully Submitted,

Rena Steinzor, Board Member and Member Scholar,
Karen Sokol, Senior Policy Analyst
Center for Progressive Regulation

[27] See 69 Fed. Reg. 8089, 6 C.F.R. §29.9(d).