

**From:** "David Sobel" <sobel@epic.org>  
**To:** "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>  
**Sent:** Monday, June 16, 2003 5:07 PM  
**Attach:** epic-cii-comments.pdf  
**Subject:** Comments on Proposed CII Rule

Attached please find (in PDF) EPIC's comments on the Department's proposed rule.

Thank you.

- David Sobel

--

.....  
David L. Sobel, General Counsel \* +1 202 483 1140 x.105  
Electronic Privacy Information Center \* +1 202 483 1248 (fax)  
1718 Connecticut Ave., N.W. Suite 200 \* sobel@epic.org  
Washington, DC 20009 USA \* <http://www.epic.org>

**Before the Department of Homeland Security  
Washington, D.C. 20528**

**In the Matter of  
Procedures for Handling Critical Infrastructure Information;  
Proposed Rule RIN 1601-AA14**

**Comments of the Electronic Privacy Information Center**

**June 16, 2003**

Pursuant to the notice published by the Department of Homeland Security ("DHS") regarding a proposed rule establishing procedures for the receipt, care and storage of information about critical infrastructure vulnerabilities,<sup>1</sup> the Electronic Privacy Information Center ("EPIC") submits the following comments.

EPIC is a non-profit research center in Washington, D.C. that examines the privacy and civil liberties implications of computer networks, the Internet and other communications media. We appreciate the opportunity to contribute to the proposed rulemaking for the implementation of Section 214 of the Homeland Security Act of 2002.<sup>2</sup> That section, among other things, prohibits the public disclosure of information relating to the security of the nation's critical infrastructure -- such as electric power grids, communication networks, financial systems, chemical plants, and water sources -- that companies or individuals have voluntarily submitted to the Department of Homeland Security. EPIC has a particular interest in this rulemaking, as we frequently make use of the Freedom of Information Act ("FOIA") to obtain information from the government on a range of policy issues, including computer security, consumer privacy, and encryption controls. The public disclosure of this information improves government oversight and accountability. It also allows for an informed public debate about government activities.

Given these important functions of public records law, the statutory exemption to FOIA for voluntarily submitted critical infrastructure information should be construed narrowly. As Homeland Security Secretary Ridge has testified, this exemption is "limited" in nature, designed

---

<sup>1</sup> Procedures for Handling Critical Infrastructure Information; Proposed Rule, 68 Fed. Reg. 18524 (proposed Apr. 15, 2003) (to be codified at 6 C.F.R. at 29).

<sup>2</sup> Pub. L. No. 107-296, 116 Stat. 2135 (2002).

to apply only to information that would not otherwise be shared with the government.<sup>3</sup> As currently conceived, the proposed rule would expand the exemption beyond the limited scope authorized by Congress. The statute covers only information that is submitted to the Department of Homeland Security. The proposed rule, however, would allow companies to submit critical infrastructure information to any federal agency, which then would be obligated to presume that it is protected from public disclosure and to forward it to DHS.

This proposed expansion is contrary to clear Congressional intent, as evidenced by the fact that the House of Representatives voted down a proposed amendment to the statute that would have allowed *any* federal agency to receive critical infrastructure information submissions, not just DHS. It also would negatively impact the ability of a government agency to obtain and use critical infrastructure information that already is in the public domain or that may be obtained through the agency's authority under other laws, an effect that is prohibited under section 214 (c) of the statute. Under the proposed rule, if an agency receives information from a regulated entity that is marked as protected critical infrastructure information, then the agency must forward the material to DHS and it may not distribute or make public the information until DHS reviews the validity of the submission, regardless of whether the agency may have independent authority to obtain the information. This limitation on agencies' regulatory authority is inconsistent with the explicit mandate of the statute.

For these reasons, which are further elaborated below, DHS must amend its proposed rule and should incorporate the following recommendations.

- **The proposed rule must be amended to eliminate the provisions allowing critical infrastructure information to be submitted to federal agencies other than the Department of Homeland Security.**

Section 214 of the Homeland Security Act, which is referenced as the Critical Infrastructure Information Act of 2002, provides that any information about critical infrastructure vulnerabilities that is voluntarily submitted to a covered federal agency for use in helping preventing attacks on those systems shall be exempt from public disclosure under the Freedom of

---

<sup>3</sup> *Homeland Security Department Hearing Before the Senate Judiciary Comm.*, 107th Cong. (June 26, 2002) (statement of Tom Ridge, Director of Homeland Security); *see also*, *Prehearing Questionnaire for the Nomination of Tom Ridge for the Secretary of the Department of Homeland Security Before the Senate Government Affairs Comm.*, 108th Cong. (answer to question 68).

Information Act.<sup>4</sup> It also establishes that government agencies or third parties may not directly use the critical infrastructure information ("CII") in any civil action arising under federal or state law.<sup>5</sup> The statute defines a "covered federal agency" as the Department of Homeland Security.<sup>6</sup>

The proposed rule would broaden the scope of the statute to include information that is submitted to any agency in the federal government. Specifically, it defines "submission to DHS" expansively to include "any transmittal of CII from any entity to DHS. The CII may be provided to DHS either directly or indirectly via another Federal agency, which, upon receipt will forward it to DHS."<sup>7</sup> This definition directly contravenes Congressional intent. Prior to passage of the Act, Representative Tom Davis introduced an amendment that would have defined the statutory term "covered federal agency" to include not only DHS but also any agency designated by DHS or any agency with which DHS shares critical infrastructure information. As Representative Davis remarked on the House floor, this amendment, if passed, would have "allowed other departments and agencies involved in fighting the war on terrorism to also receive this voluntarily provided information."<sup>8</sup> The amendment was debated and ultimately rejected by a vote of 233-195.<sup>9</sup> Congress chose not to authorize agencies other than DHS to accept and protect CII, and DHS may not establish that authority for federal agencies without Congressional authorization.

While the proposed rules would not allow these federal agencies to "acknowledge and validate the receipt" of protected critical infrastructure information,<sup>10</sup> this limiting provision does not save the proposed rule from falling outside the scope of Congressional authorization. Section 29.6 (b) of the proposed rule establishes that any information submitted in accordance with established procedures "will be presumed to be treated as Protected CII from the time the

---

<sup>4</sup> § 214(a)(1)(a).

<sup>5</sup> § 214(a)(1)(c).

<sup>6</sup> § 212(2).

<sup>7</sup> § 29.2 (i), 68 Fed. Reg. at 18525.

<sup>8</sup> 148 Cong. Rec. H5828 (2002) (statement of Rep. Davis).

<sup>9</sup> 148 Cong. Rec. H5850-5853 & H5869-H5870 (2002).

<sup>10</sup> § 29.6(a), 68 Fed. Reg. at 18527.

information is received by a Federal agency or a DHS component."<sup>11</sup> This presumption of protection will have the effect of making all federal agencies not mere conduits for information submitted to DHS, but rather *de facto* authorities that may accept and protect CII. As a result, federal agencies would function exactly as they would have if the Davis amendment had been accepted.

The proposed rule, therefore, exceeds its statutory authority, and DHS must amend it to reflect Congressional intent. In particular, DHS must eliminate the provisions that allow CII to be provided to DHS indirectly through other federal agencies.

- **The regulations should include procedures that allow federal agencies to demonstrate that the critical infrastructure information submitted to DHS already is within the public domain or is otherwise obtainable by the agency under other legal grounds.**

The purpose of the Critical Infrastructure Information Act is to create an incentive for private sector companies to provide information to the Department of Homeland Security about critical infrastructure vulnerabilities that they otherwise would not have shared due to concerns that the information might be released to the public under the Freedom of Information Act.<sup>12</sup> DHS, in turn, may use that information to analyze and help eliminate the security risks of these systems. The statute clarifies that the FOIA exemption of the Act applies only to voluntarily submitted information, and not to information that is customarily in the public domain or that companies already must submit to the government. The statute is unambiguous on this point; section 214 (c) reads:

Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered in subsection (a), including any information lawfully and properly disclosed to the public and to use such information in any manner permitted by law.

The proposed rule does not follow this statutory mandate because it will have the effect of limiting the ability of agencies to receive and use critical infrastructure information that they obtain independently.

---

<sup>11</sup>68 Fed. Reg. at 18527.

<sup>12</sup> See *supra*. n. 3.

Under the proposed rule, regulatory agencies would have no opportunity to participate in the DHS Program Manager's process of evaluating whether the submitted information qualifies for protection under the statute. Agency participation in this decision making is critical to ensure that information that already must be submitted to the government will not be categorized erroneously as protected CII. A CII submission to DHS may not receive protection from public disclosure if any other federal agency may use that information during licensing or permitting determinations or other regulatory proceedings, or if the agency may obtain the information through the exercise of its authority under any other statute, regulation, or legal rule. DHS staff simply will not have the expertise necessary to accurately make this determination for submissions from industries subject to wide variety of government regulations. Accordingly, the proposed rules for this validation process should detail procedures for the DHS Program Manager to consult with relevant regulatory agencies when initially evaluating the validity of a CII submissions. Similarly, these agencies should have the ability to participate in the continued review of information classified as protected CII. For example, when a FOIA request involves responsive documents that have been classified as protected CII, agencies should be consulted on whether this information is now in the public domain or may be obtained through other legal means.

Without these agency consulting procedures in place, DHS possibly may classify a submission as protected CII despite the fact that the information already must be provided to the government or has been made publicly available. As a result, an agency's ability to use independently obtained critical infrastructure information will be limited, an effect prohibited by the statute.

- **DHS must modify several of the proposed provisions that limit the ability of government agencies and third parties to use critical infrastructure information that is obtained independently.**

As examined above, the Critical Infrastructure Information Act prohibits DHS from construing the statute to limit the ability of government entities and third parties to obtain and use critical infrastructure information that already has been properly disclosed to the public or has been obtained through other lawful means. Several of the proposed rule's provisions, however, limit this ability, and they must be revised.

*Section 29.3(a) Freedom of Information Act access and mandatory submissions of information:* This section clarifies that the CII Act and corresponding regulations do not apply to mandatory submissions of information to the government. In addition, it prohibits companies submitting mandatory information to the government from claiming that it should enjoy CII protected status. This provision, however, fails to instruct companies that they also may not claim protected status for critical infrastructure information that is customarily in the public domain. This prohibition should be noted here or under a separate heading in the regulations.

*Section 29.3(d) Independently obtained information:* Similarly, this section fails to state that the CII protection procedures do not limit the ability of government entities and third parties to use CII that already has been released to the public. The section should follow the language of section 214 (c) of the statute which indicates that independently obtained information includes "information lawfully and properly disclosed generally or broadly to the public."

*Section 29.3(c) Restriction on use of protected CII by regulatory and other federal agencies:* This provision prohibits federal agencies from utilizing "CII for regulatory purposes without the written consent of the submitter." Under the statute, agencies are not prohibited from using *all* critical infrastructure information, they are only prohibited from using CII that is not customarily in the public domain or otherwise lawfully obtainable and that has been voluntarily submitted to DHS. The proposed regulations define this as "protected critical infrastructure information" or "protected CII."<sup>13</sup> Accordingly, the word "CII" in this section should be amended to "Protected CII."

*Section 29.6 (b) Presumption of Protection:* Under this proposed provision, all information submitted to the government claimed to be critical infrastructure information automatically will enjoy protection under the statute until the DHS Program Manager decides that it does not meet the standards of the statute. The presumption of protection applies even if an agency can easily demonstrate that the information could be obtained through independent means. The rule fails to establish a clear timeline for the Program Manager to review the legitimacy of the claim, and as a result, agencies may be prohibited indefinitely from using information that should never have been treated as protected. This is a clear limitation on agencies' authority to obtain and use CII through other lawful means, and this provision should be eliminated. Alternatively, the rule should specify procedures by which an agency may apply

---

<sup>13</sup> § 29.2 (f), 68 Fed. Reg. at 18525.

for expedited review for submitted information that it has reason to believe does not meet the qualifications for protection.

Without amendments to these provisions, the proposed rule contradicts the express terms of the statute and should not be promulgated.

- **DHS should amend the regulations to shift the burden to companies to demonstrate that the submitted information qualifies for protection from public disclosure.**

The proposed rules indicate that the Department of Homeland Security will only provide a cursory review of a company's claims that submitted critical infrastructure information qualifies for protected status under the Act. Section 29.6 (3) indicates that in evaluating the legitimacy of submissions, the "Program Manager shall give deference to the submitter's expectation that the information qualifies for protection."<sup>14</sup> Given the breadth of the protections afforded to validated CII under the Act, DHS should not simply rely on the discretion of the submitter when evaluating whether the information meets the statutory definition of critical infrastructure information.

Under the Act, validated CII may not be released to the public and may not be directly used by any party in a civil action arising under federal or state law. This grant of civil immunity, coupled with the proposed validation procedures that amount to DHS rubber-stamping CII submissions, may encourage abuses of the program. A company may submit documents about its critical infrastructure systems in an attempt to shield itself from legal liabilities. During his confirmation hearing, Secretary Ridge pledged that he would work to ensure that the FOIA exemption would not lead to such abuses. He said, "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."<sup>15</sup> As a first step in honoring that pledge, DHS should modify the proposed rule to provide for a more searching evaluation of a submission's validity.

---

<sup>14</sup> 68 Fed. Reg. at 18527.

<sup>15</sup> *Nomination of Tom Ridge for the Secretary of the Department of Homeland Security Hearing Before the Senate Government Affairs Comm.*, 108th Cong. (Jan. 17, 2003) (statement of Tom Ridge, Director of Homeland Security).



### **Conclusion**

For the foregoing reasons, EPIC submits that the Department of Homeland Security must amend its proposed rules to reflect the express terms of the statute and Congressional intent. The proposed rule implementing the FOIA exemption for CII exceeds its statutory authority. It is also contrary to the public interest, as it will adversely impact both the public's right to oversee important government activities and government agencies' abilities to perform their traditional regulatory functions.

Respectfully Submitted,

**David L. Sobel**  
General Counsel

Electronic Privacy Information Center  
1718 Connecticut Ave. NW, Suite 200  
Washington, D.C. 20009  
(202) 483-1140

**Kerry Smith**  
Law Clerk