

American Library Association.txt

Subject: Comments on "Procedures for Handling Critical InfrastructureInformation"
Date: Mon, 16 Jun 2003 16:23:45 -0400
From: "Camille Bowman" <cbowman@alawash.org>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

To whom it may concern:

Attached are comments (in both Microsoft work and "pdf" formats) submitted by the American Library Association in response to the Notice of proposed rulemaking on "Procedures for Handling Critical Infrastructure Information," 6 CFR Part 29, RIN 1601-AA14.

Please contact me if there are any problems receiving this email and attachments.

Camille Bowman

DHS_CII comments.doc Name: DHS_CII comments.doc
 Type: WINWORD File (application/msword)
 Encoding: base64
 Description: DHS_CII comments.doc

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

**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 American Library Association

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, the American Library Association submits the following comments.¹

The American Library Association (ALA) is the oldest and largest library association in the world with some 64,000 members, primarily school, public, academic and some special librarians, but also trustees, publishers, and friends of libraries. The Association's mission is to provide leadership for the development, promotion and improvement of library and information services and the profession of librarianship in order to enhance learning and ensure access to information for all.

Right to know laws, of which FOIA is one, provide information to individuals about the risks involved in their choices and allow them to decide whether or not to encounter these risks. They also promote democratic decision-making and the power of ordinary citizens by equipping them with the information they seek to participate in the decision-making process on a more equal footing.

The American Library Association (ALA) is, first and foremost, opposed to the overly-broad scope of the restriction on access to information held by the government and the resultant constriction of the public's ability to hold government accountable created by Section 214 of the Homeland Security Act of 2002 and implemented in this proposed rule. As Homeland Security Secretary Tom Ridge has testified, this exemption is "limited" in nature, designed to apply only to information that would not otherwise be shared with the government.²

We are also deeply concerned that, given the problems identified below, critical infrastructure information, if so designated by any corporate entity, receives "Protected" status unless—and, more importantly, until—it is deemed not protected. This will likely put much information in a

¹ 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).

² *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).

black hole of unaccountability for extensive periods of time. This is not, in our view, the way to protect and secure the health and safety of the American people and to ensure the accountability of government.

FOIA Requests

An exemption from disclosure requirements under FOIA is one of the primary protections for Protected CII created by the Homeland Security Act. It is, however, to be expected that requests will be received to which Protected CII may be responsive, as well as for Protected CII itself. As this was such a critical component of the legislation, ALA would have expected that the proposed rule would establish procedures for management of a request under FOIA for which Protected CII may be responsive or for Protected CII. It does not, except to say (at Section 29.8 (g)) that it shall be treated as exempt.

- **ALA urges that clear guidelines be established, within the Department's normal FOIA process, for handling of Protected CII requested under FOIA and Protected CII that may be responsive to a FOIA request.**

The lack of procedures for handling a FOIA request to which Protected CII is responsive or for Protected CII itself also highlights the lack of procedures for ongoing evaluation and review of the continued eligibility of the submitted CII for protected status.

- **ALA recommends that, at a minimum, a FOIA request to which Protected CII is responsive or for Protected CII should trigger a re-review of the CII by the FOIA officer to confirm that the information continues to meet the requirements for the CII program.** A process needs to be created for submitting an evaluation of the information to DHS, for its further review and either the continued application of the protected CII status or initiation of procedures to remove the protected CII status.

Moreover, there may be pieces of a submission that do not qualify as protected CII.

- **ALA recommends that the proposed rule also establish procedures for the partial release of submitted information. Such procedures would be in keeping with standard practice for exemptions under FOIA.**

While in many portions of this proposed rule DHS has only echoed the statute, there are a number of critical instances in which it either expands on what the statute says or tries to win in regulation a battle that proponents of this statute lost in legislation.

An instance of an expansion of the language of the statute is in an area of central importance to ALA: restrictions on the use of protected critical infrastructure information (Section 29.3(b)).

The statute says, at Section 214 (a)(1)(C), that such information

shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third

party, in any civil action arising under Federal or State law if such information is submitted in good faith;

(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this subtitle...

The statute says nothing about use for regulatory purposes without the written consent of the submitter. Yet the proposed rule makes this express statement at Section 29.3 (c). It is notable that this statement appears in Section 29.3 “Effect of Provisions” rather than Section 29.8 “Disclosure of Information” where the provisions of Section 214 (a)(1) are implemented. Moreover, in the portion of 29.3(c) where this prohibition is stated, the proposed rule fails to say that *Protected* CII may not be used in this manner, saying only that CII may not. This may, as noted below, be merely an editorial omission, but we think it is notable.

SCOPE

Protected Critical Infrastructure Information

ALA applauds the Department’s acknowledgment that not all Critical Infrastructure Information is Protected.. While the first part of the definition at Section 29.2 (f) echoes the legislation, it goes on to lay out the requirements that information must meet, in addition to being CII, in order to receive the program’s protections

...when accompanied by an express statement as described in Sec. 29.5 of this chapter.

This information maintains its protected status unless the CII Program Manager renders a final decision that the information is not Protected CII.

This distinction is inconsistently applied in the proposed rule, however. One example of this is in Section 29.3 (c). This appears to be an editing problem, but we would urge that the term “Protected CII” be used whenever referring to information managed by the program.

Extension to All Federal Agencies

The Homeland Security Act, in Section 214, extends “protection” to “critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily *submitted to a covered Federal agency for use by that agency* regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement...”

From the outset of the legislative debate, the question of which federal agencies would be covered by the CII provisions was intensely argued, and an amendment that would have allowed *all* federal agencies to accept CII was defeated. 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."¹ The amendment was debated and ultimately rejected by a vote of 233-195.² 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. Section 211 of H.R. 5005 is clear: "The term 'covered Federal agency' means the Department of Homeland Security."

The proposed rule acknowledges this sole authority in Section 29.5 "Authority to receive Critical Infrastructure Information." This section states that

(a) The Secretary of Homeland Security shall designate the DHS IAIP [Information Analysis Infrastructure Protection] Directorate as the sole entity authority authorized to acknowledge and validate the receipt of Protected CII

The proposed rule also, however, suggests the CII program would apply to *any* agency that handles such information:

29.1 (b) Scope. These procedures apply to all Federal agencies that *receive*, care for, or store CII voluntarily submitted to the Federal Government pursuant to the CII Act of 2002.

In case there was any question as to whether "receive" meant that a company could *submit* CII to an agency other than DHS, Sections 29.2 (i) and 29.5 (b)(1) remove the ambiguity:

Sections 29.2 (i) Submission to DHS as referenced in these procedures means 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 of the CII, will forward it to DHS.

Section 29.5 (b)(1) CII shall receive the protections of section 214 of the CII Act of 2002 only when

(1) Such information is voluntarily submitted either directly to the IAIP Directorate or indirectly to the DHS IAIP Directorate by submitting it to any Federal agency which then, pursuant to the submitter's express direction, forwards the information to the DHS IAIP Directorate.

The indirect provision of CII to DHS is clearly intended to allow all agencies to receive CII. This is equally clearly opposite the intent of Congress as expressed in the defeat of the amendment that would have permitted this.

- **ALA urges that the Department revise Sections 29.1 (b) and 29.2 (i) to bring them into compliance with the law.**

¹ 148 Cong. Rec. H5828 (2002) (statement of Rep. Davis).

² 148 Cong. Rec. H5850-5853 & H5869-H5870 (2002).

This revision is all the more necessary in light of the procedures set out in Section 29.4 (c-d). Section 29.4 (c) allows for appointment of CII Officers for “any DHS component or other entity that works with Protected CII,” and (d) sets out their responsibilities. The Department, however, is the sole recipient of funds to manage a CII program and the Homeland Security Act clearly placed this responsibility in DHS. If any agency can be forced to receive CII, other agencies may be forced to:

- (1) Oversee the storage and handling of Protected CII;
- (2) Establish and maintain an ongoing self-inspection program, to include periodic review and assessment of the entity’s storage, handling, and use of Protected CII;
- (3) Establish additional procedures as necessary to prevent unauthorized access to Protected CII; and
- (4) Ensure prompt and appropriate coordination with the CII Program Manager regarding any request, appeal, challenge, complaint, or suggestion arising out of the implementation of these procedures.

As the resource demands of this new CII program are unknown, agencies forced to work with CII for which protection is claimed may be forced to reallocate resources away from existing priorities.

- **ALA urges that the rule should limit the receiving and management of CII submissions to DHS, where the law intended that it be housed and where the resources have been allocated to address this program. Such limitation would also help to address the potentially extensive time delay from the submission of CII to the determination of the CII Program Manager that the information is not Protected CII.**
- **ALA also recommends that a time limit be delineated within which the CII Program Manager (or his or her designee) must make a determination as to whether the submitted information qualifies as Protected CII.**

At the same time, the proposed rules do not clearly delineate a process for following the statutory mandate that the FOIA exemption applies only to voluntarily submitted information, and not to information that companies must already submit to the government or that is customarily in the public domain:

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.

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. This will have the effect of limiting the ability of agencies to receive and use critical infrastructure information that they obtain independently.

- **ALA recommends that the participation of federal agencies be included in the decision about the protected status of submitted CII to ensure that information that already must be submitted to the government, is already within the public domain, or is otherwise obtainable by the agency under legal grounds will not be categorized erroneously as protected CII.**

Proposed Rule 29.6 also contains one glaring omission from the acknowledgment, receipt and validation process: there is no time limit within which the CII Program Manager (or his or her designee) must make a determination as to whether the submitted information qualifies as Protected CII. The federal FOIA, and every state Freedom of Information or Right to Know Act, contains a time limit for compliance with a filed request for information.¹ Such a requirement ensures that the requestor receives an answer when the need for that information is still ripe. Nowhere is this more necessary than in the highly sensitive arena of infrastructure vulnerability. A mandated period in which the agency must act benefits the public interest because it ensures that DHS will engage in timely review of sensitive issues.

DEFINITIONS

Customarily in the Public Domain

Section 29.2 (b) defines Critical Infrastructure Information or CII as information not customarily in the public domain and related to the security of critical infrastructure or protected systems.

- **ALA recommends that the guidelines include a definition of “customarily in the public domain.”** Without a detailed explanation of what does and does not qualify, CII program managers may apply the clause very broadly.
- **ALA urges that DHS establish clear evaluation procedures for assessing whether “information” (a very broad term over which there was significant legislative debate) is “in the public domain.”**

Voluntary or Voluntarily

29.2 (j) defines Voluntary or Voluntarily, when used in reference to any submission of CII to DHS, as “submitted in the absence of DHS's exercise of legal authority to compel access to or submission of such information.” If the Department persists in extending the scope of agencies that can *receive* CII, then, logically, the Department must similarly expand the scope of the “legal authority to compel access to or submission of” CII. Thus, if company-designated CII can be submitted to any federal agency, then the definition of voluntarily must be expanded to the absence of the exercise of legal authority of any agency to compel access to or submission thereof. At an absolute minimum, the definition of voluntarily must be applied only in the absence of the exercise of legal authority... of the agency *receiving* the CII submission.

¹ The Federal FOIA states that an agency has 20 days to respond to a FOIA request with an indication as to whether it will comply with or deny the request. 5 U.S.C. § 552(a)(6)(A)(i).

- **ALA urges that the definition of “voluntary” should be “submitted in the absence of authority to compel access or submission of the information,” as the “exercise” of such authority is open to interpretation. At a minimum, the term “in absence of exercise of legal authority” needs detailed explanation of what does and does not qualify.**

Indeed, Section 29.3 (a) makes this point that the CII Act of 2002 and these procedures do not:

apply to or affect any requirement pertaining to information that must be submitted to a Federal agency or pertaining to the obligation of any Federal agency to disclose such information under the Freedom of Information Act;

apply to any information that is submitted to a Federal agency pursuant to any legal requirement. The fact that a person or entity has voluntarily submitted information pursuant to the CII Act of 2002 does not constitute compliance with any requirement to submit that information or any other such information to a Federal agency under any other provision of law.

The proposed rule prohibits the marking as submitted or protected under the CII Act of 2002 or to be otherwise afforded the protections of the CII Act of 2002 of information that is required to be submitted to a Federal agency to satisfy a provision of law.

- **ALA recommends that this section also instruct companies that they may not claim protected status for submitted information that is customarily in the public domain.**

The proposed rule extends extensive protection to submitted CII, and the process as envisioned will be burdensome on all involved federal personnel and will accord protected status to information that may not merit it for potentially lengthy periods of time.

- **ALA strongly recommends that DHS amend the regulations to put the burden of proof (that the information qualifies for protected status) on submitting companies, rather than leaving a burden of dis-proof on agency personnel.**

Good Faith

Section 29.6 (f) states that “In the event the CII Program Manager determines that any information is not submitted in good faith accordance with the CII Act of 2002 and these procedures, the Program Manager is not required to notify the submitter that the information does not qualify as Protected CII. Section 29.8 (i) also states that Protected CII shall not be used without the written consent of the submitting party “in any civil action arising under Federal or State law if such information is submitted in good faith for homeland security purposes.”

Nowhere in the rule is “good faith “ defined.

- **ALA recommends that the guidelines include a clear definition of “good faith.”**
- **ALA urges that DHS establish clear evaluation procedures for assessing whether information has been submitted in “good faith.”**

CONTROL OVER DISCLOSURE

The proposed rule allows a submitting entity to retain virtually complete control over information it has willingly given to the government. The proposed rule requires (29.8 (d)) state and local government officials, prior to disclosing Protected CII to even first responders, to get “authorization from the CII Program Manager, who shall be responsible for obtaining written consent for any such ... disclosure from the person or entity that submitted the information.” Moreover, the CII Program Manager *may not* authorize such further disclosures unless the Program Manager “first obtains the written consent of the person or entity submitting the information.” This is a road-map for a disaster.

- **ALA urges that the final rule must allow greater discretion to state and local governments, and their employees, to use protected CII to prevent and respond to emergencies.**
- **ALA recommends that the final rule contain an exemption allowing a federal government officer or employee to disclose Protected CII in the event of an actual emergency or proven imminent emergency.**

As the entity is seeking protection for information submitted to the government on the assertion that it is related to risks and vulnerabilities in the national critical infrastructure with which it wants the government’s assistance, allowing the submitter to exert sole control over that information defeats the purpose of enlisting government assistance.

- **ALA recommends that a submitting entity should be required to trade some measure of control over Protected CII in exchange for the assistance it receives in remedying a security vulnerability—and the other benefits it receives for such submission.**

While ALA commends the Department for acknowledging some appropriate role for whistleblowers, Section 29.8 (f) limits the instances in which an officer or employee of the United States can disclose Protected CII with the knowledge that he or she will not be prosecuted. The rule only allows disclosures by a government employee, with prior written approval of specified DHS persons, to Congress or the United States Comptroller General, or in furtherance of the investigation or prosecution of a criminal act. In order to disclose Protected CII without such prior approval the employee must evidence:

- (1) an employee’s or agency’s conduct in violation of criminal law or other law, rule or regulation affecting the critical infrastructure; or

(2) mismanagement, a gross waste of funds, an abuse of authority or a substantial and specific danger to public health or safety affecting the critical infrastructure.

However, if that employee wrongly asserts the existence one of these bases for disclosing information, s/he will be prosecuted. No clear standards exist for determining whether the employee is correctly gauging whether mismanagement, gross waste of funds, abuse of authority, a “specific danger to public health or safety” or whether the information actually relates to the protection of critical infrastructure.

- **ALA urges that the final rule should allow a whistleblower to disclose protected CII without fear of prosecution upon *demonstration of a reasonable belief* of the existence of one or more justifications for disclosure.**

CONCLUSION

The American Library Association (ALA) is opposed to the overly-broad scope of the restriction on access to information held by the government and the resultant constriction of the public’s ability to hold government accountable created by Section 214 of the Homeland Security Act of 2002 and implemented in this proposed rule. We are deeply concerned, given the problems identified in these comments—problems with scope, with lack of definition of central terms and of guidelines for evaluating their application, with the complex system for handling protected CII, with the severe limits on disclosure (beyond even those anticipated in the statute), and with the absence of any challenge or appeal process—that vast amounts of information will enter into a black hole of unaccountability and irremediation. We reiterate that this is not, in our view, the way to protect and secure the health and safety of the American people and to ensure the accountability of government.

We urge that the final rule be amended to take into account the issues addressed in these comments.

Respectfully submitted,



Emily Sheketoff
Executive Director
American Library Association
Washington Office