

Silha Center.txt

Subject: Electronic comments on Proposed Rulemaking/Procedures for Handling CII
Date: Thu, 12 Jun 2003 12:51:19 -0400
From: "Jane Kirtley" <kirtl001@tc.umn.edu>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

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

Attached please find the comments of the Silha Center for the Study of Media Ethics and Law on the Proposed Rule establishing Procedures for Handling Critical Infrastructure Information.

Please contact me as soon as possible if you should have any difficulty opening the attachment.

Thank you for the opportunity to comment.

Jane E. Kirtley
Silha Professor of Media Ethics and Law
Director, Silha Center for the Study of Media Ethics and Law
School of Journalism and Mass Communication
University of Minnesota
111 Murphy Hall
206 Church Street, SE
Minneapolis, MN 55455
612 625 9038 (voice)
612 626 8012 (fax)
kirtl001@tc.umn.edu (e-mail)

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

BEFORE THE DEPARTMENT OF HOMELAND SECURITY

In re: Notice of Proposed Rulemaking Procedures for Handling Critical Infrastructure Information

COMMENTS OF THE SILHA CENTER FOR THE STUDY OF MEDIA ETHICS AND LAW

Submitted June 12, 2003

The Silha Center for the Study of Media Ethics and Law submits the following comments to the Department of Homeland Security (DHS, “Department”) in response to its April 15, 2003 invitation, published at 68 Fed. Reg. 18523, seeking comments regarding its Proposed Rulemaking to establish Procedures for Handling Critical Infrastructure Information (CII) to implement Section 214, subtitle B of Title 2, of the Homeland Security Act of 2002 (the “Critical Infrastructure Information Act of 2002” or “CII Act”), to be codified at 6 CFR Part 29.

The Silha Center for the Study of Media Ethics and Law is a research center located within the School of Journalism and Mass Communication at the University of Minnesota. Its primary mission is to conduct research on, and promote understanding of, legal and ethical issues affecting the mass media. The Silha Center also sponsors an annual lecture series; hosts forums, conferences and symposia; produces the *Silha Bulletin*, a quarterly newsletter, and other publications; and provides information about media law and ethics to the public.

Purpose of these comments

We recognize that certain highly-sensitive Critical Infrastructure Information may, at least for limited periods of time, need to be withheld from the general public to protect legitimate security concerns. We also recognize that the success of the CII program as currently structured relies, in large part, on the voluntary participation of the private sector. We are concerned, however, that the proposed rules go too far in allowing submitters to categorically assert a presumptive necessity for secrecy. Rather than working from a presumption of openness and creating procedures that will ensure that any decisions to withhold information will be narrowly tailored, the Department's proposed rules reverse that presumption. Secrecy is the default rule; access, the exception. The ability of the press to inform the public about deficiencies in the nation's critical infrastructure will be undermined by the over-broad protection of business information under the proposed rules.

There is a fine line between encouraging information-sharing by the private sector and facilitating abuse of what should be a very narrow exemption. We are concerned that some corporations will, in fact, abuse the proposed rules in order to shield themselves from liability and to deprive the public of vital information. Under the proposed rules, DHS will do little, if anything, to discourage this.

Accordingly, we urge DHS to:

- Develop a final rule that provides clarity and precision in its terminology
- Strengthen and speed up validation proceedings to insure a free flow of information to the public

- Untie the hands of government officials seeking to share, use, and distribute CII to prevent terrorism and promote public health and safety
- Protect legitimate whistleblowing on the part of conscientious government employees by removing criminal penalties.

We address these concerns more fully in the comments below. We also comment on specific provisions of the proposed rule.

Sharpen definitions

Some of the most compelling concerns raised by the proposed CII rules spring from their imprecise and ambiguous definitions.

“Submitted to DHS.” Id. at § 29.2(i). When Congress was debating the Critical Infrastructure Information Act of 2002, a proposal to allow submission of CII to all federal agencies was voted down. The proposed rules exceed the scope of the law and violate clear Congressional intent by expanding the definition of “submission” to include information received first by other agencies and then passed on to DHS. *Id.* at § 29.2(i). The proposed rules require agencies to forward information expressly marked as CII to DHS. *Id.* at § 29.5(c). Corporations submitting information to any government agency need merely label the information as CII and ask that it be sent to the CII Program Manager to receive presumed secret status. The other federal agencies apparently have no discretion to independently evaluate the validity of this request. *Id.* at § 29.5 (d). These provisions are inconsistent with the unambiguous language of the statute.

“Submitted to DHS” should mean exactly that: CII that is provided directly to DHS. This definition should be revised to reduce the possibility for abuse.

“Voluntary or Voluntarily.” Under the proposed rules, “voluntary or voluntarily” means “submitted in the absence of DHS’s exercise of legal authority.” *Id.* at 29.2(j). By its own terms, this rule requires the *exercise* of authority. Therefore, “voluntary or voluntarily” would include information that could be required to be submitted, but which has not yet been formally demanded by DHS. To clarify this, “voluntary or voluntarily” should be defined more narrowly, to be limited to submissions made in the absence of *any legal* (e.g. regulatory) authority, whether exercised or not, of DHS or any government agency.

Revise validation procedures

Deference to Submitters. The proposed rules grant broad discretion to the submitter to determine what is CII. *Id.* at § 29.2(b); *Supplementary Information: Background.* The deference paid to submitters undermines the integrity of the validation process. *Id.* at § 29.6(e)(1).

In its revisions to the proposed rules, DHS should recognize that the power to withhold information from the public is not a duty that should be lightly assigned. Rather than deferring to the submitting corporation, DHS should utilize the expertise of existing government access professionals to judge whether information indeed qualifies as CII. These professionals bring a valuable skill-set, developed through long experience in applying the processes of the Freedom of Information Act to evaluate specific requests, that would be easily transferable to the requirements and needs of DHS. Failing to utilize these existing government resources will result in unnecessary duplication of efforts, and will ultimately undermine the flow of information to the public.

Criteria. Under the proposed rules, the CII Program Manager has sole authority “to validate the satisfaction of the definition of CII as established by the law.” *Id.* at § 29.6(e). The validation procedures under the proposed rules do not define the process by which it will be determined that information submitted must concern critical infrastructure, have been submitted voluntarily, and in good faith. Although these requirements may seem self-evident, they must be made explicit in the proposed rules.

The rules should provide much more detailed procedures for determining what information is, or is not, “CII,” “voluntarily submitted,” and submitted “in good faith.” Conceivably, the section marked “Reserved” is where these important procedures will appear. *Id.* at § 29.6(e)(2). If so, these procedures should also be subject to public comment because they represent the essence of how and whether the CII program will work as Congress intended.

Rejection. The proposed rules provide that the Program Manager may reject information which he or she deems as unqualified for protection. Submitters, however, will be notified that their information did not qualify for protection and will be given a second chance to argue that their information is really CII. *Id.* at § 29.6(e)(i). Failing that, submitters may elect — as the DHS presumes they will — to have non-qualifying information destroyed. *Id.* at § 29.6(e)(i)(D)-(ii). And, if submitters choose not to respond to an adverse notification, the Program Manager must destroy the information except under very limited circumstances. *Id.* As a consequence, submitters have nothing to lose by labeling non-qualifying information as CII. The incentive for companies to shield themselves by providing information to the government labeled “CII” is simply too great. If a company does submit information as “CII” in bad faith, the only “punishment”

is that the Program Manager will not be “required” to notify that company that the information did not qualify for protection. *Id.* at § 29.6(e)-(f).

The proposed rules, perhaps inadvertently, create a system where information submitted by the private sector — even information submitted in bad faith — will *never* be released to the public. At a minimum, abuse of the CII Act should mean the information is deemed unprotected, released to the public, and used as the government sees fit.

Presumption of Protection. Information is presumed to be protected CII as soon as it is filed with a government agency. *Id.* at § 29.6(b). But the Department should withhold information from the public based only on a carefully defined and narrowly tailored case-by-case analysis. Each submission to DHS marked “CII” merits prompt and thorough scrutiny, not an automatic presumption that the information is protected CII.

Further, although the proposed rules require the CII Program Manager to acknowledge receipt of the information within thirty days, they provide no timeline for reviewing and validating the information as CII. This means that the presumed protection could last indefinitely, because the power to reverse the presumption of protection and to reject submitted information as non-CII is also significantly limited by the proposed rules. *Id.* at § 29.6(b), § 29.6(d)(1). Only the CII Program Manager can reject submitted information. *Id.* at § 29.6(e). The reality of reviewing and validating all the submitted information in a careful manner makes it very likely that non-qualifying information will be concealed for years. Meanwhile, the ability of the press and public to obtain this information is in limbo. There must be a required response time for validating submissions, and it should be brief.

Provide for Redaction

The proposed rules make no provision for redacting CII information and releasing the balance of CII submissions. Portions of documents that contain legitimate CII may be redacted, but non-CII should be available for disclosure. This would prevent companies from bundling “trace” amounts of CII into submissions in order to prevent the entire submission from being disclosed, and would be consistent with existing FOIA processing procedures.

We note that the proposed rules provide for the issuance of general “advisories, alerts and warnings” concerning threats to critical infrastructure. *Id.* at § 29.8(e). But the rules also require that CII itself, as well as relevant identifying information about submitters, must be withheld. Without more detail, these alerts constitute, at best, unspecified hints of danger, rather than meaningful and useful warnings. Providing at least the redacted information to the press and public might help give these warnings some much-needed substance.

Empower government officials who discover critical infrastructure failures

The “no questions asked” approach of the proposed rules may serve the privacy needs of business, but does not serve the needs of the public. Although the argument has been made that immunity from suit, as well as secrecy, is necessary to induce the private sector to share information, promising companies that information submitted will never be used against their interests goes too far. *Id.* at § 29.3(c). The Department should not be a storehouse of industry inadequacies, with no viable enforcement remedies. Under the proposed rules, DHS could not alert a regulatory agency to inspect a site that filed CII

has revealed to be a security risk without the consent of the company. The Department, other federal agencies, and State and local governments are unable to share, use, and distribute information freely and effectively. *Id.* at § 29.8(b).

The proposed rules contain many examples of these information breakdowns. For example, they provide that the CII Program Manager will, in effect, “deputize” government employees to serve as CII Officers when CII is provided by DHS to other government agencies. *Id.* at § 29.4(c). These CII Officers are charged with preventing unauthorized access to protected CII. *Id.* at § 29.4(d)(3). But lacking the appropriate expertise, unequipped to make proper use of CII, and facing termination, imprisonment, and fines for disclosure, these employees inevitably will err on the side of secrecy. *Id.* at § 29.9(d). This approach hamstring government officials in serving the public, and is profoundly at odds with the presumption of openness that is essential to our system of government.

The government officials who are closest to critical infrastructure problems and are the most knowledgeable about them are at the State and local level. But, as is the case with federal entities, State and local governments are forbidden to forward CII to another party without CII Program Manager authorization, which is in turn dependent upon the consent of the company. *Id.* at § 29.8(d)(2). These public servants are muzzled from informing the public of specific, immediate, and grave risks.

Lastly, while the proposed rules provide that State and local governments may freely use CII that they gain independently, they may be required to prove that they were not “tipped-off” by a DHS source, should the federal government instigate a criminal

investigation in the belief that they had a “leak” within DHS. *Id.* at § 29.8(g)(2), § 29.9(b).

In short, despite the statement that CII “will be utilized for securing the United States,” the effect of the proposed rules is to place industry secrecy ahead of national security. *Id.* at *Supplementary Information: Background*.

Encourage whistleblowing

Whistleblower protections under the proposed rules are limited to protecting whistleblowers who “report up” to superiors. *Id.* at § 29.8(f)(2). Simply put, this is not how whistleblowing works. The whistleblowing protections should be expanded to allow for disclosure to Congress, other government agencies, the press, and the public when reasonably necessary. The proposed rules compound these problems by criminalizing legitimate whistleblowing by civil servants. *Id.* at § 29.8(f)(3).

Journalists who obtain critical infrastructure information without relying on the government as a source could also be compromised. Consider a journalist who learns of the weakness of a computer system from a source within an information technology company. If that company has submitted identical or similar information to DHS, the criminal penalties provision might be used to initiate a government investigation. *Id.* at § 29.9(b). This investigation might identify the source of the information within the company’s ranks. The government might then subpoena the reporter to reveal the source. This source might face civil or even criminal penalties at the instigation of the company. Under threat of termination, fines, and imprisonment, whistleblowers in both the public and private sectors will be chilled by this language, impairing the ability of the press to gather and report information of vital importance to the public. *Id.* at § 29.9(d).

Conclusion

For all the foregoing reasons, we urge DHS to significantly revise the proposed rules to insure, at a minimum, that traditional levels of access and government openness are maintained. For the benefit of journalists who cover government and industry activities, but also for the benefit of the public, we encourage DHS to reconsider and clarify these proposed rules.

The Department must narrow the opportunities for companies to abuse these procedures. The Department should be a storehouse of critical infrastructure information, not a dumping ground for industry wrongdoings disclosed under the pretext of an over-broad exemption. The Department cannot rely solely on the good faith of businesses in formulating these proposed rules. Americans will be no safer from terrorism under the approach reflected in the proposed rules.

We appreciate the opportunity to comment on the proposed rules.

Respectfully submitted,

Jane E. Kirtley, Silha Professor of Media Ethics and Law
Director, Silha Center for the Study of Media Ethics and Law
Thomas Corbett, Silha Research Assistant
Silha Center for the Study of Media Ethics and Law
School of Journalism and Mass Communication
University of Minnesota
111 Murphy Hall
206 Church Street, SE
Minneapolis, MN 55455
612 625 3421