

Society of Professional Journalists.txt

Subject: Comments to NPRM 68 Fed Reg 18524  
Date: Mon, 16 Jun 2003 15:38:52 -0400  
From: "Lystad, Robert" <RLystad@bakerlaw.com>  
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>  
CC: "Leger, Robert" <RLEGER@springfi.gannett.com>, <mmckerral@amcity.com>, <igratz@mpbc.org>, <across@mis.net>, <ian@kpax.com>, <charles\_davis@jour.missouri.edu>, "Brown, Bruce" <BBrown@bakerlaw.com>, "Powell, Michael" <MPowell@bakerlaw.com>

Please find attached the comments by the Society of Professional Journalists to the proposed procedures for handling critical infrastructure information, 6 CFR Part 29.

Thank you.

Robert D. Lystad

<<DHS Comment E-mail Letter 6-16-03.doc>>

Robert D. Lystad  
Baker & Hostetler LLP  
Suite 1100  
1050 Connecticut Ave., NW  
Washington, DC 20036  
202-861-1707  
Fax: 202-861-1783  
rlystad@bakerlaw.com

\*\*\*\*\*

THIS MESSAGE IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL, AND EXEMPT FROM DISCLOSURE UNDER APPLICABLE LAW.

If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution, forwarding, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the sender immediately by e-mail or

Society of Professional Journalists.txt  
telephone, and delete the original message immediately.

Thank you.

\*\*\*\*\*

DHS Comment E-mail Letter 6-16-03.doc

6-16-03.doc	Name:	DHS Comment E-mail Letter
(application/msword)	Type:	WINWORD File
	Encoding:	base64
6-16-03.doc	Description:	DHS Comment E-mail Letter

---

BAKER  
&  
HOSTETLER LLP  
COUNSELLORS AT LAW

---

WASHINGTON SQUARE, SUITE 1100 • 1050 CONNECTICUT AVENUE, N.W. • WASHINGTON, D.C. 20036-5304 • (202) 861-1500  
FAX (202) 861-1783

ROBERT D. LYSTAD  
WRITER'S DIRECT DIAL NUMBER (202) 861-1707  
E-MAIL: RLYSTAD@BAKERLAW.COM

June 16, 2003

Via E-mail ([cii.regcomments@DHS.gov](mailto:cii.regcomments@DHS.gov)) and Regular Mail

Associate General Counsel (General Law)  
Department of Homeland Security  
Washington, D.C. 20528

Re: Notice of Proposed Rulemaking  
Procedures for Handling Critical Infrastructure Information  
6 CFR Part 29

Dear Sir/Madame:

As counsel to the Society of Professional Journalists ("the Society"), we are submitting these comments on behalf of the Society in response to the notice of proposed rulemaking issued by the U.S. Department of Homeland Security ("DHS") at 68 Federal Register 18524 (April 15, 2003) calling for comments to the proposed rules to implement Section 214 of the Homeland Security Act of 2002 regarding the receipt, care and storage of Critical Infrastructure Information ("CII") voluntarily submitted to the federal government.

The Society is a voluntary, non-profit organization dedicated to improving and protecting journalism. As the nation's largest and most broad-based journalism organization, the Society has actively sought to protect its members' and the public's constitutional, statutory and common law rights of access to public records and proceedings and, in so doing, promote the free flow of information vital to a well-informed citizenry.

Preliminary Comments

The notice of proposed rulemaking issued in April to implement § 214 of the Homeland Security Act has the potential to affect not only DHS, but also virtually every other government agency, as well as the public's ability to gain access to vital information from these agencies concerning federal government actions.

The proposed rule outlines the establishment of a critical infrastructure protection program that protects from disclosure to the general public any CII which is voluntarily submitted either directly or indirectly to DHS. Procedures for Handling Critical Infrastructure Information ("CII Procedures"), 68 Fed. Reg. 18524 (proposed April 15, 2003). Essentially, the CII program proposes granting corporations that voluntarily submit information on critical infrastructure vulnerabilities secrecy, civil immunity, preemption of state and local disclosure laws, and protection from whistleblowers. *Id.*

As currently written, however, many provisions in the proposed rule are overly broad in terms of the type and amount of information covered and far too deferential to the private providers of such information at the expense of the safety and well-being of the general public. If the proposed rule were to take effect as written, it has the potential to both hinder the missions of many federal regulatory agencies beyond DHS itself while also providing a safety net for bad actors in the private sector, all without fulfilling the proposed rule's intended purpose of protecting the security of the nation's critical infrastructure.

The Society believes that the proposed CII guidelines can be modified to better serve the interests of both national security and the American public. For example, the rule should narrow the focus of what types of information can be designated as protected CII and limit the scope of the CII program to DHS itself rather than extending its purviews to all federal agencies. Through these modifications and others, DHS can achieve its goals of effective CII protection without preventing public access to information vital to the welfare of the U.S. citizenry.

#### CII Program Should Be Limited to Direct Submissions to DHS

The overall scope of the CII program was a key issue of intense debate during the passage of the Homeland Security Act, and an amendment which would have allowed all federal agencies to accept CII was voted down. Despite this, however, the proposed rule suggests that the CII program would apply to *any* government agency that handles such information. Section 29.2(i) of the proposed rule provides that

*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.

CII Procedures, 68 Fed. Reg. at 18525.

This provision allowing all government agencies to receive CII submissions rather than restricting the receipt of such submissions to DHS alone is the most significant example of the proposed rule's unwarranted overbreadth. In order to serve the interests of allowing the government to protect legitimate CII while also preventing infringement on the public's right of access to vital, non-protected information, the CII program should be limited to direct submissions to DHS only, for several reasons. First, a program that allows all agencies to receive CII submissions could result in the extension of CII protections to non-CII and even

required agency submissions. Thus, material that routinely is available to the public under the Freedom of Information Act could be withheld from disclosure merely because portions of such materials contain CII. For example, if a required report containing some additional CII were to be filed with an agency other than DHS, then the non-CII portions of the report, or even the entire report, could be withheld from the public under the proposed rule. Limiting the CII program to direction submissions to DHS would present less potential for such confusion. Such a limitation would also create fewer opportunities for companies to misuse CII protections for information connected to other agencies and concerning the well-being of the public, such as matters related to the environment, worker safety and health threats.

Second, from an efficiency perspective, extending the CII program to other government agencies will also burden those agencies by forcing them to modify the ways in which they handle information submissions in order to conform with the new CII protections. The Homeland Security Act placed the responsibility for handling CII directly on DHS, which is expected to be the second largest federal agency and thus have extensive resources available to deal with the burdens imposed by the CII program.

Finally, by extending the CII program to agencies beyond DHS, it becomes possible that other agencies may be forced to work with extensive amounts of CII and therefore be forced to reallocate resources away from existing priorities. Because resource demands of this new CII program are unknown, it is unreasonable for DHS to shift responsibility for this program to other agencies without a more clear understanding of how the CII program could impact the operations of those agencies. Thus the proposed rule should again limit the receipt and management of CII submissions to DHS, where the resources have been set aside to handle the program.

#### Proposed Rule's Definition of "Voluntary" Should be Narrowed

The proposed rule provides that information must be submitted "voluntarily" in order to qualify as CII. The rule's definition of what constitutes voluntarily submitted information, however, is overly broad and allows far too much information to fall into that category.

Section 29.2(j) of the proposed rule defines voluntarily submitted information as information "submitted in the absence of DHS's exercise of legal authority to compel access to or submission of such information." CII Procedures, 68 Fed. Reg. at 18525-26. According to this definition, the only information that would be considered not "voluntary" is that which DHS has exercised legal authority to obtain. This language effectively means that all other information submitted to the government, for any reason, would qualify as voluntarily submitted under the proposed rule.

The Society believes that the overbroad scope of this definition would prevent public access to a far wider range of information than necessary to further the interests of national security. In the worst case, the current definition of "voluntary" would allow a corporation to effectively hide, under the guise of being CII submissions, information required by any number of health and safety, labor, environmental and energy laws, among others. Originally, the requirement that CII submissions had to be voluntary was intended to protect information

currently collected across government agencies from disappearing. In order to fulfill that purpose, the proposed rule's definition of "voluntary" should *exclude* information collected by any federal agency.

The definition of "voluntary" should also not merely exclude information that an agency has *exercised* its legal authority to obtain. Simply because an agency has the authority to require submission and the information was submitted does not necessarily mean that the agency "exercised" its authority to compel the submission. For example, information subpoenaed by an agency could still be deemed "voluntary" if the agency has not taken affirmative steps to exercise its authority to enforce the subpoena. Thus, the Society believes that "voluntary" should be defined as submitted in the absence of authority to compel access or submission of the information.

#### Degree of Latitude Given to Entities Submitting CII Information is Overly Broad

The current proposed rule provides private companies with too much leeway and control over the entire CII program at the expenses of both legitimately safeguarding national security interests and keeping the American public informed of critical safety information. The Background section of the proposed rule provides that

Although the Homeland Security Act establishes a working definition of critical infrastructure information, the Department relies upon the discretion of the submitter as to whether the volunteered information meets the definition of critical infrastructure information.

CII Procedures, 68 Fed. Reg. at 18524.

As this wording indicates, the CII procedures shift the majority of authority and control over information to the submitting corporations. Providing corporations carte blanche when it comes to CII submissions is unsettling, especially given the current climate of corporate deception scandals, which have shed legitimate doubt on many companies' abilities to act consistently in accord with the public's best interests.

Under the proposed rule, the high degree of discretion provided to corporations would allow submitting companies to essentially send *any* information to *any* government agency and merely attach the label "CII" to the submission in order to allow the information to qualify for the stringent nondisclosure protections of the proposed rule. Further exacerbating this potential for overuse and abuse of the CII provisions is the fact that the proposed rule gives no guidance to businesses on identifying needed CII, nor does it contain an effective policing mechanism for ensuring that only bona fide CII will be so marked. Furthermore, there are no penalties provided in the proposed rule for intentionally or negligently marking as "CII" information that is not.

When considering reformulations of the proposed rule's policies, DHS should consider the well-established procedures for information submission outlined by the Freedom of Information Act. Under the FOIA, companies have the ability to label information as either confidential business information or proprietary information, but it is ultimately the

government's judgment once the information is requested as to whether the claim is valid and if the information should be released. Moreover, the FOIA requires that exempt information be segregated and redacted so that as much of an agency record as possible may be disclosed. The plan for CII-marked materials, however, contains no such segregation requirement.

The Society praises DHS for its inclusion of the provision outlined in Section 29.3(a), which provides 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." CII Procedures, 68 Fed. Reg. at 18526. This language from the proposed rule is noteworthy in that it prohibits corporations from haphazardly or inaccurately labeling *required* government agency submissions as CII. This section notwithstanding, however, the proposed rule still provides corporations with far too little guidance on what types of non-required submissions would qualify as legitimate CII, and the Society encourages DHS to follow a path similar to that it has taken here with regards to required submissions and narrow the seemingly boundless discretion with which corporations can use the CII label with regard to non-required agency submissions.

The CII program should provide greater guidance to submitting corporations while also providing for enhanced governmental scrutiny of information submitted as CII such as that provided for by the FOIA. The Society believes that the proposed rule should contain more exacting guidelines for companies as to what types of information would qualify as CII and provide for penalties to ensure that companies do not take undue advantage of the program to prevent from disclosure information that should otherwise be made available to the public.

#### Presumption of All Submitted Information as CII is Unnecessarily Over-Inclusive

Another far too expansive aspect of the proposed CII rule is the presumption that all information submitted as CII qualifies as legitimate CII, outlined by Section 29.6(b) of the proposed rule. CII Procedures, 68 Fed. Reg. at 18527. The proposed rule provides that the standard procedure for all information submitted as CII should be that it automatically receives CII protections, whether or not the submitted information does indeed meet the DHS's definition of CII. The protections can only be eliminated when the CII Program Manager renders a decision that the information does not qualify for the protections.

This presumption compounds the problem of providing submitting companies with too much discretion because there is no requirement that the information be evaluated by the Program Manager within a certain timeframe. Without a deadline, non-qualifying information could potentially receive the CII protections for years while the Program Manager considers the determination or while simply sitting in an agency's "in-box" awaiting processing. Under the FOIA — even with a mandatory deadline — there are requests that have remained undecided for years, which should signal just how much worse that process would be without the deadline. Such delays in CII processing are extremely likely if the program receives any significant amount of participation since the proposed rule allows only the Program Manager to render decisions on information. The Society believes that the proposed rule should contain procedures for FOIA officers and CII officers to expedite the process, either for information they believe

does not meet the requirements for protection or for information that is responsive to a FOIA request.

#### Government Should Have More Discretion in Handling Non-CII Submissions

The proposed rule also demonstrates its over-reliance on submitting corporations in its procedure for handling information that does not qualify as CII. As written, the rule would allow the submitter to choose if the non-CII information is retained by the government without CII protections or if the information should be disposed of. CII Procedures, 68 Fed. Reg. at 18527. The Society believes, however, that the public interest will best be served through a process that would consider the reason that the submitted information did not qualify as legitimate CII before offering the submitter a choice in how to deal with such information.

If, for example, the information is found not to be considered “voluntary” because of an ongoing regulatory process or overlapping with required submissions, then the Program Manager should have the option of transferring the information to the appropriate regulatory agency. If the information does not address critical infrastructure specifically but still addresses issues of public safety or concern, there should be a balancing test by which the Program Manager considers the public benefits of the information before offering the submitting corporations the option of destroying the information.

#### Procedures for Handling CII Requested Pursuant to FOIA

The proposed rule stipulates that protected CII submissions receive exemption from the disclosure requirements under FOIA, which is provided for in the rule by Section 29.8(g). CII Procedures, 68 Fed. Reg. at 18528-29. However, the proposed rule fails to establish any procedures for management of FOIA requests for protected CII other than to simply state that the CII will be considered exempt from such requests. The Society urges DHS to formulate and adopt clearly defined procedures for handling FOIA requests for protected CII. Such procedures should include enhanced scrutiny and review of the potential CII status of any protected CII requested under FOIA, potentially by a FOIA officer handling any such request. The proposed rule should also set up procedures for the partial release of information submitted under the CII program if pieces of a submission do not qualify as protected CII, which would be in keeping with the standard practice for exemptions under FOIA.

#### Proposed Rule Should Not Provide for Criminal Penalties for Unauthorized CII Disclosure

Under the current provisions of the proposed rule, CII that contains evidence of fraud, waste or public safety risks could not be disclosed even to Congress unless the disclosing individual/entity has received written consent from the corporation that submitted the information or authorization from within DHS itself. CII Procedures, 68 Fed. Reg. at 18528. Even more unsettling is that if a government employee did blow the whistle to Congress, another federal agency or anyone other than the Inspector General or a designee of DHS, then they would face criminal charges under the current proposed rule. *Id.*



The Whistleblower Protection Act traditionally has provided protection for individuals who make unauthorized disclosures of information for appropriate reasons, often including but not limited to the safety and health of the public. The criminal penalties sanctioned by the proposed rule for unauthorized CII disclosure will take priority over the Whistleblower Protection Act, however, unless DHS specifically states that the proposed rule's criminal penalties do not apply to whistleblower actions. The Society believes that the federal government should not turn its back on the value whistleblowing has and continues to play in protecting American citizens from bad actors and urges DHS to amend the proposed rule provide that the criminal penalties for unauthorized CII disclosure will not apply to legitimate whistleblowing activities as described in the Whistleblower Protection Act.

### Conclusion

The need to protect information vital to our nation's critical infrastructure is undoubtedly more significant than ever. The Society believes, however, that DHS should take care to implement a CII program that will accomplish the goal of preventing CII-related security hazards while not unduly jeopardizing one of the core bedrocks of U.S. democracy — namely, a well-informed citizenship — by limiting the public's access to information in a way that could threaten, rather than enhance, the safety of Americans.

The Society appreciates the careful attention that DHS is devoting to the regulations implementing the CII program, and also for the opportunity to comment. For further information about the Society's comments and suggestions, please feel free to contact us.

Sincerely yours,

Robert D. Lystad

cc: Mr. Robert Leger, President, SPJ  
Mr. Gordon "Mac" McKerral, President-Elect, SPJ  
Mr. Irwin Gratz, Secretary-Treasurer, SPJ  
Mr. Al Cross, Immediate Past-President, SPJ  
Mr. Ian Marquand, Co-Chair, SPJ FOI Committee  
Mr. Charles Davis, Co-Chair, SPJ FOI Committee