

Radio Television News Directors Association.txt  
Subject: Comments of the Radio-Television News Directors Association attached  
Date: Mon, 16 Jun 2003 16:24:48 -0400  
From: "Kirby, Kathleen" <kkirby@wrf.com>  
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Kathleen A. Kirby  
Wiley Rein & Fielding LLP  
1776 K Street NW  
Washington, DC 20006  
202.719.3360  
202.719.7049 (fax)  
kkirby@wrf.com

DOC038.PDF           Name: DOC038.PDF  
                      Type: Acrobat (application/pdf)  
                      Encoding: base64  
                      Description: DOC038.PDF

---



Wiley Rein & Fielding LLP

1776 K STREET NW  
WASHINGTON, DC 20006  
PHONE 202.719.7000  
FAX 202.719.7049

Virginia Office  
7925 JONES BRANCH DRIVE  
SUITE 6200  
McLEAN, VA 22102  
PHONE 703.905.2800  
FAX 703.905.2820

www.wrf.com

June 16, 2003

Kathleen A. Kirby  
202.719.3360  
kkirby@wrf.com

**BY E-MAIL**

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

Re: 6 C.F.R. Part 29  
Procedures for Handling Critical Infrastructure Information

Dear Sir/Madam:

The Radio-Television News Directors Association ("RTNDA"), by its attorney, hereby submits its comments in response to the above-referenced regulations published in the Federal Register on April 15, 2003. RTNDA is the world's largest professional organization devoted exclusively to electronic journalism. RTNDA represents local and network news executives in broadcasting, cable and other electronic media in more than 30 countries.

The notice of proposed rulemaking establishes for Federal agencies the uniform procedures 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. RTNDA believes the content of the proposed rules is troubling and has far reaching implications for the public. The CII rule proposed by DHS requires significant revisions to ensure that the program does not reduce openness or permit misuse by corporations.

**1. Scope of CII Program**

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.

RTNDA submits that the rules should be revised to limit the scope of the CII program significantly. As the Homeland Security Act was being debated, the question of which federal agencies would be covered by the CII provisions was intensely deliberated. An amendment that allowed all federal agencies to accept CII was voted down. Despite this, the proposed rule suggests that the CII program would apply to *any* agency that handles CII information, not just DHS.

The expansion to allow all agencies to receive CII submissions is the single most significant problem with DHS's proposed rules. RTNDA submits that the CII program should be limited in scope (*i.e.*, limited to direct submissions to DHS) for several reasons. First, a program that allows all agencies to receive CII directly could extend CII protections to non-CII, and conceivably to required agency submissions. For example, if a report required to be filed by a regulated entity with a government agency contained additional information that could be labeled CII, then required portions of the report—or even the entire report—could be withheld from the public under the CII protections. If the CII program were limited to direct submissions to DHS, there would be less possibility of confusion and overuse of CII protections for submissions to other agencies of information of keen public interest, for example, information concerning the environment, worker safety and health threats.

Second, a broad CII program will make it more difficult for federal agencies to manage information and to determine effectively and efficiently what information may or may not be made public. It is inevitable that a broad program will cause significant delays in the sharing of information with other federal agencies and with the public.

## **2. Definition of Voluntary**

29.2 (j) Voluntary or Voluntarily, when used in reference to any submission of CII to DHS, means submitted in the absence of DHS's exercise of legal authority to compel access to or submissions of such information.

In order to qualify as CII, information must be submitted "voluntarily." The proposed rules, however, define voluntary so broadly as to afford a vast amount of information CII protection. Under the proposed definition, the only information that is not "voluntary" is that which DHS has obtained pursuant to an exercise of the agency's legal authority. Thus, all other information submitted to the government for any reason qualifies as voluntarily submitted. The provisions would allow companies to withhold from public scrutiny, under the CII protections, information required to be submitted by any number of regulations, including environmental, health and safety, labor, transportation, and energy laws. Much of this information would otherwise be publicly available. RTNDA submits that the definition of voluntary should be revised to cover only that information that is submitted to DHS in the absence of authority to compel access or submission of the information.

Associate General Counsel  
June 16, 2003  
Page 3

Potentially extending CII protection (including exemption from the Freedom of Information Act ("FOIA")) to any information required to be filed with a Federal agency under various laws and for any number of regulatory purposes invites abuse by submitting corporations and disservices the public interest.

### **3. Criminal Penalties for Unauthorized Disclosure**

RTNDA also is particularly concerned about the criminal penalties imposed by the proposed rules for disclosure of CII by a civil employee. Under the proposed rules, CII that evidences waste, fraud or serious public safety risks could not be disclosed to the public, other agencies or even to Congress without written consent from the corporation that submitted the information. In fact, if a government employee did whistleblow to Congress or another Federal agency or anyone other than the Inspector general or a designee of the Secretary of DHS, they would face criminal charges.

Whistleblowers have been and continue to be important sources of information concerning illegal or inappropriate government actions. The government historically has understood the value of unauthorized disclosures in certain instances, and has protected them under the Whistleblower Protection Act. Unfortunately, the Whistleblower Protection Act applies only to information lacking specific protections from disclosure, such as protections for classified and national security information. DHS should revise its CII rules, therefore, to state specifically that the criminal penalties do not apply to disclosures as described in the Whistleblower Protection Act. Without the protections that normally are afforded government employees, there will exist no freedom to report on government misconduct. This ability is fundamental to our democratic society.

### **4. Procedures for Managing CII**

The proposed rules appear to shift authority and control over submitted information from the government to corporations. Although the Homeland Security Act establishes a working definition of CII, under the proposed rules, DHS would rely upon the discretion of the submitter as to whether the volunteered information meets that definition. Under the FOIA, when companies submit information to a government agency, they are able to request that certain information be withheld from public view because it is confidential or proprietary. It is ultimately the government's decision, however, whether or not the claim is valid, and whether or not the information should be released. Under the proposed rules governing the

Associate General Counsel  
June 16, 2003  
Page 4

receipt of CII, corporations are given far too much latitude in controlling the free flow of information. DHS should specify strict requirements and procedures that corporations must follow in order to qualify for CII protections.

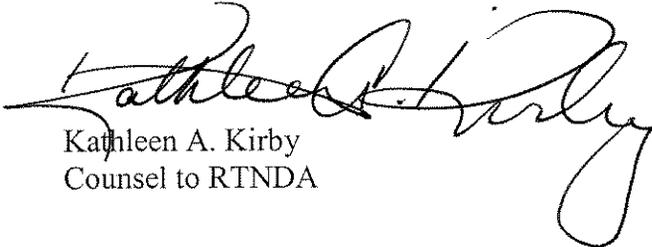
The good faith requirement incorporated in both the rules and the underlying legislation remains the only safeguard specifically addressing the possibility that submitters may attempt to misuse the CII program for the incentives it offers. Unfortunately, the proposed rule does little to define what constitutes "good faith," neither setting forth a list of attributes nor providing an explanation of the procedures to be used to test submissions against this requirement.

Further, the program needs more than one Program Manager conducting the initial validation of submissions in order to avoid massive delays and backlogs. There should be an additional review of protected CII status whenever the information is requested through FOIA. Finally, the rules should be revised to incorporate procedures to allow portions of records to be released if there are pieces that are not properly classified as CII. Such procedures would be consistent with what is currently practiced under FOIA.

### **Conclusion**

The CII rules as proposed have the potential to significantly and adversely affect openness and good government. RTNDA urges DHS to revise the rules as set forth above.

Respectfully submitted,



Kathleen A. Kirby  
Counsel to RTNDA