

The Real Estate Roundtable.txt

Subject: [FR Doc: 03-09126];[Page 18523-18529]; Critical Infrastructure Information; handling procedures

Date: Mon, 16 Jun 2003 15:56:36 -0400

From: <Jeffrey.Knight@shawpittman.com>

To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

CC: <rplatt@rer.org>,  
<Sheldon.Weisel@shawpittman.com>,  
<JerryJacobs@shawpittman.com>

Dear Sir/Madam:

I am writing on behalf of The Real Estate Roundtable to provide comments on the Department of Homeland Security's proposed rule entitled "Procedures for Handling Critical Infrastructure Information," published at 68 Fed. Reg. 18524 (April 15, 2003). The Roundtable's comments on the proposed regulations are attached as an Adobe Acrobat file. Please contact me if you have any problems accessing the attached document or need additional information regarding this submission.

(See attached file: Comments of The Roundtable.pdf)

Jeffrey A. Knight  
Shaw Pittman LLP  
2300 N Street, NW  
Washington, DC 20037  
ph: 202.663.9152  
fax: 202.663.8007

This electronic message transmission contains information from the law firm Shaw Pittman LLP that may be confidential or privileged. The information is intended solely for the recipient and use by any other party is not authorized. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this information is prohibited. If you have received this electronic transmission in error, please notify us immediately by telephone (1.202.663.8000, or in the UK, 020 7847 9500) or by electronic mail postmaster@shawpittman.com. Thank You.

	Name: Comments of The Roundtable.pdf
Comments of The Roundtable.pdf	Type: Acrobat (application/pdf)
	Encoding: base64
	Description: Comments of The Roundtable.pdf

# ShawPittman LLP

*A Limited Liability Partnership Including Professional Corporations*

SHELDON J. WEISEL  
202.663.8096  
sheldon.weisel@shawpittman.com

June 16, 2003

**By Electronic Mail and Hand Delivery**

Attn: Associate General Counsel (General Law)  
Department of Homeland Security  
Washington, DC 20528

**Re.: Comments on DHS Proposed "Procedures for Handling Critical Infrastructure Information," 68 Fed. Reg. 18524 (April 15, 2003)**

Dear Sir/Madam:

I am writing on behalf of The Real Estate Roundtable to provide comments on the Department of Homeland Security's proposed rule entitled "Procedures for Handling Critical Infrastructure Information," published at 68 Fed. Reg. 18524 (April 15, 2003). The Roundtable is a national organization that brings together leaders of the nation's top public and privately-held real estate ownership, development, lending, and management firms with the leaders of major national real estate trade associations to jointly address key national policy issues relating to real estate and the overall economy. Collectively, the members of The Roundtable hold portfolios containing over five billion square feet of developed property, including critical financial, telecommunications, transportation, and energy infrastructure.

The Roundtable's comments on the proposed regulations are enclosed with this letter. Please contact me if you have any questions or need additional information regarding this submission.

Sincerely,



Sheldon J. Weisel  
Counsel to The Real Estate Roundtable

Enclosure

cc: Roger Platt, Esq., The Roundtable

**COMMENTS OF THE REAL ESTATE ROUNDTABLE  
ON THE DEPARTMENT OF HOMELAND SECURITY  
PROPOSED PROCEDURES FOR HANDLING CRITICAL INFRASTRUCTURE  
INFORMATION, 6 C.F.R. PART 29**

**[68 Fed. Reg. 18524 (April 15, 2003)]**

**June 16, 2003**

## **I. INTRODUCTION**

The Real Estate Roundtable submits these comments on the Department of Homeland Security's (DHS) proposed "Procedures for Handling Critical Infrastructure Information," 6 C.F.R. part 29, published at 68 Fed. Reg. 18524 (April 15, 2003). The Roundtable is the organization that brings together leaders of the nation's top public and privately-held real estate ownership, development, lending, and management firms with the leaders of major national real estate trade associations to jointly address key national policy issues relating to real estate and the overall economy. Collectively, members of The Roundtable hold portfolios containing over five billion square feet of developed property valued at more than \$450 billion. Participating trade associations represent more than one million people involved in virtually every aspect of the real estate business.

The billions of square feet of office buildings, apartments, hotels, retail facilities, and other spaces that comprise the nation's real estate stock are among the most densely populated sites in the country. Clearly, this fact has not escaped those who wish to spread terror among the U.S. populace and inflict widespread economic damage. As the U.S. Attorney General warned in February, when the nation's terrorism alert system was first raised to Orange (high), "... al Qaeda leaders have emphasized planning for attacks on apartment buildings, hotels and other soft or lightly secured targets in the United States." As highlighted by the World Trade Center's destruction, large commercial buildings not only provide a physical setting where Americans converge, but they often house important national infrastructure – from telecommunications switching equipment to energy lines and water mains. Other buildings house critical financial infrastructure, such as our country's leading stock and community trading exchanges.

The Roundtable is, therefore, committed to advancing sound homeland security strategies in partnership with DHS. In the most concrete example of our efforts to help the industry better meet its growing responsibilities in this area, The Roundtable and federal homeland security officials in February announced the creation of a formal public-private partnership to help protect U.S. real estate assets against potential terrorist attacks. The partnership is supported by the Real Estate Information Sharing and Analysis Center (RE-ISAC), which was initially organized by The Roundtable. It is now supported by 10 major real estate trade associations. The RE-ISAC will facilitate information sharing with the DHS. The proposed CII regulations are, therefore, directly relevant to the success of these efforts and will directly affect the members of The Roundtable.

## **II. PROPOSED PROCEDURES FOR HANDLING CRITICAL INFRASTRUCTURE INFORMATION**

DHS is proposing procedures for the handling of Critical Infrastructure Information (CII) by DHS and other federal agencies and (through express agreement) by state, local, and foreign governments under authority of the Homeland Security Act of 2002 (Pub. L. 107-296). As a whole, The Roundtable is pleased with the proposed regulations being considered by DHS. For

the most part, the proposal appears to create uniform procedures for the receipt, acknowledgement, storage, and disposal of CII.

However, the proposed regulations could be improved in several ways to make the procedures for acknowledging, handling, and using CII more consistent and to make outcomes more predictable after information is submitted to DHS. Our review of the rule language has also identified some drafting inconsistencies in the proposed language, which The Roundtable would like DHS to correct in the final rule. With the changes we suggest below, we believe the regulations will provide greater predictability in anticipating how the part 29 procedures will be interpreted and applied.

**(1) *Advance Determinations for Categories of CII.*** The proposed regulations provide that only information that is voluntarily submitted for use in protecting critical infrastructure or other security or informational purposes may qualify as Protected CII, and only when properly marked by the submitter. There are types of information that almost certainly would qualify as Protected CII (e.g., incident reports); however, it is less clear for other types of information (e.g., information provided by a submitter in support of a CII claim) whether they would qualify as Protected CII. This uncertainty will tend to discourage individuals from submitting information that may be important for use by DHS and federal agencies in protecting critical infrastructure if, for example, the information reveals sensitive information about the individual's business. Because it may be difficult for DHS to anticipate the types of information that may be submitted by individuals seeking protection as CII, the regulations should contain procedures by which DHS will make (and publish) advance determinations that certain categories of information generally qualify as Protected CII. Information that falls within these categories should then be presumed to be Protected CII unless the information was not marked as required by § 29.5(b)(3).<sup>1</sup> These category determinations would help ensure that similar information would receive similar treatment, thus improving predictability and encouraging the submission of critical information to DHS. Other federal agencies, such as the U.S. Environmental Protection Agency (EPA), have confidential business information regulations that contain procedures for advance category determinations, which could be used as a model. *See, e.g.,* 40 C.F.R. § 2.207.

**(2) *Procedures for Submitting Information Supporting a CII Claim and Protection of Such Information.*** Under the proposed regulations, when information is received by DHS, the CII Officer would make a preliminary determination whether the information qualifies as Protected CII. In the event the CII Officer makes a preliminary determination that the information does not qualify as Protected CII, § 29.6(e)(1)(i) would require the CII Officer to send a notice to the submitter requesting that more information be submitted within 30 days to support the CII claim. These procedures should be improved to allow an extension of time to provide comments upon a showing by the submitter that more time is necessary to provide the necessary information. Extensions of time should be freely granted because no other party is likely to be prejudiced by the extension (e.g., it is very unlikely that there will be a pending request under the Freedom of Information Act, 5 U.S.C. § 552, (FOIA) at this time). In addition,

---

<sup>1</sup> This would be a broader presumption of protection than provided in § 29.6(b), which only applies to information submitted in accordance with the CII procedures *until* the CII Program Manager renders a final decision on whether the information is Protected CII.

for clarification, the regulation should provide that all comments and supporting information provided by the submitter are themselves Protected CII, as long as the comments are marked as required by § 29.5(b)(3). Last, in the event DHS does not receive a response after sending the § 29.6(e)(1)(i) notice, the CII Officer should be required to attempt to verify that the submitter received the initial notice. If the submitter did not receive the notice, or if DHS did not receive the response, because it was lost in transmission, additional time should be provided for the submitter to provide the information. *See, e.g.,* EPA's confidential business information regulations at 40 C.F.R. § 2.205(b)(4).

**(3) Return of Information to the Submitter or Protection of Information Maintained by DHS for Law Enforcement or National Security Reasons.** In the event the CII Program Manager makes a final determination that information does not qualify as Protected CII, § 29.6(e)(1)(ii) would require the CII Program Manager to follow the submitter's stated preference (if available) of either maintaining the information without protection as CII or disposing of it in accordance with the Federal Records Act. This provision (with a conforming change to § 29.6(e)(1)(i)(D)) should allow the submitter to elect that the information be returned if the CII Program Manager makes a final decision that it is not Protected CII. Allowing the submitter to request that the information be returned would provide greater confidence that the information was managed in accordance with the part 29 procedures and would not add a substantial burden for DHS. In the event that the submitter could not be contacted or if a response was not received by DHS, § 29.6(e)(1)(ii) provides that the CII Program Manager may dispose of the information or keep it if s/he determines that the information is necessary for law enforcement or national security reasons. In the event DHS keeps the information, the rule should *require* DHS to treat the information as Protected CII.

**(4) Appeal of CII Determinations.** As proposed, the regulations do not contain procedures for the appeal or reconsideration of final CII determinations by the CII Program Manager. At a minimum, an administrative appeal process should be provided if DHS maintains § 29.6(e)(1)(ii) as proposed, which includes the option of maintaining information without protection from disclosure for law enforcement or national security reasons. In such circumstances, the regulations should permit the submitter to appeal an adverse final determination to an administrative office within DHS (*e.g.,* the legal office) and provide that DHS shall maintain the disputed information as Protected CII (under § 29.6(b)) until resolution of the appeal.

**(5) Disclosure of Information by DHS and Other Federal Agencies.** Section 29.5(d)(2) states that a federal agency or other component of DHS "may not disseminate, distribute, or make public the information *until* the CII Program Manager has notified the agency or component that the [CII] Program Manager has acknowledged and validated the information." (Emphasis added) This sentence implies that the agency or DHS component may disclose the information after the CII Program Manager has acknowledged and validated the information, which is contrary to the restrictions on disclosure in §§ 29.6 and 29.7. This provision could be eliminated entirely because it is essentially redundant of the requirement that information submitted under a CII claim be presumed to be Protected CII (and, thus, subject to the protections of § 29.7) until a determination otherwise is made by the CII Program Manager. In the alternative, the sentence could be corrected by stating that the agency or DHS component "may not disseminate, distribute, or make public the information *unless and until* the CII

Program Manager has notified the agency or component that the CII Program Manager has *made a final determination that the information is not Protected CII, the time for appeal of the CII Program Manager's decision has passed without action by the submitter, and that the submitter has not requested that the information be returned or disposed of in accordance with the Federal Records Act.*"

**(6) Notice and Participation in FOIA Matters.** Proposed § 29.8(g) provides that Protected CII is exempt from disclosure pursuant to a request under FOIA, 5 U.S.C. § 552; and, if the Protected CII has been provided to a State or Local Government, it is protected from disclosure under State and local laws. However, the proposed regulations do not address defense against a FOIA or State or local FOI suit in the event of a challenge regarding the Protected CII. The rule should state that in the event DHS or a State or Local Government agency is sued for disclosure of Protected CII, DHS or the State or Local Government agency must notify the submitter that the FOI suit has been filed and give the submitter the right to participate in the defense of the FOI suit. Participation by the submitter in such actions is important because DHS or the State or Local Government agency often will not have the information necessary fully to defend the FOIA suit. Other federal agencies have regulations that contain procedures for defense of FOIA actions, which could be used as a model. *See, e.g.,* EPA's confidential business information regulations at 40 C.F.R. § 2.214.

**(7) Rule Language Comments.** Our review of the rule language has identified some potential drafting errors, inconsistencies, or oversights in the proposed regulations. The following list identifies these potential issues, but does not attempt to identify each instance where the language appears in the proposal.

- The regulation contains inconsistent language as to which federal agencies the information must be submitted in order to qualify as Protected CII. For example, the definitions of "Protected CII" (§ 29.2(f)) and "Voluntary" (§ 29.2(j)) state that Protected CII is CII that is voluntarily submitted "to DHS," while § 29.5 provides that CII may be submitted either to the "DHS IAIP Directorate" or to "another federal agency" with a direction that the information be submitted to the DHS IAIP Directorate. Section 29.5(c) adds that CII must be submitted to the "CII Program Manager" to qualify as Protected CII. We note that the definition of "Submission to DHS" appears to be an effort to address this issue; however, the defined term does not appear in the critical provisions under § 29.5. We suggest that these provisions be corrected to state that CII submitted to "DHS or to another federal agency with direction to provide the information to DHS" qualifies as Protected CII.
- The regulation appears inconsistent in specifying the markings that must be placed on information in order for it to qualify as Protected CII. These provisions are critical, given the importance of complying with the marking requirements of the rule. Section 29.5(d)(1)(i)-(ii) provides that the CII must be marked "Protected CII," while § 29.5(b)(3)(i) requires a marking substantially similar to "This information is voluntarily submitted to the Federal Government in expectation of disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002." Section 29.8(d)(1) provides that the CII provided to State and Local Governments

must be marked “Protected Critical Infrastructure Information.” We recommend that these provisions be reconciled, and that the rule only require that information must be “marked with the words ‘Critical Infrastructure Information,’ ‘Protected Critical Infrastructure Information,’ ‘CII,’ ‘Protected CII,’ or substantially similar language.”

- Section 29.7(e) specifies that Protected CII shall only be transmitted by U.S. first class, express, certified, or registered mail, or through secure electronic means. However, Protected CII may include oral communications, which cannot be transmitted by any of those means. While CII submitted orally to DHS or another agency must be followed by a written statement within 15 days, it is possible, even likely, that the information provided orally will need to be shared with other agencies or State and local law enforcement before the written information is provided. This provision should be amended to allow transmission of oral Protected CII by any method that prevents unauthorized disclosure.
- Section 29.8(i) provides that Protected CII may not be used in any civil action without written consent by the submitter “if such information is submitted in good faith for homeland security reasons.” This qualifying language appears unnecessary because information cannot qualify as Protected CII if (among other requirements) it is not related to homeland security and submitted in good faith compliance with the part 29 procedures. *See* §§ 29.2(b), 29.6(f). The language should be deleted because it could be read to add an ambiguous threshold determination that would have to be addressed by DHS or submitters in preventing the use of Protected CII in civil actions.
- Section 29.9(a) requires “all persons authorized to have access to Protected CII” to report suspected violations of the part 29 procedures. This reporting obligation should apply to all DHS officers, employees, contractors, and subcontractors (regardless of whether they are authorized to have access to the Protected CII), and to all other persons who are authorized to have access to the Protected CII.
- Certain defined terms (*e.g.*, Local Government, Submission to DHS) appear inconsistently capitalized, which could lead to potential confusion and inconsistency when interpreting the regulations. We suggest that defined terms be capitalized consistently in order to minimize this concern and to put the reader on notice that the term is defined in the rule.



Feel free to contact any of the following individuals if you have questions or need additional information regarding these comments:

Roger Platt  
Senior Vice President and Counsel  
The Real Estate Roundtable  
202.639.8400

Sheldon J. Weisel  
Shaw Pittman LLP  
202.663.8096

Jeffrey A. Knight  
Shaw Pittman LLP  
202.663.9152