

6/19

# Piper Rudnick

1200 Nineteenth Street, N.W.  
Washington, D.C. 20036-2412  
main 202.861.3900 fax 202.223.2085

JAMES J. HALPERT  
jim.halpert@piperudnick.com  
direct 202.861.3938 fax 202.223.2085

## Facsimile

Date: June 17, 2003

To:	Phone:	Fax:
Baruck Weiss, Esq. Department of Homeland Security	202-786-0249	202-772-9735

Original ☐ will / ☒ will not follow.

Pages (including fax sheet):

Comments:

2127/306489-1

*The information contained in this facsimile message is confidential and, if addressed to our client or certain counsel, is subject to the attorney-client or work product privilege. This message is intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and return the original message to us at the above address via the U. S. Postal Service.*

Piper Rudnick LLP • In Illinois, Piper Rudnick, an Illinois General Partnership



June 16, 2003

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

Re: Procedures for Handling Critical Infrastructure Information 6 C.F.R. Part 29,  
(RIN 1601-AA14)

Dear Sir or Madam:

Attached to this letter, please find the electronic filing of the Internet Commerce  
Coalition (ICC) in this proceeding.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read "James J. Halpert". The signature is stylized with a large, sweeping "H" and "A".

James J. Halpert, General Counsel  
1200 19<sup>th</sup> Street, N.W.  
Washington, DC 20036  
(202) 861-3938



Before the  
United States  
Department of Homeland Security

(RIN 1601-AA14)

Notice of Proposed Rulemaking  
Procedures for Handling Critical Infrastructure Information  
6 C.F.R. Part 29

**COMMENTS OF THE INTERNET COMMERCE COALITION**

June 16, 2003

The Internet Commerce Coalition (ICC) appreciates the opportunity to respond to the Department of Homeland Security's (DHS') Notice of Proposed Rulemaking in this proceeding issued on April 15, 2003 (68 Fed. Reg. 18524-29) to implement Section 214, Title II of the Homeland Security Act of 2002 ("the Act"), P.L. 107-296.

**I. INTRODUCTION AND SUMMARY**

The ICC's members, AT&T, AOL Time Warner, BellSouth, Cable & Wireless, eBay, MCI, SBC, Verizon, USTA, CompTel and ITAA, are leading Internet companies and Internet trade associations, who have a vital stake in cyber-security and protection of our nation's critical infrastructure. They have made major investments in repeated upgrades in network security, participate actively in industry and government-industry *forums* on network security, and want to share critical infrastructure information with the federal government in order to enhance preparedness against attacks against communications networks.

Protecting the confidentiality of voluntarily submitted information regarding threats, vulnerabilities and planned remedial measures is essential for our members to work with the government in an open and cooperative way to enhance network security. For this reason, we supported passage of Section 214 of the Homeland Security Act, and commend the Department on its carefully considered NPRM and its strong proposal to protect the confidentiality of voluntarily submitted critical infrastructure information ("CII").

The remainder of these comments suggests several refinements to the proposed rule that are fully consistent with the intent of Section 214, and would improve incentives to voluntarily submit critical infrastructure information to the federal government in several significant ways:

- providing clearer protection of CII that DHS provides to foreign governments, state and local governments, and to government contractors;
- clarifying the procedures relating to treatment by federal agencies of CII that is submitted indirectly through them to DHS;
- clarifying that notes of oral communications of CII are covered the Final Rules; and
- providing for notice to the submitting party of a determination that CII was not submitted in good faith.

## II. SUGGESTED CLARIFICATIONS OF THE PROPOSED RULE

### A. Disclosure of CII (§ 29.8)

#### 1. Disclosures to Foreign Governments

The ICC is particularly concerned about the dearth of protections in § 29.8(j) regarding provision of CII to foreign governments. First, we note that 6 U.S.C. § 133(a)(1)(D) contains no exemption for, or authority for, disclosures to foreign governments, and that the exemption is on tenuous legal ground. We understand that there may be situations in which it is imperative as a matter of policy that DHS share CII with foreign governments. However, this does not obviate

the need for clear safeguards for these disclosures, if they are to occur, to protect the identity of the submitter, as well as all information that relates specifically to the submitter, or that is proprietary or business-sensitive, and to provide notice to the submitter of any information disclosed.

In many cases, foreign governments that own the competitors of U.S. Internet and telecommunications companies could be interested in using CII relating to U.S. competitors to their commercial advantage. This clarification is essential if companies that own and operate networks are to voluntarily provide CII without fear that the information will identify them and be used against them by their foreign competitors.

Recommendations:

1. In order to provide clear guidance to DHS employees regarding disclosures to foreign governments, amend § 29.8(j) so that it expressly repeats the redaction safeguards in the second sentence of § 29.8(e), but applies them to the CII Program Manager. Subsection 29.8(j) should be amended at the end of the subsection as follows: "Before disclosing Protected CII to a Foreign Government, the CII Program Manager shall protect from disclosure the source of the Protected CII, any information that is proprietary, business-sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriate for disclosure to a Foreign Government. The CII Program Manager or his designee shall also provide notice to the submitter of the CII that was disclosed and the Foreign Government to which it was disclosed."
2. As in § 29.8(b)'s restrictions regarding disclosures to state and local governments, DHS should condition disclosure on compliance with the restrictions on further use or disclosure as set forth in § 29.8(d)(2) and (d)(3).

3. In order to protect against disclosures of CII for criminal investigations and prosecutions for conduct that is lawful under U.S. law, amend the final clause of § 29.8(j) to require that the investigation or prosecution be "of a criminal act in violation of the laws of the United States or any state."

## 2. Disclosures to State or Local Governments

The ICC commends DHS for clearly preempting, in § 29.8(g)(1), state FOIA laws in the case of CII that DHS discloses to state governments and for providing, in § 29.8(b), for an express agreement by state or local government officials regarding the restrictions imposed upon their use of CII by 6 U.S.C. § 133(a)(1)(E). However, we are concerned that § 29.8(b) does not mention or cross-reference those requirements clearly enough and, as a result, may cause confusion, particularly among state and local authorities who receive CII from DHS. We are also concerned that there is no sanction for violations by either State or local governments or their contractors.

### Recommendations:

1. To provide clearer guidance regarding the obligations of state and local governments regarding CII, amend the final sentence of § 29.8 so that it reads as follows: "Protected CII may be made available to a State or local government entity only if such entity pursuant to its enters an express agreement with the Program Manager to comply with the requirements of § 29.8(d) that acknowledges the understanding and responsibilities of the recipient."

2. Amend § 29.8(d)(4) to provide for some sanction for violation of the responsibilities of § 29.8(d), such as barring all further disclosures of Protected CII that will be available to a State or local government contractor who has violated § 29.8(b), and providing that any State or local

government agency that violates § 29.8 may receive Protected CII only with the written consent of the submitting person or entity.

### 3. Disclosure to Federal Contractors

The ICC is not convinced that disclosure of Protected CII to federal contractors is necessary, but should DHS believe that this exception is necessary, we urge that contractors be bound by protections similar to those for contractors' access to classified information. In general, we support the regarding proposed safeguards, in § 29.8(c), governing *disclosure* of CII by DHS contractors. However, the proposed regulations do not require that DHS contracts bind contractors to comply with § 29.7, just as contractors are currently required to respect classified data. Furthermore, the safeguards in § 29.8(c) do not restrict the use of CII obtained by government contractors for any purpose other than fulfilling their contract. This is in sharp contrast to § 29.8(d)(3), which expressly restricts re-use by state and local governments.

#### Recommendations:

1. Amend § 29.8(c) to require Federal contractors to comply with § 29.7. The first sentence of § 29.8(c) should be amended to as follows: "(c) Disclosure of Protected CII to Federal contractors may be made only after a CII Officer certifies that the contractor is performing services in support in support of the purposes of DHS, and has agreed by contract to comply with all the requirements of § 29.7."

2. Amend the final sentence of § 29.8(c) as follows: "Contractors shall not further disclose Protected CII to any of their components, employees, or other contractors (including subcontractors) without the prior written approval of a CII Officer unless such disclosure is

expressly authorized in writing by the submitter, and may not use Protected CII for any purpose other than fulfilling the terms of their contract."

#### **B. Indirect Submission Of CII (§ 29.5)**

The ICC supports DHS' proposal to provide for protection of CII submitted indirectly through another federal agency. This interpretation is fully consistent with the plain language of 6 U.S.C. § 133(a), promotes sound policy by encouraging submission of CII through other agencies that better understand the industries they regulate, and protects that information if it is provided with express direction to submit it to DHS.

However, the ICC is concerned that the procedures governing protection of CII submitted in this manner are not sufficiently clear. Subsections 29.5(c) and (d) do not clearly require other agencies to forward CII to DHS, nor do they specify a time within which agencies should forward CII to DHS. Furthermore, § 29.5(d)(2) is clearly intended to be helpful in this regard by stating that agencies forwarding CII may not disclose CII until the information has been acknowledged and validated by the CII program manager. However, it says nothing about whether the same protection applies in the event that an agency should fail to forward the CII to DHS, and it is phrased somewhat confusingly by suggesting that the information may be disclosed after submission, thus subverting the intent of the FOIA exemption.

#### **Recommendations:**

1. Amend § 29.5(c) to provide for mandatory and prompt submission of CII to DHS by receiving agencies within 7 days, or a similar period.
2. Amend § 29.5(d)(2) to state that "The Federal agency or DHS component forwarding the information to the CII Program Manager may not disseminate, distribute, or make public the



information only after the CII Program Manager has notified the agency or component that the Program Manager has acknowledged and validated the information, and then only subject to the provisions of § 29.8."

#### **C. Treatment of Orally Submitted CII (§ 29.5)**

The ICC supports the NPRM's proposal in § 29.5(b)(ii) to protect orally submitted CII if a written or otherwise tangible statement is submitted within 15 days of the oral submission. However, the current formulation does not clearly address the status of notes regarding submission of CII. This ambiguity may chill rapid oral submission of CII.

##### Recommendation:

1. Amend the definition of Critical Infrastructure Information in § 29.1(b) to cover notes of oral conversations.

#### **D. Determinations of Bad Faith Submission and Changes of Status (§ 29.6)**

The ICC agrees generally with the Department's proposal that bad faith submission of CII should result in lack of protection under the proposed rules. However, we disagree with the proposal in the first sentence of § 29.6(f) that there be no requirement to notify the submitter if the Program Manager determines that such information was not submitted in good faith. The submitting party should have an opportunity in the event of a clerical error or an erroneous decision of the merits to seek reconsideration of that determination, and should be notified that CII they intended to submit in good faith has been denied protected status.

##### Recommendation:

1. Amend § 29.6(f) in line 6 as follows "the Program Manager ~~is not required to shall~~ notify", and strike the last sentence of the subsection.

With regard to the change in status of CII, § 29.6(g) provides appropriate safeguards for changing status. However, the NPRM does not specifically provide for a process by which a submitting party may request removal of protection for CII that it has previously submitted because the information is no longer confidential. Such a provision may provide DHS with greater flexibility, and may be worth including in the Final Rule.

Recommendation:

1. Amend § 29.6(g) to add a new sentence at the end providing that a submitting party may submit a request to the CII Program Manager for withdrawal of Protected CII status for information that it has previously submitted.

### III. CONCLUSION

The ICC congratulates DHS on its NPRM and asks DHS to make all of the foregoing clarifications in the Final Rule to provide more effective, appropriately tailored incentives and safeguards for voluntary submission of CII as contemplated by Section 214 of the Homeland Security Act.

We thank you for considering our views.

Respectfully submitted,

*James J. Halpert*

James J. Halpert, General Counsel  
1200 19<sup>th</sup> Street, N.W.  
Washington, DC 20036  
(202) 861-3938