

Sprint.txt

Subject: Comments, RIN 1601-AA14  
Date: Mon, 16 Jun 2003 14:24:03 -0400  
From: "Jackson, Christine C [CC]" <Christine.C.Jackson@mail.sprint.com>  
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>  
CC: "Fingerhut, Mike B [CC]" <Michael.B.Fingerhut@mail.sprint.com>

Comments of Sprint Corporation.

<<RIN1601-AA14.pdf>>

Christine C. Jackson  
Phone - 202-585-1911  
Fax - 202-585-1897

RIN1601-AA14.pdf           Name: RIN1601-AA14.pdf  
                                  Type: Acrobat (application/pdf)  
                                  Encoding: base64  
                                  Description: RIN1601-AA14.pdf

**Before the  
DEPARTMENT OF HOMELAND SECURITY  
Washington D.C. 20528**

In the Matter of	)	
	)	
Procedures of Handling Critical	)	
Infrastructure Information	)	RIN 1601-AA14
	)	
Notice of Proposed Rulemaking	)	
_____	)	

**COMMENTS OF SPRINT CORPORATION**

Sprint Corporation (“Sprint”) hereby respectfully submits its comments on the above-captioned *Notice of Proposed Rulemaking (NPRM)* issued by the Department of Homeland Security (“DHS”) and published in the April 15, 2003 edition of the Federal Register. 68 F.R. 18524. The *NPRM* seeks to “establish[] 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.” 68 F.R. 18524.

Sprint believes that the DHS has done an excellent job in creating a regulatory structure for the protection of CII as contemplated by Section 214 of the Homeland Security Act. 6 U.S.C. §133. In fact, Sprint is concerned with only three of the proposed regulations and believes that its concerns can be easily accommodated without compromising the apparent purpose of those provisions.

First, under proposed Section 29.6(f), the CII Program Manager would not have to “notify the submitter” of what is claimed to be CII that “the information does not qualify as Protected CII” if the CII Program Manager “determines that any information is not submitted in

good faith [in] accordance with the CII Act of 2002 and these procedures.” Sprint agrees that Section 214 should not enable an entity to seek the protections afforded thereunder for information that clearly would not, under any reasonable set of circumstances, be viewed as “not customarily in the public domain and related to the security of critical infrastructure or protected systems.” 6 U.S.C. §131(3). Sprint also agrees that the CII Program Manager should not be burdened with evaluating such dubious submissions. Nonetheless, Sprint believes that even if the CII Program Manager finds that an entity is not acting in good faith by claiming that the information being submitted qualifies for protected status, the submitting entity should at the very least be afforded an opportunity to explain why it believes the information does qualify. Fundamental fairness and due process require that a party to an adverse administrative decision be given an explanation for the decision and an opportunity to explain why the decision is incorrect. Thus, Sprint recommends that Section 29.6(f) be modified to require the CII Program Manager to (1) inform the submitter of information of its determination that the information was not submitted in good faith; (2) afford the submitter a 10-day window to present additional evidence as to why the submission should be given CII protection; and (3) allow the submitter to withdraw the information it voluntarily submitted if the CII Program Manager still believes that the request for CII protection was not been made in good faith.

Second, Sprint believes that proposed Section 29.8(j) needs to be revised to clearly delineate the restrictions that will accompany the disclosure of critical infrastructure information to foreign governments. Section 29.8(j) authorizes the CII Program Manager to provide CII to foreign governments without the consent of the submitter but only “to the same extent it may provide advisories, alerts, and warnings to other governmental entities as described in §29.8(e) ... or in furtherance of an investigation or the prosecution of a criminal act.” By citing Section

29.8(e) here, Sprint interprets the provision as requiring the CII Program Manager to “protect from disclosure the source of any voluntarily submitted CII that forms the basis for the warning; and any information that is proprietary, business-sensitive, relates specifically to the submitting person or entity or is not appropriately in the public domain.” Section 29.8(e). However, to avoid any possible contrary interpretation, Sprint recommends that Section 29.8(j) be modified to include the Section 29.8(e) limitations on the type of information to be provided to foreign governments. Sprint further recommends that the CII Program Manager inform the submitting entity that its “scrubbed” critical infrastructure information is being furnished to foreign governments and provide the submitting entity the opportunity to review the information so as to ensure that no confidential information is being provided.<sup>1</sup>

Third, proposed Section 29.9 provides that for the reporting and investigation of “any possible violations of security procedures, the loss or misplacement of Protected CII and any unauthorized disclosure of Protected CII.” Subparagraph (c) of this provision states that “[i]f the CII Program Manager or the IAIP Security Officer determines that an unauthorized disclosure occurred or that Protected CII is missing, the CII Program Manager shall notify the submitter of the information.” The problem with this provision is that the CII Program Manager will only notify the submitter of the information after the investigation is complete and only if it is determined that an unauthorized disclosure of CII occurred or that CII is missing. Thus, the submitter of the information would be in the dark, possibly for several months as the

---

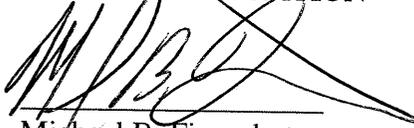
<sup>1</sup> Sprint assumes that since there is no comparable language in Section 29.8(e) authorizing the disclosure of CII, properly scrubbed, in connection with advisories alerts, warnings to relevant companies etc. without informing the entity submitting the information, the IAIP (Information Analysis Infrastructure Protection) Directorate will inform such entity of the disclosure. If Sprint’s assumption here is incorrect, Sprint recommends that this provision be modified to clarify that the submitting entity will be notified when its CII is being disclosed under this provision and that the entity will be given an the opportunity to review the information so as to ensure that no confidential information is being disclosed.

investigation proceeded, that its CII could be missing or had been wrongfully disclosed. Sprint believes that the CII Program Manager should notify the submitter of the information both that an investigation has begun as well as the outcome of the investigation. By providing such information to the entity submitting the information at the outset of the investigation, the submitting entity would be able to take temporary measures to protect its critical infrastructure on the assumption that the information was disclosed improperly while the investigation ensued.

With these three modifications, Sprint supports the adoption of the proposed rules.

Respectfully submitted,

SPRINT CORPORATION



Michael B. Fingerhut  
Richard Juhnke  
401 9<sup>th</sup> Street NW, Suite 400  
Washington, D.C. 20004  
(202) 585-1909

Its Attorneys

June 16, 2003