

Cellular Telecommunications and Internet Association.txt

Subject: Procedures for Handling Critical Infrastructure Information comments from CTIA

Date: Mon, 16 Jun 2003 16:40:18 -0400

From: "Christine Blomquist" <CBlomquist@ctia.org>

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

Please find attached a copy of the electronic comments filed by the Cellular Telecommunications & Internet Association (CTIA) to the Department of Homeland Security on the Procedures for Handling Critical Infrastructure Information.

<<030616 DHS Comments.pdf>>

	Name: 030616 DHS Comments.pdf
030616 DHS Comments.pdf	Type: Acrobat (application/pdf)
	Encoding: base64
	Description: 030616 DHS Comments.pdf

**Before the
Department of Homeland Security
Washington, D.C. 20528**

In the Matter of)	
)	
Procedures for Handling Critical)	RIN 1601-AA14
Infrastructure Information)	
)	
)	

**COMMENTS OF THE
CELLULAR TELECOMMUNICATIONS & INTERNET ASSOCIATION**

Michael F. Altschul
Senior Vice President, General Counsel

Kathryn Condello
Vice President, Industry Operations

Christopher Guttman-McCabe
Director for Regulatory Policy

**CELLULAR TELECOMMUNICATIONS
& INTERNET ASSOCIATION**

1250 Connecticut Ave., N.W.,
Suite 800
Washington, D.C. 20036
(202) 785-0081

Its Attorneys

Dated: June 16, 2003

**Before the
Department of Homeland Security
Washington, D.C. 20528**

In the Matter of)
)
Procedures for Handling Critical) RIN 1601-AA14
Infrastructure Information)

**COMMENTS OF THE CELLULAR
TELECOMMUNICATIONS & INTERNET ASSOCIATION**

The Cellular Telecommunications & Internet Association (“CTIA”)¹ hereby submits the following comments regarding the above-captioned *Notice of Proposed Rulemaking* (“NPRM”),² which examines uniform procedures for Federal agencies to implement Section 214 of the Homeland Security Act of 2002.³ CTIA supports the goal of protecting the “critical infrastructure” and reducing the “vulnerability of the United States to Acts of Terrorism,”⁴ and pursuant to that goal, CTIA believes there are elements of the NPRM that could be enhanced in order to reduce the vulnerability of our nation’s critical infrastructure.

¹ CTIA is the international organization of the wireless communications industry for both wireless carriers and manufacturers, and acts as one of four Coordinators within the Information & Telecommunications Critical Infrastructure Sector. Membership in the association covers all Commercial Mobile Radio Service (“CMRS”) providers and manufacturers, including cellular, broadband PCS, ESMR, as well as providers and manufacturers of wireless data services and products.

² *Procedures for Handling Critical Infrastructure Information*, Notice of Proposed Rulemaking, 68 Fed.Reg. 18524-29 (“NPRM”) (April 15, 2003).

³ Section 214, Title II, of the Homeland Security Act of 2002 (Pub.L. 107-296).

⁴ NPRM at 18524.

I. INTRODUCTION

One of the primary goals of the Department of Homeland Security (“Department”) is to protect critical infrastructure against further terrorist attacks.⁵ To do that, the Department must have critical infrastructure information on network architecture and topology, as well as potential and actual vulnerabilities. Section 214 of the Homeland Security Act of 2002 “provides for the establishment of a critical infrastructure protection program that protects from disclosure to the general public any critical infrastructure information which the public may voluntarily provide to the Department.”⁶ To facilitate its goal to protect critical infrastructure, any critical infrastructure protection program must be based on policies that engender trust and facilitate voluntary information sharing by private companies regarding critical infrastructure protection. This approach is key since more than 80% of the Nation’s critical infrastructure is privately held.

As the Department recognizes, “the receipt of information pertaining to the security of critical infrastructure . . . is best encouraged through the assurance that such information will be utilized for securing the United States and will not be disseminated to the general public.”⁷

Companies that submit information voluntarily must feel comfortable that they are not creating a security risk by allowing indiscriminate or unmanaged access to that information. CTIA believes that with the following modifications, the rules proposed in the NPRM will provide an improved level of comfort to those companies that choose to voluntarily submit information.

⁵ See http://www.dhs.gov/dhspublic/theme_home1.jsp

⁶ NPRM at 18525.

⁷ *Id.*

II. THE PROPOSED DEFINITION OF CRITICAL INFRASTRUCTURE INFORMATION MUST BE EXPANDED TO INCLUDE NETWORK INFORMATION AND TOPOLOGY

In order for the Department to fulfill its mandate regarding the protection of critical infrastructure, the definition of critical infrastructure information (“CII”) in Section 29.2 should be expanded to include information regarding the locations, mapping, configuration and/or topology of critical infrastructure networks. The location and configuration of these CI networks is the foundation upon which any risk or vulnerability assessments are conducted. It is extremely important that any such information, if submitted to the Department, be accorded the same protection as other data and information described in the NPRM. Companies that voluntarily submit data on confidential information regarding their networks (information that could be used for terrorist purposes, or possibly anticompetitive purposes) must feel secure that information will not be made public or be treated with less care than other CII.

III. THE DEPARTMENT SHOULD ACT AS A REPOSITORY FOR CRITICAL INFRASTRUCTURE INFORMATION.

The Department should act as a repository for critical infrastructure information. For the wireless industry, facing multiple Federal mandates including homeland security related requests resulting in significant capital and human resource expenditures, controlling the number of requests for critical information would be extraordinarily beneficial. On the Federal level alone, wireless carriers and manufacturers, as well as other critical infrastructure operations, are faced with a barrage of homeland security related requests. When extended to the regional, state, and local level, the number of requests is increasing exponentially. If left unchecked, the sheer number of requests will undoubtedly lead to a higher level of security risk.

While Section 29.3 of the NPRM states that “these procedures shall not be construed to limit or in any way affect the ability of Federal, State, or local Government entity, agency, or

authority, or any third party, under applicable law, to obtain information by means of a different law, regulation, rule, or other authority,”⁸ CTIA believes the Department should act as the nationwide gatekeeper, through which requests for CII should be directed. Once information is submitted to the Department, critical infrastructure companies should not also have to submit the same information to other areas of federal, state, or local government. Nor should these same companies be required to determine whether requests for CII outside of the Department are valid requests.

Rather, CTIA strongly urges that DHS, or its designated sector agents, be responsible for ensuring that requests for voluntary CII information are appropriate and that the measures designed to protect CII are in place. CTIA supports the proposal in the NPRM that “protected CII may be made available to a State or local government entity only pursuant to its express agreement with the Program Manager that acknowledges the understanding and responsibility of the recipient.”⁹ This will result in a three-fold benefit. First, precious resources of the critical infrastructure providers, both capital and human, will be saved. Second, if state, local or federal entities request the information from the Department, it will not lose the Freedom of Information Act protection proposed under this NPRM. Third, the proposal will provide some level of assurance that the recipients have instituted adequate controls to ensure the continued protection of such information.

⁸ NPRM at 18526.

⁹ NPRM at 18528.

IV. THE DEPARTMENT SHOULD FORMALLY DESIGNATE AT LEAST TWO AGENTS PER CRITICAL INFRASTRUCTURE SECTOR TO ACT AS THE RECIPIENTS OF CRITICAL INFRASTRUCTURE INFORMATION

While Section 29.5 of the NPRM states “the Secretary of Homeland Security shall designate the DHS IAIP Directorate as the sole entity authorized to acknowledge and validate the receipt of Protected CII,”¹⁰ CTIA believes that other entities should be designated as recipients of CII. Section 29.2 (i) of the proposed rules already suggests that 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. CTIA believes that the Department should specifically designate at least one Federal Agency (point of contact) for each sector as an official recipient of CII, and should additionally designate one non-Federal Agency Agent to act as a recipient of CII information. At a minimum, it is recommended that each critical infrastructure sectors’ Information Sharing and Analysis Center (ISAC), or possibly the ISAO as defined in Section 29.2 (d) of the NPRM, should receive such an agent designation.

The ISAC/ISAO mechanism, where instituted, is a logical alternative recipient for CII materials. ISACs, as encouraged by the President in his National Strategy for Homeland Security, already operate as a clearinghouse where members share information about vulnerabilities, threats, and incidents. These organizations are designated to gather, analyze, and disseminate information on vulnerabilities, as well as potential threats that are relevant to its members. The work of these groups should be built upon, and not duplicated by the Department.

¹⁰ NPRM at 18526.

V. ONCE INFORMATION IS SUBMITTED TO DHS, IT SHOULD BE PROTECTED AS CII AND ALSO PERMANENTLY IDENTIFIABLE AS CII

CTIA strongly supports the proposal in Section 29.6 of the NPRM that “all information submitted in accordance with the procedures set forth herein will be presumed to be treated as Protected CII from the time the information is received by a Federal agency or DHS component,”¹¹ or as recommended above, a DHS-designated sector agent. In addition, CTIA believes that the presumption of protection detailed in Section 29.6 of the NPRM should be extended to CII submitted to the Department in the interim before the rules are adopted.

CTIA believes that the tracking concept proposed in the NPRM should be extended to CII after it receives a final designation. The tracking number, or CII identification mark, should be provided to highlight information that has been recognized by DHS as critical. This will help to ensure that further external requests for this information are channeled through DHS, and to provide a means of sharing this information by the contributor with appropriate non-government recipients, including customers.

Additionally, there are two areas that are not in line with the rest of the NPRM with regard to “notice” to entities that submit information voluntarily. First, under proposed section 29.6 (f), the Critical Infrastructure Information (“CII”) Program Manager can make a determination that information was “not submitted in good faith [in] accordance with the CII Act of 2002 and these [proposed] procedures,” but does not have to notify the submitter of this determination. Second, pursuant to Section 29.6 (e)(ii) of the NPRM, under certain circumstances the Program Manager has the authority to keep information that has not received a

¹¹ NPRM at 18527.

CII designation if “there is a need to retain it for law enforcement and/or national security reasons.”¹²

There are multiple problems with these exceptions. Under section 29.6 (f), there is no standard by which a determination of “bad faith” is made, and no notification of that determination is required. At the very least, any determination of “bad faith” should result in a notification of that determination, pursuant to section 29.6 (e), to the submitting party. This will give potential submitters confidence that information submitted is to be reviewed and not summarily dismissed without notification. Under Section 29.6 (e)(ii), if the Program Manager decides to keep the submitted information for “national security reasons,” then it stands to reason that such information is indeed CII and should be treated accordingly. Perhaps more importantly, the two exceptions detailed above, even if only occurring in rare cases, are contrary to the spirit of cooperation that is necessary in order for information to be submitted voluntarily. Even a small possibility that voluntarily submitted CII could be made public, or left unprotected, will dissuade critical infrastructure owners and operators from making voluntary submissions. As a result, the Department will not get all the information it needs, including information it may specifically request.

Finally, regarding the Department’s disclosure of information, possibly to the general public, Section 29.8 (e) states that “in issuing a warning, the IAIP Directorate shall 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 otherwise not appropriately in the public domain.”¹³ While CTIA agrees that the Department should make every effort to protect the identities of parties that submit

¹² NPRM at 18527.

¹³ NPRM at 18528.

information voluntarily, CTIA also believes that before any such information is released to the public, the company submitting the information should be notified of the impending disclosure. Submitting parties should be made aware of the substance of the warning as well as the mechanism by which it will be delivered.

Disclosure of this information should be well understood by all parties involved, and should be treated as consistently as possible across all sectors. The process, which could have significant economic impact in the instance of wrongly-issued warnings, should be subject to separate notice and comment to ensure that a balanced and thought out process is incorporated into each of the sector's ISAC efforts, as well as at the Department of Homeland Security.

VI. CONCLUSION

For the foregoing reasons, the NPRM should be amended as detailed above before formal rules are adopted.

Respectfully submitted,

/s/ Michael Altschul

**CELLULAR TELECOMMUNICATIONS
& INTERNET ASSOCIATION**

1250 Connecticut Ave., N.W., Suite 800
Washington, D.C. 20036
(202) 785-0081

Michael F. Altschul
Senior Vice President & General Counsel

Kathryn Condello
Vice President, Industry Operations

Christopher Guttman-McCabe
Director for Regulatory Policy

Its Attorneys

Dated: June 16, 2003

CERTIFICATE OF SERVICE

I, Christine Blomquist, hereby certify that a copy of the foregoing “Comments of the Cellular Telecommunications & Internet Association” was sent on this 16th day of June 2003 by electronic mail and via first class U.S. mail, postage prepaid, to the following:

Associate General Counsel (General Law)
Department of Homeland Security
Washington, DC 20528
e-mail: cii.regcomments@dhs.gov

/s/ Christine Blomquist
Christine Blomquist