

MCI.txt

Subject: Comments of MCI
Date: Mon, 16 Jun 2003 16:11:58 -0400
From: "Cristin Flynn" <Cristin.Flynn@mci.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>
CC: "Rick Whitt" <Richard.Whitt@mci.com>

Attached are the Comments of MCI, also known as worldCom, Inc., in response to the Department's Notice of Proposed Rulemaking regarding proposed rules for the protection of critical infrastructure information.

Please do not hesitate to contact me if there are any questions.

Thanks very much,

Cristin

Cristin L. Flynn
Counsel
Internet Law & Policy
MCI (WorldCom, Inc.)
(202)736-6450
(202)736-6460 (fax)

CII NPRM Final.doc Name: CII NPRM Final.doc
 Type: WINWORD File (application/msword)
 Encoding: base64
 Description: CII NPRM Final.doc



**Before the
The Department of Homeland Security Notice of Proposed Rulemaking**

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

June 16, 2002

Comments of MCI

MCI (MCI), also known as WorldCom, Inc., files its comments in response to the Department of Homeland Security (DHS) Notice of Proposed Rulemaking (NPRM) to establish procedures for handling critical infrastructure information (CII).¹ DHS seeks to create processes for federal agencies to implement the Critical Infrastructure Information Act of 2002, also known as section 214 of the Homeland Security Act of 2002. MCI supports generally the processes and procedures set forth in the NPRM, and respectfully requests several limited clarifications of scope to promote clarity and consistency of enforcement.

INTRODUCTION

MCI recognizes the importance of information sharing and the role it plays in protecting the critical infrastructure of the United States. As the largest IP network operator in the world, MCI is a leader in both physical and cyber-security to protect its networks, and the services it provides to its customers. MCI is a longstanding and active participant in the National Communications System's National Coordinating Center for telecommunications crisis coordination and response. Additionally, MCI is the only

¹ Department of Homeland Security, Notice of Proposed Rulemaking, Procedures for Handling Critical Infrastructure Information, 6 CFR Part 29 (April 15, 2003) at (I) (hereinafter, CIIA NPRM).



telecommunications company with an operations team qualified to enter into hazardous situations to restore services.²

MCI's UUNET cyber-security teams are also industry leaders in information sharing and promoting critical infrastructure protection. Recently, MCI was awarded two key Information Security Leadership Awards in the Internet Service Provider (ISP) category by the SANS Institute.³ MCI shared information on how to mitigate those attacks with the ISP community and the Federal Government, and continues to lead the industry to increase security baselines for network security.

I. The Critical Infrastructure Information Act

MCI strongly supports the goal of the Critical Infrastructure Information Act (CIIA, or the Act), that seeks to encourage the owners and operators of our nation's critical infrastructure to share information about potential threats, vulnerabilities, or national-security level infrastructure concerns with the federal government. As will be set forth more fully below, MCI seeks several clarifications on the process in which certain aspects of critical information will be managed, but generally supports the process proposed by the Department of Homeland Security.

The term "critical infrastructure" is treated expansively, to encompass the broadest possible scope of information aimed at reducing potential or actual terrorist threats to the nation's infrastructure. MCI strongly supports the scope of the Act, aimed

² The MCI MERITSM team has been used to restore services in a US Postal Service sites contaminated by anthrax, as well as in response to a train tunnel chemical fire in Baltimore, MD and in downtown New York City following September 11.

³ MCI and its security team received the *Award for Leadership in Mitigating Denial of Service Attacks* for its proactive efforts in developing and sharing new and aggressive techniques to identify and block Distributed Denial of Service attacks (DDOS) against its customers. MCI also received the *Award for*



at "the protection of vital physical or computer-based systems and assets, collectively referred to as 'critical infrastructure,' the incapacitation or destruction of which would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of these matters."⁴

As recognized in the Act, any information about a critical infrastructure "that is voluntarily submitted to a covered Federal agency" shall be exempt from Freedom of Information Act requirements, as well as exempt from use in civil actions and certain other proceedings.⁵ These are very important protections, and are important and monumental steps towards establishing a trusted environment for information sharing. However, it is important to note that while procedures and processes are important and must be clear and unambiguous, it will be critical to provide a benefit back to the provider of the information in order to ensure that the channels remain open. Thus while the CIIA is an important step towards creating a trusted environment with which to share information with the Federal Government, it is not a complete elimination of all barriers to information sharing.

A. Obligation of "Good Faith" and the CIIA

The Department should give further consideration to use and application of the "good faith" requirement in Section 29.6(f). While MCI strongly supports the premise that CII submitted in good faith should be protected, the "good faith" obligation is missing from the Homeland Security Act itself. Section 29.6(f) states that "In the event

Leadership in Rapid Response to Worm Activity for its security team's quick and decisive work in decoding and halting the Code Red and SQL-Slammer worms.

⁴ CIIA NPRM at (I).

⁵ Homeland Security Act of 2002, Pub. L. 107-296, Critical Infrastructure Information Act of 2002 (CIIA), Title 2, subsection (b), at § 214.



that the CII Program Manager determines that any information is not submitted in good faith accordance with the CII Act of 2002 and these procedures, the Program Manager is not required to notify the submitter that the information does not qualify as protected CII."⁶ Ambiguity exists as to the context and interpretation of the term "good faith" as justification for submitting CII.

MCI raises two issues for further consideration. First, the Department should reconsider how a good faith analysis will be provided by the CII Program Manager, specifically when section 29.6(b) provides a "Presumption of Protection" for all information submitted in accordance with the Act's procedures. Absent a test or certification requirement to establish good faith, there is no procedure set forth either in the Act or in the NPRM for submitters of CII to establish that the data has, in fact, been submitted in good faith. Section 29.2(f), when setting forth the definition of "Protected Critical Infrastructure Information" does not include a "good faith obligation", which inserted, would need to be modified by the Department, as would sections 29.5(b)(1) and (b)(3).⁷

Moreover, a good faith declaration is not required in the transmittal language set forth in the "Express Statement" of Section 214(a)(2) of the Act, nor is it included in section 29.5 of the NPRM. Absent a clear and unambiguous process to establish good faith, MCI recommends that determinations of an absence of good faith should be left to the judicial system or an administrative judicial review that applies due process.

⁶ CIIA NPRM, § 29.6(f).



Second, if the Department retains a "good faith review" function as a part of the CII Program Manager's responsibilities, the Department should establish a process whereby the submitter of the CII is notified of the Program Manager's decision, and has the right to reclaim the information provided. At present, the current process is lacking such protection.

B. Changing status of CII to Non-CII

A clarification on the timing and triggering events that address when CII is deemed Non-CII would also strengthen section 29.6(g). As it currently reads, section 29.6(g) states, "Only the CII Program Manager or the Program Manager's designee may change the status of Protected CII to non-Protected CII and remove its Protected CII markings." It is not clear what circumstances would trigger the change, and whether the submitter of the information would be notified of the modification, and the right to reclaim the information. If a regular review process will be established to determine which CII has become public information, that process should be detailed in these procedures.

C. Authority to Receive Critical Infrastructure Information

MCI supports the designation of the DHS Information Analysis and Infrastructure Protection (IAIP) directorate as the appropriate sole recipient to acknowledge and receive critical infrastructure information.⁸ The proposed regulations permit CII to be provided directly to IAIP, or indirectly, to another Federal agency, which then submits the CII to IAIP, at the submitter's request.

⁷ Both these subsections set forth the scope and protection of CII, and reflect the language set forth in § 214(a)(2) of the Act.



MCI proposes that the regulations encourage that CII be sent to IAIP in the first instance, and then disseminate back to any other Federal agencies on an as-needed basis. The very premise of the CIIA is to provide a certain level of confidence to critical infrastructure operators that information provided to the Federal government will remain as confidential as possible in order to ensure adequate treatment of the potential threat or vulnerability. While there are instances in which Federal agencies may need to be the recipient of first instance, generally, the all agencies should support IAIP as the focal point for receipt and control of CII. Federal agencies should be encouraged to use the DHS IAIP process whenever possible, and should only accept CII as a secondary measure, and in very limited circumstances.

D. Sharing Information With Foreign Governments

In the limited circumstances in which a CII is to be provided to a foreign government in furtherance of an investigation or the prosecution of a criminal act, MCI respectfully requests that Section 29.8(j) be modified to provide notice to the submitter that such information is being shared. As presently constructed, no notice is required to the CII provider. However, once information is shared with a foreign government for an investigation or potential prosecution, there are no guarantees that the information will remain protected CII in that foreign country. In most instances, it is unlikely that the CII owner will receive the same or similar protections from the foreign jurisdiction as are available in the United States. Accordingly, if information will be provided to a foreign

⁸ CIIA NPRM, §29.5(a).



government in accordance with section 29.8(j), notice should be provided to the CII provider.

II. CONCLUSION

MCI supports the efforts of the Department of Homeland Security to develop clear and unambiguous procedures to implement the Critical Infrastructure Information Act. As was noted in the National Strategy to Secure Cyberspace, working to ensure the protection of our nation's critical infrastructure requires a strong "public private partnership." The procedures set forth are an important step towards cementing that partnership going forward, and MCI looks forward to working with the Department on these issues in the future.

Dated: June 16, 2003

Respectfully submitted,

S/ _____
Cristin L. Flynn
Counsel
Internet Law & Policy
MCI (a/k/a WorldCom, Inc.)
1133 19th Street NW
Washington DC, 20036
(202)736-6450