

United States Telecom Association.txt
Subject: Procedure for Handling Critical Structure Information
Date: Mon, 16 Jun 2003 16:24:44 -0400
From: "Meena Joshi" <mjoshi@usta.org>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>
CC: "Michael McMenamin" <mmcmenamin@usta.org>

Electronically filed herewith is the United States Association 's comments to the
Department of Homeland Security regarding its proposed rules.

Meena Joshi
Administrative Assistant
United States Telecom Association
1401 H Street, NW, Suite 600
Washington, D.C. 20005-2164
mjoshi@usta.org
P: (202) 326-7273
F: (202) 218-3540
www.usta.org

NOTE: This message, and any attachments, is intended only for the above--identified
recipient(s). The information contained herein may be privileged, confidential or
proprietary, and its use or disclosure by other than the intended
recipient(s) is prohibited and may be unlawful. If you have received this
electronic communication in error, kindly delete it without re-publication or
printing and notify me immediately.

03June16DHSCommentsfinal.doc

Name: 03June16DHSCommentsfinal.doc
Type: WINWORD File (application/msword)
Encoding: base64
Description: 03June16DHSCommentsfinal.doc



1401 H Street NW
Suite 600
Washington DC
20005-2164

Tel (202) 326-7244
Fax (202) 326-7333
wmccormick@usta.org
www.usta.org

June 16, 2003

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

Re: *Procedures for Handling Critical Infrastructure Information; Proposed Rule.*

The United States Telecom Association (USTA),¹ through the undersigned, hereby provides comments to the Department of Homeland Security's (DHS) *Procedures for Handling Critical Information; Proposed Rule* (Proposed Rules).² Pursuant to Executive Order 12866, the DHS now seeks comment on its proposed rules.

On May 22, 1998, the President signed Presidential Decision Directive 63 (PDD-63), Critical Infrastructure Protection, designed to defend the nation's critical infrastructure from physical and cyber intrusions. PDD-63 calls for a national effort to assure the security of the vulnerable and interconnected infrastructure of the United States (U.S.), most notably telecommunications. The foundation of PDD-63 stresses the critical importance of cooperation between the government and the private sector because the critical infrastructure of the U.S. is primarily owned and operated by the private sector.

President Bush on November 25, 2002, signed into law the Homeland Security Act, which created and provided the core responsibilities for DHS.³ Under section 214 of the Homeland Security Act, DHS must protect voluntarily shared critical infrastructure information (CII).⁴ Section 214 "provides for the establishment of a critical

¹ USTA is the Nation's oldest trade organization for the local exchange carrier industry. USTA's carrier members provide a full array of voice, data and video services over wireline and wireless networks.

² 68 Fed. Reg. 18,524 (to be codified at 6 C.F.R. Part 29)(proposed April 15, 2003)(Proposed Rules).

³ Homeland Security Act {Pub. L. 107-296}.

⁴ *Id.* at § 214, subtitle B of Title 2.

infrastructure protection program that protects from disclosure to the general public any critical infrastructure information which the public may voluntarily provide to the Department.”⁵ DHS’s proposed rules establish uniform procedures for the receipt, care and storage of CII for all Federal agencies that receive such information. The CII procedures apply to “United States Government contractors, to Foreign, State, and local governments, and to government authorities, pursuant to their express agreements.”⁶

Because of the critical role that local exchange carriers (LEC) play in the Nation's communications infrastructure, USTA member companies place an extremely high value on the security and reliability of their service, networks and facilities. Ensuring the security of USTA member networks is essential to safeguarding the U.S. and provides the impetus for USTA to comment in this proceeding.

In the past, USTA members have been reluctant to provide information related to CII for fear that such information would not be protected from release under the Freedom of Information Act (FOIA)⁷ or similar state laws. Under FOIA, Federal government agencies are required to make their records available upon request. A Federal agency may withhold requested information if such information meets one of nine exceptions including: classified national defense or foreign relations information, internal agency rules or practices, information prohibited from disclosure by another Federal law, trade secrets or confidential business information, legally protected inter-and intra-agency communications, and certain law enforcement-related information. The agency whose records are being requested bears the burden of proving that any records are exempt from disclosure. Information that may be withheld under FOIA may be disclosed by an agency as a matter of administrative discretion, if not explicitly prohibited by law, and if the agency determines such disclosure would not cause foreseeable harm. USTA member companies have had serious trepidations about making their CII available to Federal agencies because they were not assured that their CII fell under one of the nine exceptions or that guidelines were not in place that would set the proper parameters for agency discretion to release CII.

USTA contends that, for the most part, all telecommunications network (including both voice and data) vulnerability information, and sensitive outage and intrusion information that have been provided to the Federal government should not be disclosed. USTA recognizes that cooperation between the governmental national security/emergency preparedness entities and private networks is necessary to promote security in the information and communications sector. Section 214 of the Homeland Security Act was enacted to address the FOIA issues and the sensitivity that CII providers have to disclosure of such information. Likewise, USTA praises DHS for putting forth rules that will eventually add substance to section 214 of the Homeland Security Act. USTA now provides comments in regards to DHS’s proposed rules.

⁵ Proposed Rules at 68 Fed. Reg. 18,524.

⁶ *Id.*

⁷ 5 U.S.C. § 552.

IAIP Coordination of CII with OGC

Pursuant to section 29.4 of the proposed rules,⁸ the Under Secretary of the Information Analysis Infrastructure Protection (IAIP) Directorate is the senior official within DHS who is responsible for directing the CII program. The Under Secretary for IAIP is charged with the authority to appoint the CII Program Manager to “direct and administer the CII program.” Likewise, the CII Program Manager has the authority to appoint one or more CII Officers to provide “proper management and oversight” of CII.

USTA agrees that the designation of a CII Program Manager or Officer in the proposed rules within the IAIP Directorate is correct. USTA, however, believes that the IAIP Directorate should coordinate with DHS’s Office of General Counsel (OGC) in regards to classification and dissemination of CII. The determinations that the Under Secretary, Program Manager or Officer of IAIP will make in regards to FOIA and information sharing are not always going to be routine in nature and will likely require interpretation of the law. For this reason, USTA requests that the proposed rules be amended to require the Under Secretary, Program Manager, and Officer of IAIP to coordinate with DHS’s OGC [when classifying and disseminating CII](#).

Disclosure of Information to Federal Contractors

Under the proposed section 29.8 (c):⁹

Disclosure of protected CII to Federal contractors may be made after a CII Officer certifies that the contractor is performing services in support of the purposes of DHS. The contractor shall safeguard Protected CII in accordance with these procedures. Contractors shall not further disclose Protected CII to any of their components, employees, or other contractors (including subcontractors) without prior written approval of a CII Officer unless such disclosure is expressly authorized in writing by the submitter.

At the outset, USTA notes that contractors are not explicitly provided for under section 214 of the Homeland Security Act. USTA, however, appreciates DHS’s inclusion of contractors within its proposed disclosure of information rules. Given the sensitivity of the information that CII providers will be presenting DHS, USTA contends that DHS must ensure that contractors possess the same requisite security clearances that Federal government employees will have in fulfilling their duties and responsibilities in handling CII. DHS must also ensure that a contractor have the requisite security clearance prior to sharing CII.

⁸ See Proposed Rules § 29.4, 68 Fed. Reg. 18,526.

⁹ *Id.* at § 29.8, 68 Fed. Reg. 18,528.

USTA believes that DHS should limit the number of contractors who have access to CII because of the inherent sensitivity of the information that LECs will be providing, *e.g.* maps and locations of central offices. In addition, section 29.9 of the proposed rules does not provide criminal or administrative penalties for contractors, or state and local government officials who provide unauthorized disclosure of CII.¹⁰ Providing for specific criminal and civil penalties for unauthorized disclosure of CII is a critical deterrent for unlawful behavior. Thus, protecting, limiting dissemination, and deterrence from unlawful disclosure of CII by contractors are key concepts that DHS needs to take into further account when finalizing its proposed rules.

Responding to FOIA Requests or State and Local Access Laws

In the post September 11, 2001 era, USTA member companies have encountered a flurry of state-by-state, municipality-by-municipality, county-by-county inquiries and mandates on private sector infrastructure owners. These mandates on USTA member companies have become unsustainable, and if left uncoordinated will lead to grossly inefficient and idiosyncratic security programs. USTA member companies are diverting valuable resources in order to respond to state, municipal, and county inquiries instead of investing in security programs. Thus, USTA contends that there is a compelling argument for Federal leadership and partnership with states, municipalities and counties in the formation of regularized inquiries to avoid inefficient duplication by multiple governmental entities. However, this should not be interpreted as a call for Federalization of security, but rather, should be viewed as a call for coordination among Federal, State and local municipalities in regards to assembling information necessary to protect CII within DHS.

The nature of our Federal system apportions responsibility among Federal, State and local authorities'. Like many other service providers, USTA members are regulated at all three levels, and the task of responding to requests for information is placing an increasing burden on their resources. In addition, USTA member companies realize the importance of providing consistent information to all levels of government yet without better coordination at the Federal level, our member companies fear they will be tasked with duplicative and conflicting requests for information. Thus, USTA proposes that DHS be the primary repository and clearing house for all CII information for Federal, State and local governments.

USTA contends that regardless of what governmental entity or authority seeks CII, LECs should submit their CII only to DHS. The Federal law now provides DHS with the requisite authority to exempt CII from Federal FOIA disclosure. USTA believes that most state and local governments have FOIA laws or information access laws that are not as stringent or broad enough to protect LEC CII, which is most troubling to USTA members. In addition, by having DHS as the main repository and clearing house

¹⁰ *Id.* at § 29.9, 68 Fed. Reg. 18,529.

for CII, Federal, State and local governments will not have to make duplicative requests to LECs to provide information that is already being held by DHS. USTA believes that the administrative burden placed on LECs to provide duplicative information can be averted simply by having Federal, State, and local governments obtain the CII they require from DHS. DHS can then disseminate the information under the Federal law to other Federal, State and local governments ensuring the protection of the LEC provided CII. Finally, USTA believes that any Federal agency that has or will acquire LEC CII through governmental request should send such CII information immediately to DHS for retention, as DHS has the proper legal authority to protect LEC CII from disclosure.

USTA is well aware that section 214 of the Homeland Security Act does not preempt state law and that the proposed rules under section 29.8(g) mirror the provisions of section 214. The USTA proposal does not advocate preemption, as a statutory change to section 214 would be required. Rather, USTA seeks DHS rules that would require DHS to become the CII repository for Federal, State and local governments and that all requests for LEC CII be first made to DHS by Federal, State and local governments. In addition, USTA seeks a DHS requirement that Federal, State and local governments make their initial CII inquiry to DHS, before seeking such information independently from LECs. Under the USTA proposal, State and local governments could still solicit information from USTA member companies. If the information was not currently held by DHS, the LEC would consider the request and respond accordingly to the Federal, State, or local government requestor. Of course, if the information had already been provided to DHS, LECs would refer the Federal, State or local government requestor back to DHS.

Disclosure to Foreign Governments

USTA is quite concerned about section 29.8(j) of the proposed rules that would allow a foreign government to receive CII from DHS.¹¹ Under the proposed section 29.8(j), Disclosure to foreign governments:

The CII Program Manager, or the Program Manager's designee, may provide Protected CII to a Foreign Government without the written consent of the person or entity submitting such information to the same extent it may provide advisories, alerts, and warnings to other governmental entities as described in § 29.8(e) of this chapter, or in furtherance of an investigation or the prosecution of a criminal act.

Section 214 of the Homeland Security Act and its legislative history do not provide for disclosure of CII to foreign governments. The proposed rules do not mention any other ancillary authority that DHS may have to provide CII to a foreign government. Section 214(a)(1)(D)(i) authorizes the release of CII absent the written consent of the submitter

¹¹ *Id.* at § 29.8(j) 68 Fed. Reg. 18,528.

“in furtherance of an investigation or the prosecution of a criminal act,” but it does not allow for release to foreign governments. Thus, USTA questions whether DHS has the statutory authority to disclose CII to a foreign government.

USTA contends that the section 214 statutory safeguards are not applicable to foreign governments that could further disseminate the CII to other entities within or outside of that foreign country. USTA believes that the possibility exists that CII sent to a foreign government to prevent a crisis, could potentially one day form the basis of some act of terrorism. Thus, USTA questions the need and relevance of providing CII to foreign governments, given the sensitive nature of the information.

If indeed, DHS has the requisite authority to provide CII to a foreign government, USTA questions whether a CII Program Manager is the correct individual within DHS to have this authority. Given the nature of the material that may be provided and the international aspect of the request, we contend that the Secretary of DHS or a senior level designate within the Secretary’s Office be the interface for the decision to make CII available and for the information exchange.

Acknowledgement, Validation, and Making of Receipt

Pursuant to section 29.6(e)(D)(ii) of the proposed rules:¹²

If the CII Program Manager makes a final determination that the information is not protected CII, the Program Manager, per the submitter’s stated preference, shall either maintain the information without the protections of the CII Act of 2002 or dispose of it in accordance with the Federal Records Act. If the submitter, however, cannot be notified or the submitter’s response is not received within thirty (30) days after the submitter received the notification, the Program Manager shall destroy the information in accordance with the Federal Records Act unless the Program Manager determines that there is a need to retain it for law enforcement and/or national security reasons.

USTA believes that if the CII Program Manager determines that the CII does not fall within the protections of the Homeland Security Act, the CII should be returned to the LEC who provided it. This would preclude the need for the Program Manager to follow the procedures set forth in the Federal Records Act and would ensure that this most sensitive LEC information is protected. In the event that the Program Manager determines that the information is not protected CII but should be retained for law enforcement or national security reasons, the information should be exempt from FOIA disclosure. Thus, USTA proposes that DHS amend the aforementioned proposed rule to state that . . . the Program Manager determines that there is a need to retain it for law

¹² Id. at § 29.6(e)(D)(ii), 68 Fed. Reg. 18,528.

Department of Homeland Security

June 16, 2003

Page 7

enforcement and/or national security reasons *and such information shall be considered exempt from disclosure pursuant to FOIA.*

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION



By: _____

Its Attorneys:

Michael T. McMenamin
Lawrence E. Sarjeant
Indra Sehdev Chalk
Michael T. McMenamin
Robin E. Tuttle

1401 H Street, N.W, Suite 600
Washington, D.C. 20005
(202) 326-7300

June 16, 2003