USTA
UNITED STATES TELECOM ASSOCIATION

1401 H Street NW
Suite 600
Washington DC
20005-2164

Tel (202) 326-7300
Fax (202) 326-7333
www.usta.org

May 20, 2004

Ms. Janice Pesyna
Office of the General Counsel
Department of Homeland Security
Washington, D.C. 20528

Re: *Request for Comments – Procedures for Handling Critical Infrastructure Information; Interim Rule, 6 CFR Part 29*

Dear Ms. Pesyna:

The United States Telecom Association (USTA) submits these comments in response to publication by the Department of Homeland Security (DHS or the Department) of an interim rule (the Interim Rule) with request for comments regarding procedures to implement section 214 of the Homeland Security Act of 2002 (HSA) regarding the receipt, care, and storage of critical infrastructure information (CII) voluntarily submitted to DHS.[1]

USTA is the nation's oldest trade organization for the local exchange carrier (LEC) industry.[2] As LECs, USTA's members provide the backbone of our country's communications infrastructure, and ensuring the security of information regarding that infrastructure is invaluable to our members and the primary motivation for USTA's participation in this proceeding.

USTA commented on the Notice of Proposed Rulemaking (NPRM) published by DHS on April 15, 2003, regarding the receipt, care, and storage of CII[3] and remains especially concerned about the control and monitoring of CII that flows to federal, state, and local government entities, federal contractors, and to foreign governments. USTA appreciates the opportunity to provide the following comments on a few aspects of the Interim Rule.

---

[1] *Request for Comments – Procedures for Handling Critical Infrastructure Information; Interim Rule,*6 C .F.R. Part 29 (rel. Feb. 20, 2004).
[2] USTA's carrier members provide a full array of voice, data, and video services over wireline and wireless networks.
[3] *Procedures for Handling Critical Infrastructure Information: Proposed Rule*, 6 C.F.R. Part 29 (June 16, 2003) (USTA Comments).

DISCUSSION

1. Indirect Submissions

USTA urges DHS to revise section 29.2(i) of the final rule to clarify that only DHS and no other federal government agency shall be the recipient of voluntarily submitted CII.[4] USTA's members are gravely concerned about releasing vulnerability and outage information regarding their voice and data telecommunications networks to federal agencies that might be required to release the information under the Freedom of Information Act (FOIA).[5] In order to avoid any question of the FOIA status of CII submitted to another entity within the federal government prior to its transmission to DHS, the final rule should state clearly that (1) CII submitted indirectly to DHS should be transmitted immediately to DHS by the federal agency originally receiving it, (2) the agency originally receiving CII should not retain a copy of it, and (3) the receiving agency must promptly submit the CII to DHS within a set time frame (preferably no more than seven days).

The Department is likely to encounter organizational obstacles while responding to the flood of CII submitted by industry. For this reason, USTA supports a phased implementation of the program, limiting the materials the CII program manager can receive from other federal agencies until the program reaches its third phase.[6]

2. Protected CII Program Management and Administration

DHS envisions granting access to Protected CII (as such term is defined in the Interim Rule)[7] to federal, state, and local government entities requesting it pursuant to an "express written agreement" with DHS.[8] As required by Section 214(a)(1)(E) of the HSA[9] and section 29.8(d)(3) of the Interim Rule,[10] CII provided to federal, state, or local

---

[4] 6 C.F.R. § 29.2(i).
[5] 5 U.S.C. § 552.
[6] *See* Fred Herr, Implementation of the CII Act of 2002: Program Overview, Presentation at Joint Meeting of Sector Coordinators and ISAC Council (Feb. 18, 2004). During the first phase, material may be submitted only through the Protected CII program office and disseminated to Information Analysis Infrastructure Protection (IAIP) analysts only. In the second phase, the program office will accept materials submitted through IAIP, and will disseminate information to IAIP analysts and other DHS entities. In the third phase, the program will have full operating capability, and the program office will accept submission of material through any DHS entity and disseminate information to IAIP analysts, DHS entities, and federal, state, and local governments.
[7] 6 C.F.R. at § 29.2.
[8] *Id*. § 29.8(b).
[9] 6 U.S.C.A. § 133 (a)(1)(E) (Supp. 2004).

entities is not subject to state or local law requiring disclosure of information, may not be disclosed or distributed without the written consent of the submitter, and may be used for critical infrastructure protection, criminal investigation, or criminal prosecution purposes. These requirements of law should be stated in the express written agreements contemplated by DHS in order to assure those submitting CII that their information will not be disclosed improperly.

Sharing Protected CII with federal, state, and local entities will make those entities responsible for protecting this information. This is troublesome given that DHS has no way to guarantee compliance. Until safeguards are in place, USTA member companies may be disinclined to provide CII. USTA encourages DHS to develop and implement processes for regularly auditing compliance by federal, state, and local entities with their express written agreements.

3. Storage of Protected CII

USTA is troubled by the Department's revision of section 29.7(b) regarding storage of Protected CII. In response to comments that proposals to store Protected CII in a "locked desk" were insufficient to protect against unauthorized access, DHS revised section 29.7(b). The revisions, however, appear to de-emphasize the importance of safeguarding CII. The Interim Rule is now so vague that it is impossible to discern exactly how DHS will safeguard information. DHS says, "When Protected CII is in the physical possession of a person, reasonable steps shall be taken to minimize the risk of access to Protected CII by unauthorized persons."[11] It adds, "When Protected CII is not in the physical possession of a person, it shall be stored in a secure environment that affords it the necessary level of protection commensurate with its vulnerability and sensitivity."[12] The implication of this section of the Interim Rule is that DHS will make a subjective judgment about whether certain information is more sensitive than other information. Federal regulations, however, must be specific, leaving no room for such subjective judgments. If industry is to continue to voluntarily share CII, it must have reasonable assurances that the CII will be secure. DHS should review federal regulations for properly storing sensitive confidential information and prescribe specific security measures to safeguard information in the final rule.

4. Disclosure of Information

Disclosing Information to Contractors

USTA supports requiring contractors to comply with the rules regarding disclosure of Protected CII. While section 29.8(c) of the Interim Rule requires contractors to enter into express written non-disclosure agreements before handling CII and to agree to comply

---

[10] 6 C.F.R. § 29.8(d)(3).
[11] *Id*. at § 29.7(b).
[12] *Id*.

with all of the requirements of the CII program, it does not appear to prescribe any penalties for contractors who violate the requirements of the CII program.[13] Section 29.9(d) of the Interim Rule establishes criminal and administrative penalties for officers and employees of the United States who divulge CII without authorization, but it does not mention contractors.[14] USTA contends that contractors should be subject to the same penalties for disclosing CII as are federal employees. Furthermore, USTA maintains, as it did in its previous comments, that prior to sharing CII with contractors, DHS should verify that contractors possess the same security clearances as federal government employees who handle CII. [15]

Sharing Information with Foreign Governments

DHS believes that through the establishment of formal agreements with foreign governments, protected CII can be safely shared with foreign governments. USTA strongly disagrees. Not only does DHS lack the statutory authority to disclose CII to foreign governments,[16] but sharing this information raises a serious concern that the information could fall into the wrong hands. Another concern is that many foreign governments own or finance companies that compete with American technology companies and service providers, and access to CII could give them a commercial advantage. Still another concern is that Section 214 statutory safeguards would be of no effect if foreign governments further disseminate Protected CII to other countries or organizations.

Although the Department seeks to protect homeland security, it should be mindful of the nation's economic security, as well. If DHS expects American companies that own and operate the nation's telecommunications networks to provide CII voluntarily, DHS must assure these companies that their CII will not be disclosed to foreign competitors and will be disclosed to foreign governments only for purposes related to or affecting national security.

5. Return and Withdrawal of Material

Many of those commenting on section 29.6 of the proposed rule argued that material should be returned to its owners in the event that DHS makes a final validation determination that the material is not Protected CII. DHS rejected this argument, saying

---

[13] 6 C.F.R. § 29.8(c).
[14] *Id*. at § 29.9(d).
[15] USTA Comments at 3.
[16] *See* USTA Comments at 5. Neither Section 214 of the HSA nor its legislative history provide for disclosure of CII to foreign governments. *See also* 69 Fed. Reg. 8079. Although DHS acknowledged that it received 14 sets of comments expressing concern that the Department lacked authorization to share Protected CII, it failed to issue any formal legal or statutory analysis showing that it possesses the requisite authority.

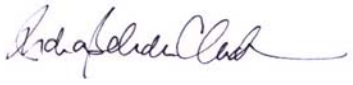
it would place too great an administrative burden on the Department. USTA urges DHS to reconsider its decision. The Department expects LECs to voluntarily share information regarding the nation's telecommunications infrastructure – information that is rife with national security and trade secret implications. Without assurances from DHS that their CII will be exempt from disclosure under FOIA, USTA's members will have little incentive to share information. USTA recommends that DHS rewrite this section to instruct the party submitting information to include a written statement requesting that its submission be returned if it does not qualify for protection. In addition, the rule could require submitters to enclose a self-addressed, stamped envelope in order to reduce the Department's administrative burden. If the Department remains unwilling to return submissions, it should, at the very least, notify a party when its information has been found not to qualify for protection or not to have been submitted in good faith so that party has the opportunity to resolve any misunderstanding about the nature of the information.

CONCLUSION

USTA urges DHS to revise the Interim Rule to address the concerns raised in these comments. While DHS has made strides toward ensuring the security of CII, it should do more to protect this information. Additional safeguards will reinforce industry's commitment to protecting our nation's critical infrastructure.

Respectfully Submitted,

UNITED STATES TELECOM ASSOCIATION



By:_____

James W. Olson
Indra Sehdev Chalk
Michael T. McMenamin
Robin E. Tuttle

Its Attorneys

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