

Coalition Supporting Confidentiality.txt

Subject: Coalition Comments to RIN 1601-AA14  
Date: Mon, 16 Jun 2003 17:00:14 -0400  
From: "Laurence Brown" <LBrown@eei.org>  
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>  
CC: "David Owens" <DOwens@eei.org>, "Ken Hall" <KHall@eei.org>, <infoshare@ls.eei.org>

June 16, 2003

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

Re: RIN 1601-AA14  
Notice of Proposed Rulemaking,  
Procedures for Handling Critical Infrastructure Information

Attention:

Attached hereto for submittal via e-mail are the comments of the Coalition Supporting Confidentiality for Critical Infrastructure Information in the above proceeding. In addition, the original and three copies are being sent this day by first-class mail.

Respectfully,

Laurence W. Brown  
Director, Legal Affairs, Retail Energy  
Edison Electric Institute  
701 Pennsylvania Ave., NW  
Washington, DC 20004

202/508-5618

Coalition\_DHS\_V3a.doc

Name: Coalition\_DHS\_V3a.doc  
Type: WINWORD File (application/msword)  
Encoding: base64  
Description: Coalition\_DHS\_V3a.doc

Coalition\_Cover-1ttr.doc

Name: Coalition\_Cover-1ttr.doc  
Page 1

Coalition Supporting Confidentiality.txt  
Type: WINWORD File (application/msword)  
Encoding: base64  
Description: Coalition\_Cover-lttr.doc

June 16, 2003

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

Re: RIN 1601-AA14  
Notice of Proposed Rulemaking,  
Procedures for Handling Critical Infrastructure Information

Attention:

Attached hereto for submittal via e-mail are the comments of the Coalition Supporting Confidentiality for Critical Infrastructure Information in the above proceeding. In addition, the original and three copies are being sent this day by first-class mail.

Respectfully,

Laurence W. Brown  
Director, Legal Affairs, Retail Energy  
Edison Electric Institute  
701 Pennsylvania Ave., NW  
Washington, DC 20004

202/508-5618

**BEFORE THE  
UNITED STATES  
DEPARTMENT OF HOMELAND SECURITY**

**PROCEDURES FOR HANDLING CRITICAL INFRASTRUCTURE INFORMATION  
6 C.F.R. PART 29**

**(RIN 1601-AA14)**

**COMMENTS IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING**

**on behalf of the**

**COALITION SUPPORTING CONFIDENTIALITY FOR  
CRITICAL INFRASTRUCTURE INFORMATION**

The Coalition Supporting Confidentiality for Critical Infrastructure Information (Coalition) strongly supports the initiative announced in the Department of Homeland Security's (the Department's) Notice of Proposed Rulemaking issued on April 15, 2003 (68 Fed.Reg. 18524-29) to implement Title II (the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§131, *et seq.*), of the Homeland Security Act of 2002 ("HSA" or "the Act") (Pub.L. 107-296). The Coalition does recommend one major substantive change, as well as several technical corrections or clarifications.

Introduction

The Coalition is an informal, *ad hoc* association of trade associations representing, and individual businesses who are, providers of critical services by means of owning or operating the nation's critical infrastructures as defined in the HSA. For purposes of this filing, the signing entities constitute the Coalition, although other entities have participated in Coalition activities over the last several years. The Coalition was directly involved in representing the interests of critical infrastructure owners and operators in seeking to create statutory protections for critical infrastructure information, as were ultimately embodied in HSA Section

214. In addition, members of the Coalition have otherwise sought to facilitate the voluntary sharing of infrastructure security information with the federal government by means such as creating, sponsoring, or being founding members of critical infrastructure Information Sharing and Analysis Centers, or “ISACs,” which qualify as “information sharing and analysis organizations” under the Act. Various members of the Coalition continue to assist the government on an active basis, both in obtaining valuable information for the Department to use in protecting homeland security, and in advertising the need for a close collaboration between infrastructure providers and their governments worldwide.

### Summary

In general, the Coalition wishes to express our appreciation for a strong, clear proposal that reflects the language and intent of Section 214 of the Act. We look forward to cooperating with the Department on strengthening mechanisms for two-way communication between the government and private-sector critical infrastructure owners and operators. We have long understood that protecting the nation’s critical infrastructure in today’s interdependent world requires a new, more cooperative relationship between industry and government, which in turn depends upon full, open communication. That level of communication itself relies on mutual trust and respect for each partner’s concerns.

The Coalition believes that the proposed regulations create a strong foundation for building the necessary trust relationships and for facilitating the development of the public private partnerships so often recognized as critical for success in protecting the Homeland. Therefore, we wish to convey our understanding that, by virtue of the clear language of the Act itself, all voluntarily submitted “critical infrastructure information” (CII, as defined by the Act), is immediately and automatically entitled to the protections of the Act, regardless of the adoption by the Department of final regulations implementing a CII Program. Further, we applaud the Department’s proposed regulations (particularly within section 29.5) for permitting “indirect” submittals of CII. This mechanism effectively implements the HSA’s explicit

requirement at Section 214(e)(2)(A) that the Department’s CII Program include “mechanisms regarding ... the acknowledgement [*sic*] of receipt by Federal agencies [*sic*] of critical infrastructure information that is voluntarily submitted to the Government.” This mechanism also conforms to, and thoughtfully clarifies, the Act’s somewhat oblique reference at Section 212(4) to “any” agency head designating the critical infrastructure protection program of “a” – rather than “the” – covered agency to receive critical infrastructure information (once that program has itself been designated “as” such a program pursuant to Section 213).

As outlined above, the Coalition is, overall, quite satisfied with the proposed regulations. Notwithstanding this, however, we do have one major criticism, as well as some further suggestions for additional, more technical corrections or clarifications. In particular, section 29.6(f) of the proposed regulations seems counterproductive, and out of step with the remainder of the proposal. After discussing that section of the proposed regulations, we discuss those sections where additional correction or clarification would be beneficial.

I. All Information Submitted Under the Protection of the Homeland Security Act Should be Treated In the Same Manner

Proposed section 29.6(f) would permit the Critical Infrastructure Information Program Manager to make a determination that information submitted with a request for protection under the Act was “not submitted in good faith [in] accordance with the CII Act of 2002 and these [proposed] procedures.” However, the provision fails to set forth any standard by which the CII Program Manager could make such a determination. Moreover, the proposed regulations would not require the Program Manager to notify a submitter of such a determination, simply stating without further justification or analysis that “[t]his is the only exception to the notice requirement of these procedures” (proposed section 29.6[e]).

This unbounded exception, even though its exercise is not mandatory, is directly contrary to the spirit of cooperation (a) intended to be fostered by the Act, and (b) well reflected in the otherwise applicable notice provisions set forth in proposed section 29.6(e).

Moreover, even if a standard for making such a decision were created and added to the Department's regulations, the possibility would still remain that some private-sector information given to the Department would be unprotected from disclosure to any entity that seeks it, without any notice to that effect provided to the submitter. A mistaken or otherwise unjustified determination of "bad faith" could seriously harm the protection of critical infrastructure. Further, this proposal will hinder the ability of the government to obtain such information in the first instance.

The risk of such unannounced and unforeseeable determinations will dissuade many private sector infrastructure owners and operators from making any voluntary submittal at all. This risk will also inhibit many others from making their submittals as complete as possible. As a result, the Department will not get all the information it needs, including information it may specifically request.

The Act itself only provides one exception to the protection of voluntarily submitted CII for "bad faith." HSA Section 214(a)(1)(C) states that CII "shall not ... be used ... in any civil action ... if such information is submitted in good faith." The structure of that section makes the intent of Congress clear. Congress intended the "bad faith" exception to be a **judicially enforced** safeguard against abusive submittals that prevent information from being properly used in litigation, not a general principle to be implemented or applied by the Department. We believe that the instances where a critical infrastructure owner or operator would actually submit any information in bad faith will be exceedingly rare. Therefore, it is both unnecessary and very likely inappropriate for the Department – part of the Executive branch – to take on a role that under the Act is clearly directed at protecting the integrity of, and the use of information in, litigation — a function administered by the Judicial branch.

Moreover, a separate provision for a determination by the Department is both unnecessary and potentially dangerous. Information either is CII as defined by the Act, or it is not. If submitted information is not actually CII, then the procedures set forth in proposed

section 29.6(e) will permit the Department to deal adequately with that submittal. If the information actually meets the definition of CII, then it should be protected unless and until a judge decides otherwise, during the course of litigation, because of a bad faith submittal. In such a situation, the judge can fashion a mechanism whereby the litigants can use the information to the extent necessary, while still affording the infrastructure owner or operator – and the nation – protection from potential public disclosure. Thereby, litigation can proceed as appropriate, and critical infrastructure can remain protected from inappropriate dissemination.

For all of the above reasons, we request that the paragraph embodied in proposed section 29.6(f) be deleted in its entirety. At the very least, if not deleted, this particular section must be modified to make it more closely conform to the statutory language. In particular, the final regulation should, in that case, stipulate that **all** CII will be equally protected unless and until a judge authorizes it to be used, under appropriate protective measures, in civil litigation. In addition, if the CII Program Manager is to be permitted to make a determination of bad faith, there should be an **objective** standard by which the Manager would make such a determination. Moreover, such modification should also make provision for notification procedures identical to those set forth in proposed section 29.6(e), in order to provide a fair opportunity to submitters to contest any such determination of bad faith, and to give potential submitters confidence that they would not be surprised at some unknown and unforeseeable later date that such a determination had been made.

The following text is one possibility for drafting language that would permit section 29.6(f) of the regulations to implement the alternative approach outlined above:

“In the event the CII Program Manager determines that any submitted information, in light of all of the circumstances under which it was submitted, and although it may meet the definition of CII, was not submitted in good faith, the Program Manager must notify the submitter of such a determination and otherwise comply with the procedures of section 29.6(e).”



It is necessary for the Department, if it decides not to delete section 29.6(f) as the Coalition suggests, to follow the procedures in section 29.6(e) in order to ensure that information which actually meets the definition of CII (and is therefore inherently sensitive) always is afforded the full protections to which CII is entitled unless and until a final determination is made that a “bad faith” submittal renders it no longer entitled to protection under the Act (similar to section 29.6[b]). However, the uncertain application and effect of this alternative provision, the very complexity of even attempting to craft language sufficient to adequately address the problems pointed out above, and the burden on the Department in attempting to administer the procedures all indicate that the best course for the Department is simply to remove the proposed section 29.6(f) from the final regulations as we suggest.

## II. Additional Items for Further Correction or Clarification

1. Proposed section 29.8(f)(2) provides for what may reasonably be termed a “whistle-blower” exception to the otherwise general prohibition against unauthorized disclosure of CII. In particular, see subparagraphs (i) and (ii). However, it is not clear to whom such disclosures may be made.

It would seem to run counter to the thrust of the proposed regulations to permit such disclosures to any member of the public. One reasonable interpretation, and what may have been intended, is that disclosures pursuant to subparagraphs (i) and (ii) are limited to the individuals named in the preceding sentence of the section: the DHS Inspector General or another designee of the Secretary. If that interpretation was not intended, or is more narrow than was intended, we suggest limiting such disclosures to some recognized governmental authority with sufficient responsibility to ensure that appropriate action can be taken to remedy the problems noted in subparagraphs (i) and (ii). However this provision is clarified, the HSA requires the Department to be as sensitive to the need to protect CII as it is to the need to remedy violations of law and/or ethics.

2. Proposed section 29.6(g) makes it clear that only CII Program Managers, or their designees, may remove the protected status from CII material. However, that section does not set forth the circumstances under, or the standards by, which such action may be taken. The Coalition suggests that this section be clarified to indicate either that (1) such action will only be taken at the written request of the originally submitting entity, or, at the least, (2) when protected CII status is removed, the CII Program Manager must contact the submitter pursuant to section 29.6(e)(1)(ii) (note also comment 5, below).

3. Proposed section 29.9 does not address the problem of violations that may be committed by contractors who receive CII under section 29.8(c), or state and local personnel who may obtain CII under section 29.8(d). The Coalition suggests clarifying either that any contractor will be subject to the provisions of section 29.9 as if an “employee” of the government, or that they will be treated the same as state and local personnel. In that regard, and consistent with Section 214(e)(2)(D) of the Act, we suggest that no transmittals of CII be made to state and local personnel unless they agree to be bound by section 29.9 of the regulations.

4. Proposed section 29.8(j) appears to authorize the release of CII to foreign governments to aid the prosecution by those governments of criminal acts. However, such releases should be made only in the course of an investigation or prosecution pursuant to treaty or other authorization to provide mutual legal assistance, and not pursuant to an independent decision by the CII Program Manager or the Department. Accordingly, the last clause of section 29.8(j) should be deleted, starting with “, or” — any disclosures made to foreign governments in support of a criminal investigation or prosecution should only be made by the appropriate law enforcement authorities under section 29.8(f)(1)(i)(A) and other legal authority. Further, the Coalition suggests that this section be clarified to ensure that information is released to foreign governments only to permit warnings, or in any event is “scrubbed” pursuant to the requirements of section 29.8(e). In addition, we suggest adding the phrase “and under the same

conditions” after the phrase “to the same extent,” to make it clear that, when communicating to foreign governments, the United States government must protect sources and proprietary data as much as must other federal agencies and state and local governments.

5. Proposed section 29.6(e)(1)(ii) addresses the treatment of material by the Department once it no longer is designated as CII. However, the proposal does not address situations where such information may have been conveyed to other Federal entities, to contractors, or to states. Neither does the proposal address the status of any such material retained for law enforcement or national security reasons. The Coalition suggests that this section be clarified by specifying that the CII Program Manager will contact any recipient of that information, inform them that it is no longer protected, and instruct them either (1) to treat it in accordance with the submitter’s instructions, or (2) destroy it if there are no such instructions, even if it is retained by the Department’s Program Manager for law enforcement or national security reasons. Further, the Coalition suggests that the regulations clarify that, when such material is retained for law enforcement or national security reasons, it will be considered exempt from FOIA disclosure pursuant to the FOIA law-enforcement or national security exemptions.

6. Proposed sections 29.6(e)(1)(i)(D), 29.6(e)(1)(ii), and 29.7(d) use the terms “destroy,” “dispose,” “disposed,” and “disposed of” when specifying how to deal with material that is not eligible for protection as CII, or is no longer to be protected. The Coalition suggests that these terms are not necessarily synonymous, and that the consistent use of “destroy” and “destroyed” is far more clear and appropriate.

7. Proposed section 29.8(a) appears to authorize access to CII under an extremely broad range of circumstances, including for such authorized government purposes as the promotion of trade, and could therefore result in harm to submitters, for instance if competitors obtained access to such information as part of such trade promotion activities. This is far more broad than is necessary to meet the objectives of the Department, or than is authorized under HSA Sections 214(f) and 214(a)(1)(D)(ii). The Coalition suggests restricting the over breadth of this

proposal by simply deleting the text of the proposed regulation after the date “2002.” The Act itself contains sufficient specificity without any need for additional language that, as the case with the proposed language, could give rise to overly expansive or even conflicting interpretations.

8. Proposed section 29.8(i) includes the phrase “for homeland security purposes.” This phrase is superfluous, and seems destined to invite unnecessary litigation over its meaning. Inasmuch as the Act already specifies all of the necessary requirements in the definition of “critical infrastructure information,” the Coalition suggests deleting the above phrase.

9. Proposed sections 29.6(c) and 29.5(d)(1) specify the marking that shall be made on CII to indicate it is protected. This is particularly important for CII that may be shared with contractors or state and local personnel. However, the two sections require different markings: “Protected CII” and “Protected Critical Infrastructure Information.” The Coalition suggests that using only one such marking will reduce confusion over whether material actually is properly subject to protection. At the least, we suggest stating in both sections that either marking can be used.

10. Proposed section 29.8(g)(1) stipulates that individuals who have questions regarding the protection of CII should contact the CII Program Manager. The Coalition suggests that this section be further augmented by adding a requirement that the Program Manager notify a submitter whenever becoming aware of FOIA litigation concerning any CII, similar to the requirements of proposed section 29.9(c).

11. Proposed section 29.5(c) refers to submittals “to the CII Program Manager,” whereas proposed section 29.5(b)(1) broadly refers to submittals “to the IAIP Directorate.” Inasmuch as all voluntary submittals to a CII program are protected under the Act, the reference in section 29.5(c) the Program Manager is overly restrictive, and should be changed to conform to section 29.5(b)(1).

12. The Coalition suggests the addition of a new section 29.3(f) to repeat the language of the Act at Section 214(a)(1)(F) that submission of voluntary information does not constitute a waiver of any otherwise applicable privilege or protection, such as for trade secrets. The proposed regulations have many other similar repetitions of the Act's requirements, presumably to aid the reader by reducing the need to cross-reference with the text of the HSA, and this would include in the regulations an important privilege provided by the Act.

13. Proposed section 29.7(b) refers to storage of CII in a locked desk or file cabinet, or in a guarded facility, after working hours. However, this does not seem adequate for large compilations or aggregations of data. For such collections, at any time of day, a secure room with limited access would be more appropriate. Moreover, the proposal could be read to permit more lax security during working hours (which are not defined) than after working hours.

Therefore, the Coalition suggests modifying this section to read as follows:

“All reasonable steps, consistent with the degree of security appropriate for the sensitivity of the Protected CII at issue, shall be taken to minimize the risk of access to Protected CII by unauthorized personnel. Protected CII shall be stored in a secure environment with limited access, such as a locked room, filing cabinet, or desk, or other secure container, within a facility where Government or Government-contracted security is provided.”

14. Proposed section 29.9(c) provides for notification of a submitter when unauthorized access to, or loss of, CII has occurred. However, there is no time period provided for such notice. The Coalition suggests that notice ought to be provided within some reasonable period after discovery of such access or loss. We suggest 72 hours as a workable period for the Department that will also allow the submitter to protect against any adverse impact that might result from that loss or unauthorized access.

15. Proposed section 29.7(e) states that protected CII may be transmitted by the U.S. Postal Service as well as by “secure electronic means.” We understand that this permits a physical

transmittal to be protected by such postal laws as those pertaining to mail tampering. However, first class (and perhaps even express) service is far less intrinsically secure than certified or registered service. If limiting physical delivery to delivery by the Postal Service, we suggest restricting such delivery to certified or registered (and perhaps also express) service. It would seem, however, to be reasonable to allow physical delivery by any reasonably secure means.

16. Proposed section 29.6(d) has three numbered subparagraphs. As printed in the Federal Register (at page 18528), the numbering of those subparagraphs reads “(1),” “(2),” and “(1),” in what appears to be a typographic error for the intended “(1),” “(2),” and “(3).”

17. Finally, in most contexts the word “Protected” in the phrase “Protected CII” is simply redundant. If it is necessary in any circumstance at all, it is only in the context of describing the marking required to ensure notice that CII is “Protected.”

### Conclusion

For all of the foregoing reasons, the Coalition respectfully requests that proposed section 29.6(f) be removed from the final regulations (or at least modified as described above),

and that the other proposed sections discussed above be clarified as described above. In conclusion, we thank you for this meritorious proposal, as well as for this opportunity to respond to it. The Coalition will be pleased to work with the Department to further clarify the proper scope of CII and any measures necessary to protect it.

Respectfully submitted,

David Y. Peyton  
Director, Technology Policy  
National Association of Manufacturers  
1331 Pennsylvania Ave., NW  
Washington, DC 20004-1790  
(202) 637-3147

Joseph Tasker, Jr.  
General Counsel & Senior Vice President  
Information Technology Association of  
America  
1401 Wilson Blvd., Suite 1100  
Arlington, VA 22209-2318  
703-284-5331

Shannon L. Kellogg  
Director, Information Security Policy  
Business Software Alliance  
1150 18<sup>th</sup> St., NW, Suite 700  
Washington, DC 20036  
202/872-5500

Bruce J. Heiman  
Executive Director  
Americans for Computer Privacy  
1735 New York Ave., NW, Suite 500  
Washington, DC 20006-5209  
(202) 628-1700

Jack Lichtenstein  
Director of Government Affairs  
& Public Policy  
ASIS International  
1625 Prince Street  
Alexandria, VA 22314  
703-518-1484

David K Owens  
Senior Vice President  
Edison Electric Institute  
701 Pennsylvania Ave., NW  
Washington, DC 20004  
202/508-5000