May 20, 2004

Ms. Janice Peysina
Office of the General Counsel
Department of Homeland Security
Washington, DC 20528

(cii.regcomments@DHS.gov)

Re: Comments on "Procedures for Handling Critical Infrastructure Information; Interim Rule" (Part IV, 6 CFR Part 29)

Attention:

Attached hereto are the comments of the Edison Electric Institute in the above proceeding. In addition, an original and three copies are being sent this day by first-class mail.

The essence of our comments is to note that the Interim Rule has already created a problem for the Department that hinders the successful performance of its mission. Our industry cannot expeditiously provide information identifying our critical facilities because that information will not be protected from public disclosure if provided directly to the Department of Energy, the Sector-Specific Agency for energy, or directly to the Information Assessment and Infrastructure Protection Directorate. Instead, under the Interim Rule, the information will be protected as Critical Infrastructure Information (CII) only if provided to the CII Program Office. The information will then be unavailable to any other office within the Department, or any other federal agency, until some protective agreement is arranged.

As noted in the attached comments, the solution is straightforward. CII should instead – as provided in the originally proposed CII regulations – be submitted to and used by a federal agency, or any office within DHS, having a delegated or legitimate purpose for obtaining it voluntarily, if labeled and accompanied by a request that it be transmitted to the Department's CII Program Office for

protection. We respectfully urge the Department to modify the Interim Rule to remove the impediment created by its current formulation.

Respectfully,

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

202/508-5618
LwBrown@EEI.org

UNITED STATES OF AMERICA
DEPARTMENT of HOMELAND SECURITY

COMMENTS OF EDISON ELECTRIC INSTITUTE TO
DEPARTMENT OF HOMELAND SECURITY ON
"PROCEDURES FOR HANDLING CRITICAL INFRASTRUCTURE INFORMATION;
INTERIM RULE"
(Part IV, 6 CFR Part 29)

Introduction

Edison Electric Institute (EEI) is the national association of U.S. shareholder-owned electric companies, affiliates, and industry associates worldwide. EEI's members are located in 49 states and the District of Columbia, and serve over 90% of all customers served by the shareholder-owned segment of the electric industry. EEI's members generate approximately 75% of all electricity generated by electric companies. Its members own approximately 70% of the nation's transmission facilities, and serve about 70% of all retail customers. EEI frequently addresses matters of importance to the industry being considered by federal and state agencies, the courts, and the U.S. Congress.

EEI has a Security Committee composed of member-company personnel, many of whom have extensive law enforcement or military backgrounds, and whose areas of responsibility, in addition to the physical security of distribution, transmission, and fossil-fuel generation facilities, can include natural gas, hydroelectric generation, and nuclear generation facilities, as well as data security and business continuity. As noted above, a number of EEI member companies own or operate nuclear power plants subject to the security requirements of the Nuclear Regulatory Commission, and hydroelectric facilities subject to the safety and security regulations of the Federal Energy Regulatory Commission. Also, a number of EEI member companies are "combination" companies – combined electric and gas companies, or operate other major gas facilities, and participate in the security activities of the American Gas Association. Moreover, several EEI member companies operate facilities subject to the maritime security regulations of

the United States Coast Guard. Thus, EEI members are significantly involved in a number of sensitive, critical security issues and protocols.

EEI was directly involved in representing the interests of electric utility and other infrastructure owners and operators in seeking to create statutory protections for critical infrastructure information (CII), that were ultimately embodied in the Critical Infrastructure Information Act of 2002, Title II Part B of the Homeland Security Act (the "HSA," 6 U.S.C. §§131, *et seq.*, Pub.L. 107-296). In addition, EEI has sought to facilitate the voluntary sharing of infrastructure security information with the federal government by such means as helping to create the Electric Sector Information Sharing and Analysis Center (ES-ISAC), and in promoting the creation of the gas and oil pipeline, water and chemical industry ISACs, all of which qualify as "information sharing and analysis organizations" as defined by the HSA. EEI also participated in helping create the Partnership for Critical Infrastructure Security, as well as the development of the National Strategy to Secure Cyberspace and the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. EEI continues to assist the government on an active basis, both in obtaining valuable information for the Departments of Homeland Security (DHS) and Energy (DOE) to use in protecting homeland security and the nation's energy infrastructure, and in advertising the need for a close collaboration between infrastructure providers and their governments worldwide.

EEI strongly supported, and commented on, the original draft regulations proposed by DHS to implement the CII Act. EEI also participated in drafting the comments to the Interim Rule filed by the U.S. Chamber of Commerce (Chamber) and the North American Electric Reliability Council (NERC). EEI fully supports those

comments, yet is submitting additional, separate comments to highlight the practical difficulties created by the current version of the CII regulations.

Comment

Section 29.5 of the originally proposed regulations acknowledged a mechanism for "indirect" submittals of CII to DHS "through" other federal agencies. This mechanism would have effectively implemented the Homeland Security Act's explicit requirement - at Section 214(e)(2)(A) - that the CII program include "mechanisms regarding ... receipt by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government." This also conforms to, and thoughtfully clarifies, the Homeland Security Act's 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.

The Interim Rule, however, while noting in the Preamble (69 Fed.Reg. 8075) that this is an issue needing further attention, completely removes this provision: "Section 29.2(i) has been revised to clarify that only the Department and no other Federal government entity shall be the recipient of voluntarily submitted CII. Sections 29.5(a), 29.5(b), and 29.5(c) have been revised to remove references to indirect submissions and to clarify that submissions must be made directly to the Protected CII Program Manager or the Program Manager's designee." Thus, under the Interim Rule, DHS has held that even material that clearly meets all other requirements of the HSA will not be afforded protection as CII unless it is submitted only and directly to the DHS CII Program Office. The information will then be unavailable to any other office within the Department, or any other federal agency, until some protective agreement is arranged.

As signatories to the aforementioned Chamber and NERC comments, EEI noted that this requirement would create serious problems in attempting to help DHS respond to

emergency situations. In fact, this has already created that very problem in assisting DHS to prepare for emergencies. Specifically, it has impeded the ability of the private sector to assist DHS in assembling lists of nationally critical facilities.

The President has directed that such lists be created (Homeland Security Presidential Decision No.7, Paras.8, 27[a and b] and 31), and has given that task to the Secretary of the Department of Homeland Defense (*supra.*, Para.13). The President has directed that the Secretary coordinate that effort with various sector-specific agencies, including the Department of Energy for the electric utility industry (*supra*, Paras. 8, 17, 18[d] and 35). Further, the President has directed that such work be done in close collaboration with the private sector (*supra*, Paras.8, 17, 19[a] and 25[a]).

DHS has already begun work on these lists. Undersecretary Frank Libutti in testimony before the House Homeland Security Appropriations Subcommittee on April 1, 2004, stated that work on such a list had already begun. (see Appendix for relevant portions of transcript). Assistant Secretary Robert Liscouski noted, in testimony before the House Select Homeland Security Committee Subcommittees on Infrastructure and Border Security, and Cybersecurity, Science, and Research and Development, on April 21, 2004, that work also had begun on the National Plan for Critical Infrastructure and Key Resources Protection and the National Response Plan. Each of those plans involves a substantially similar list (see HSPD-7[27], and HSPD-5). Finally, DHS is currently working on a "critical facilities list" related to venues for upcoming national events through the 2005 Inauguration (see HSPD-7[26]).

As directed by the President, DHS has asked DOE, as the appropriate Sector-Specific Agency, to engage the industry in creating the energy portion of those lists and plans. DOE, in turn, has asked the electric utility industry to provide input into that process. This immediately raises the thorny question of how to protect what, in essence, could become a "target list" of nationally important electric (and other) infrastructure.

DHS has not stated whether or how it can fully protect the confidentiality of any sensitive information it receives – voluntarily from the industry – through DOE, as opposed to information submitted directly to the CII Program Office pursuant to the Interim Rule.

Unless CII can be adequately protected, few – if any – private sector entities will provide it (which was the driving principle behind the Critical Infrastructure Information Act). However, without input from infrastructure owners. DHS will have to depend on or create a "list" that is very unlikely to reflect current reality. As an example, during an "Orange" threat alert level, scarce National Guard or State Police forces could be sent to utility facilities that are out-of-service or no-longer-important because the "list" of "critical facilities" was out of date or otherwise inaccurate. In fact, analogous events have already occurred.

We believe that the information being requested of our industry in order to create the aforementioned lists and plans obviously and unequivocally fits the HSA definition of CII. However, under the current version of the DHS CII rule, that information would not be entitled to CII protection simply because it was given to DOE. Thus, our industry may be unable to comply with DOE's request for that information, or may be forced to provide it only through some cumbersome, ad hoc mechanism whereby it would go directly to the DHS CII Program Office without being analyzed or fit into a larger energy context by DOE, and without even being available to the DHS Information Assessment and Infrastructure Protection Directorate (IAIP) for its own use during some unknown period until IAIP and the CII Program Office enter into an agreement regarding the care and protection of that information. Such a result, we believe, is counterintuitive and counterproductive, as well as directly contrary to the spirit, intent, and letter of the HSA.

There is a simple, effective, sanctioned solution to this problem. As provided in the proposed CII regulations, CII could be submitted to – and used by – any federal agency, as well as any office within DHS, having a properly delegated or other legitimate

purpose for obtaining it voluntarily from the private sector, as long as it was properly labeled and accompanied by a request that it be transmitted to the DHS CII Program Office for protection as CII under the HSA. Adoption of this proposal would permit IAIP, and DHS as a whole, to better fulfill their responsibilities and respond to Presidential directives in a timely fashion.

Beyond obtaining the information from the private sector, we are aware that the issue of how to provide an adequate level of that information to the states is a difficult one still subject to further development in the National Plan for Critical Infrastructure and Key Resources Protection. Nonetheless, it is critically important to create a mechanism whereby sensitive or CII information can be protected when shared with state and local entities. Too many times over the last two years, we have already seen the existing "lists" of "critical facilities" very widely released once communicated to the states. Such overbroad publication too easily risks release to the public. One protective mechanism several industries have already suggested is for DHS to notify submitters any time CII is to be released, for any purpose. Whatever the solution, if the private sector is to cooperate in correcting, updating, and otherwise improving such lists, it must be assured that such information truly will be protected and kept out of the hands of those who would do the nation harm.

Conclusion

The provision in the Interim Rule that requires CII – in order to be protected under the Critical Infrastructure Information provisions of the Homeland Security Act – to be submitted directly and solely to the DHS CII Program Office should be revised to more closely reflect the original proposal in the draft regulations permitting indirect submissions. This will enable the private sector to appropriately assist DHS in its mission by assembling information necessary to protect the nation's critical infrastructure, but

that should remain held in confidence in order to prevent its misuse by those who would do harm to the nation.

Respectfully submitted,

David K. Owens
Senior Vice President
Edison Electric Institute
701 Pennsylvania Ave., NW
Washington, DC 20004

202/508-500

From:
http://homeland.cq.com/hs/display.do?dockey=/cqonline/prod/data/docs/html/transcripts/congressional/108/congressionaltranscripts108-000001092550.html@transcripts&metapub=CQ-CONGTRANSCRIPTS&seqNum=1&searchIndex=0

In cooperation with our partners in the private sector and state and local governments, we have complied a list of 1,700 critical infrastructure and key assets that we are in the process of visiting and assessing the potential vulnerabilities, and we are doing that now. …

We must refine the list of national critical infrastructure and key assets, as you have said, Mr. Chairman. Ensuring private sector involvement in the work to do with identifying and providing protective measures to those critical infrastructure sites and sectors. …

To address these challenges, we work with or partners at state and local to refine the list of critical infrastructure. … We have identified overall in terms of the national facilities or infrastructure database about 28,000 sites or facilities. Of those, in working with state and local officials, we have for the next year identified 1,700 … .

[A] National Critical Infrastructure Program was established under … HSPD-7. It involves several key tenets [including to] identify and prioritize – keyword prioritize – the nation's critical assets and key resources … .

But what we're trying to do is get our head and arms around critical assets, identifying that which is truly central to that which we cannot afford to lose. Key critical infrastructure, key assets, the loss of which would be catastrophic, not just for a city or region but for the nation, and … we look at in terms of credibility and vulnerability loss of life, confidence with the American people. That starts to address the criteria that we look at when we, not separately but with private sector local and state authorities, ask ourselves what really is critical within the region, within the state, within the nation.

We don't do that alone.NOTE/ ... As I shared with you earlier, there are about 28,000 items of infrastructure on our database. We have chosen 1,700 to look at over the next year.

NOTE/

In addressing how the list was put together, Undersec. Lubutti noted the following:

ROGERS: General, in assembling the critical infrastructure inventory and threat assessment, an enormous undertaking, how are you going about doing that project? What's the procedure?

LIBUTTI: The procedure is to look at what across the country we believe, as I identified in the criteria, are truly critical... .

ROGERS: I know that, but what's the procedure? ...

LIBUTTI: ... We use the criteria. We talk to state and local officials and get their cut on what they believe is critical. We hold that up against the impact that together we believe has a national impact. I mean, that's how we come to grips with that. We send our team...

ROGERS: I'm looking for details. You're asking the states to assemble in their state a list, correct?

LIBUTTI: We're asking them to help us identify that which they believe is most critical within their state.

ROGERS: You're asking the states to do it?

LIBUTTI: Sir, we are taking the lead, and asking the states to help us.
…
ROGERS: So you're asking each of the 50 state governors and their ... their Homeland Security director to assemble a list in their state of what they consider to be critical infrastructure and assets.

LIBUTTI: Essentially, yes, sir.

ROGERS: Do you give them guidelines on what nationally you think they ought to be looking for?

LIBUTTI: Yes, sir. We do.

ROGERS: So that there would be some consistency then, nationally, so that they're looking for the same thing in each of their states?

LIBUTTI: Yes, sir. That's correct.

ROGERS: Are you asking them, then, to rate the degree of risk that each item is exposed to so that statewide there is some ranking of importance?

LIBUTTI: That is part of the dynamic of the process, absolutely. We do the same thing internally as well, in terms of talking to our federal partners and the other departments of government. I mean, Agriculture may bring something to the table, or Transportation may, which we hold up and give all due consideration to.

ROGERS: When you're asking the states to assemble a list, are you including in that list privately-owned assets as well?

LIBUTTI: Absolutely, sir.

ROGERS: So they're looking at federally-owned dams, state-owned whatever and locally-owned assets, as well as privately-owned?

LIBUTTI: Yes, sir. That's correct.
…
ROGERS: And what will you do with that information?

LIBUTTI: What we'll do with the data that is brought together is, again, working with the leadership that's helped us develop it is to try to prioritize those key sites that we believe run the highest risk of catastrophic failure and the following impact across the nation. We need their help as an advisory group to help us define that which is most critical. That process is reflected in the 1,700 sites we intend to visit this year.