

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

**PROCEDURES FOR HANDLING) 6 C.F.R. PART 29
CRITICAL INFRASTRUCTURE INFORMATION) RIN 1601-AA14**

**COMMENTS OF THE
NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL**

The North American Electric Reliability Council (“NERC”)¹ strongly supports the rulemaking initiative announced in the notice of proposed rulemaking issued by the Department of Homeland Security (“Department”) on April 15, 2003 (68 Federal Register pages 18524-29) to implement Section 214, Title II (the Critical Infrastructure Information Act of 2002), of the Homeland Security Act of 2002 (Pub.L. 107-296) (“the Act”). The Department proposes to establish for Federal agencies the uniform procedures to implement Section 214 of the Homeland Security Act regarding the receipt, care, and storage of Critical Infrastructure Information (“CII”) voluntarily submitted to the Federal government. NERC recommends one substantive change and suggests several technical clarifications or corrections.

Introduction

NERC is an “information sharing and analysis organization” within the meaning of Section 212 of the Homeland Security Act. NERC funds and administers the Electricity Sector Information Sharing and Analysis Center (“ES-ISAC”) and coordinates the activities of the Critical Infrastructure Protection Advisory Group (“CIPAG”), the electricity industry advisory group that provides guidance to the ES-ISAC. The electric infrastructure is critical and vital to our society. The utility participants of NERC and CIPAG have for decades involved themselves

¹ NERC is a not-for-profit corporation formed in response to the Northeast blackout in 1965 to promote the reliability of the bulk electric systems that serve North America. NERC’s mission is to ensure that the bulk electric system in North America is reliable, adequate, and secure. It works with all segments of the electric industry as well as customers to “keep the lights on” by developing and encouraging compliance with rules for the reliable operation and adequacy of supply of these systems, as well as to protect the security of the interconnected systems. NERC comprises ten Regional Reliability Councils that account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

in protecting the electric system. For the past two years, NERC and CIPAG have represented the interests of electric utility infrastructure owners and operators across all segments of the electric utility industry in seeking to create statutory protections for critical infrastructure information, as were ultimately embodied in Section 214 of the Homeland Security Act.

Summary

In general, we wish to express our appreciation for a strong, clear proposal that reflects the language and intent of Section 214 of the Act. NERC and the CIPAG 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. We believe that the proposed regulations create a strong foundation for building the necessary trust relationship.

In that light, we do have one major suggestion, as well as a few requests for further clarification. In particular, section 29.6(f) of the proposed regulations seems counterproductive and out of step with the remainder of the proposal. After discussing section 29.6(f), we will discuss those issues where additional clarification could be beneficial.

Recommendation: Delete section 29.6(f) or revise it such that all information submitted under protection of the Act is treated in the same manner.

Proposed section 29.6(f) would permit the CII 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 procedures," and release that information without prior notice to the submitter or an opportunity to contest the determination. The proposed regulations recognize that "[t]his is the only exception to the notice requirement of these procedures" (proposed section 29.6(f)). The provision also fails to set forth any standard by which the CII Program Manager could make such a determination.

This unbounded exception, even though only discretionary, is directly contrary to the spirit of cooperation intended to be fostered by the Act, and as reflected in the otherwise applicable notice provisions set forth in proposed section 29.6(e). Even if a standard by which

such a decision is to be made 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 determination of bad faith could wrongly make critical infrastructure information available to the public. Such a possibility may dissuade many private sector infrastructure owners and operators from making any voluntary submittal at all, and may 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 provides only one exception to the protection of voluntarily submitted CII for "bad faith." 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 litigation abuse, not a general principle to be implemented or applied by the Department. While we believe that the instances where a critical infrastructure owner or operator would actually submit any information in bad faith will be exceedingly rare, it is both unnecessary and possibly inappropriate for the Department, part of the Executive branch, to take on a role that 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.

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 completely modified to make it more closely conform to the statutory language. In addition, if the CII Program Manager is to be permitted to make a determination of bad faith, there should be a standard by which the Program 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 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 very complexity of the necessary modifications in itself indicates that the better course for the Department, as well as for potential submitters, is to remove section 29.6(f) from the final regulations.

Items for Further Clarification

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

2. Section 29.6(g) — Proposed section 29.6(g) states that only a CII Program Manager, or the Program Manager’s designee, may remove the protected status from CII material. However, that section does not set forth the circumstances under which such action may be taken. We suggest that this section be clarified to indicate that such action will only be taken at the written request of the originally submitting entity.

3. Section 29.7(e) — 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.

4. Section 29.8(f)(2) — 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 Department should be as sensitive to the need to protect CII as it is sensitive to the need to remedy violations of law or ethics.

Conclusion

NERC requests that proposed section 29.6(f) be removed from the final regulations (or at least modified as described above), and that proposed sections 29.6(d), 29.6(g), 29.7(e), and 29.8(f)(2) be clarified as described above. In general, we thank you for this meritorious proposal, as well as for the opportunity to submit comments. NERC will be pleased to work with the Department to further define the nature of information to be protected and effective measures for doing so.

Respectfully submitted,
**NORTH AMERICAN ELECTRIC
RELIABILITY COUNCIL**



David N. Cook
Vice President and General Counsel
North American Electric Reliability Council
116-390 Village Boulevard
Princeton, New Jersey 08540-5731
609.452.8060