

Information Technology Information Sharing and Analysis Center.txt

Subject: CORRECTED FILE ATTACHED- Ref: DHS- RIN 1601-AA14 - Comments by IT-ISAC
Date: Mon, 16 Jun 2003 19:31:43 -0400
From: "Sabo, John T" <John.T.Sabo@ca.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Two versions of IT-ISAC comments were inadvertently attached to the prior email sent at 7:20PM EDT in response to the NPRM. Please use the correct IT-ISAC comments file attached, and discard the earlier files.

Ref: DHS- RIN 1601-AA14

On behalf of the IT-ISAC, I am attaching comments of the Information Technology - Information Sharing and Analysis Center ("IT-ISAC") in the above captioned proceeding, related to Procedures for Handling Critical Infrastructure Information.

Respectfully,

John T. Sabo
Chair, IT-ISAC Policy Committee

<<ITISAC DHS- RIN 1601-AA14-FINAL-CORRECTED.doc>>

John T. Sabo
Manager, Security Privacy and Trust Initiatives
Computer Associates International
2291 Wood Oak Drive
Herndon, Virginia, 20171
USA
Phone: +1 703-708-3037
Mobile: +1 443-629-6198

Name: ITISAC DHS- RIN

1601-AA14-FINAL-CORRECTED.doc

ITISAC DHS- RIN 1601-AA14-FINAL-CORRECTED.doc

Type: WINWORD File
(application/msword)
Encoding: base64
Description: ITISAC DHS- RIN

1601-AA14-FINAL-CORRECTED.doc

COVER LETTER

SUBMITTED BY DATAGRAM: cii.regcomments@DHS.gov

Frank Nolan
Associate General Counsel (General Law)
Department of Homeland Security
Washington, D.C. 20528

Ref: DHS- RIN 1601-AA14
Notice of Proposed Rulemaking 68 F.R. 18524 15 April 2003
Procedures for Handling Critical Infrastructure Information

Sir:

Attached hereto please find the comments of the Information Technology - Information Sharing and Analysis Center ("IT-ISAC") in the above captioned proceeding.

Respectfully yours,

Miles McNamee,
President, IT-ISAC
(703) 747-4114
mmcnamee@bearingpoint.net

John T. Sabo
Chair, IT-ISAC Policy Committee
(703) 708-3037
john.t.sabo@ca.com

Mailing Address:
IT-ISAC
6303 Barfield Road
Atlanta, Georgia 30328

Before the United States Department of Homeland Security

Comments of the Information Technology)
Information Sharing and Analysis Center)
)
Notice of Proposed Rulemaking on Procedures)
For Handling Critical Infrastructure Information)
)
6 CFR Part 29 (RIN 1601-AA14))

I. Introduction

1. The Information Technology Information Sharing and Analysis Center ((IT-ISAC) is pleased to submit its comments in response to the Notice of Proposed Rulemaking published on 15 April 2003 (68 Fed Reg. 18524-29) (hereinafter “NPRM”) on behalf of the Department of Homeland Security (DHS), implementing Section 214 of Title II of the Homeland Security Act of 2002 (“HSA”) (Pub.L 107-296), the provisions commonly referred to as the Critical Infrastructure Information Act of 2002 (“CIIA”).

II. About the IT-ISAC

2. The IT-ISAC is a membership association, organized in 1999 as a LLC under the laws of the Commonwealth of Virginia, pursuant to a charge to critical infrastructure sectors from the White House at the time of the issuance of PDD 63 in 1998 to create industry-based bodies capable of providing timely information to government and other entities regarding vulnerabilities, threats, on-going attacks and remedies. The IT-ISAC’s members contribute dues to support the maintenance of the organization, which is led by a Board of Directors chosen from 14 founding member companies. The IT-ISAC’s day-to-day operations are managed by the ISS Company of Atlanta, Georgia under a renewable services contract. The IT-ISAC’s present membership includes a range of IT and IT security companies, including BearingPoint, Veridian, CSC, Symantec, Computer Associates, VeriSign, Microsoft, Cisco, Hewlett-Packard, Intel, IBM, and Oracle.

III. Background and Policy Context

3. As one of several operating ISACs actively engaged in sharing of critical infrastructure data, and one of the private sector instigators of Congress’ adoption of the CIIA, it is useful to place our comments on the proposed rules in context. We also believe our views are significant because of two other factors: (1) the early role IT-ISAC members played in advising the organizers of ISACs in many of the other critical infrastructure sectors, including transportation, oil and gas and financial services sectors, and (2) as a consequence of the emerging consensus that the IT sector, unique among all of the critical infrastructure sectors, plays an essential enabling role in the operations of

every other sector; our posture as the “feeder” technology upon which all other critical infrastructure technologies depend. This unique posture, both operationally and for information sharing exercises has been recognized in the PCCIP Report in 1997, the National Strategy to Secure Cyberspace, and the National Homeland Security Strategy, and is an element of the operational architecture of the DHS’ newly established National Cyber Security Division.

4. The IT-ISAC’s recognition of the responsibilities attendant to this important role, and the unique posture of information about threats and attacks against network assets under its ownership or custody led to early, active involvement in the evolving policy discussions regarding the architecture and rules governing information sharing mechanisms among members of the IT sector, between us and our customers, and between us and the Federal government.

5. At the time of the issuance of PDD 63¹ in 1998, the environment for such information sharing was quite different. While the potential terrorist threat to the nation’s infrastructure had long been the subject of analysis and more recently sharply profiled in the work of the President’s Commission², the looming event was the Year 2000 date rollover event, and significant IT sector assets were directed at that known vulnerability to the IT infrastructure.

6. Indeed, one significant policy element of the Y2K episode plays a seminal role in the development of the instant information sharing structure; the Year 2000 Information Readiness and Disclosure Act (“IRDA”)³ was the model on which elements of the Congressional progenitor of the CIIA, the “Davis –Moran” and “Bennett-Kyl” bills were based.⁴ The purpose of this legislation was to encourage reticent custodians of critical infrastructure assets to provide the government with timely information regarding Year 2000 date vulnerabilities, to provide opportunities for remediation of these system problems. A key element of this encouragement was a limited exclusion from exposure to FOIA release for qualifying data submissions.

7. Even prior to the galvanizing impact of the September 11 tragedies on our nation and on infrastructure custodians such as the IT-ISAC’s members, legislative and other policy proposals for the incorporation of mechanisms such as this to encourage information exchange were abundant, and debate in industry and government was extensive. Following September 11, a number of organizations have assumed the role of monitoring and reporting to the media and to the government on the posture of the critical infrastructure. Indeed, the wide spectrum of reliability and accuracy of the reporting and operational mode of these organizations is itself ample reason for careful regard to both

¹ Presidential Decision Directive 63, 22 May 1998.

² Critical Foundations, Protecting America’s Infrastructures. The Report of the President’s Commission on Critical Infrastructure Protection. GPO 1997.

³ 15 U.S.C. Sec. 1 {Note} Pub. L. No. 105-271 (October 19, 1998), 112 STAT. 2386.

⁴ Cyber Security Information Act, H.R. 2435, introduced July 10, 2001; see also Critical Infrastructure Information Security Act of 2001 “Bennett-Kyl”, S. 1456 107th Cong. 1st Session.

the statutory basis for critical infrastructure information exchange as reflected in the CIIA and in the instant regulatory proposal.

8. ISACs such as the IT-ISAC operate for the express purpose of engaging in exchange of CII. Accordingly, our “Raison d’être” and operational model are coincident; our objective is to strengthen the resilience and maintain the operational integrity of our nation’s infrastructure, both incorporating or dependant on information technology networks and related assets. Thus, we view with special interest these rules, which quite simply will define a substantial portion of how we operate.

IV. Summary of Comments

9. Our comments, which follow, are organized in sequential order following the draft regulation. Initially, we also make several observations regarding statutory sections which do not appear to be reflected in the draft regulations.

10. In general, our comments on the draft regulations reflect our belief that the essential purpose of these regulations, the Department’s supporting organizations, and indeed the statutory authority itself is to enable the prompt, effective sharing of information regarding attacks on the infrastructure and other significant events by Information Sharing organizations or others in possession of this information, and the subsequent dissemination of timely warnings by DHS or other appropriate agencies of government to the public or other communities of interest.

11. Overall, the IT-ISAC believes the regulations to be a faithful tracking of substantial elements of the statutory scheme of the CIIA. To the extent that our comments illuminate potential operational problems with the regulatory scheme, we look forward to the opportunity to provide advice and assistance as this rulemaking proceeding goes forward, and in otherwise advancing our supportive role to DHS in perfecting the draft.

12. The IT-ISAC does find, however, several departures from expected language and inconsistencies with our understanding of the legislative intent of the CIIA which may, in practice, produce difficulties in implementation, or, indeed, chilling of desired information sharing.

13. Among these are:

- our concern regarding §29.6(f) creation of an ad hoc evaluation of “good faith”;
- potential operational problems stemming from ambiguity regarding marking and acknowledgement of CII submissions in §§29.2(f), 29.3(a), 29.5(a)(3) and 29.6(g);
- the unbounded authority to grant access to Protected CII set out in §29.8(a), which the IT-ISAC believes should be deleted.

V. Section-by-Section Comment

A. Statutory provisions not reflected in draft regulations:

14. Appeal: The draft regulations do not address any administrative appeal within the DHS hierarchy, nor do they specify what must be assumed to be an available judicial appellate mechanism for an aggrieved submitter. Presumably, the statutory designation under § 213(2) of the DHS as a “covered Federal agency”, and the identification of the Secretary as the delegating official to designate the DHS IAIP under §29(5) as the “sole entity” for receipt of CII places the Secretary in the position as at least one level of administrative appeal from adverse actions under these regulations. Not only should this or any other intended administrative appellate remedy be specified, but also any presumed judicial remedy should, in our view, be clearly set out.
15. No waiver of privileges or protections: §214(a)(1)(F) of the statute provides that the voluntary submission of CII “...does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.” While §29(3) of the regulations provides detailed procedures for implementation of other limitations on ‘collateral use’ of CII, there is no clear enunciation of the protection set out in this statutory section or the Department’s intended procedures for its implementation. We believe it will be important to address this in a new regulatory section.

B. Draft regulations:

16. § 29.1(b) Scope- extended to “...Foreign...governments, and government authorities pursuant to their express agreements.” While it may be unarguably useful for these regulations to apply to address or limit the transmittal to or actions of foreign government entities with regard to protected CII, nowhere in the CIIA is there authority for such expansion, and the assertion of such scope in the absence of statutory, treaty or bilateral agreements to authorize or enable their effect could serve to void the section. IT-ISAC recommends editorial adjustment to make this section consistent with the present statutory grant of authority; as well as consideration of an amendment of the CIIA to address transfers of CII to foreign authorities. See also paragraph 31, regarding transmittal of CII to foreign governments.

17. 29(5)(b)(1) Indirect submission of CII. The final language of the CIIA leaves Section 212(2) and 212(7)'s designation of DHS as the sole "covered Federal agency." Nevertheless it is clear that mechanisms to accommodate other submissions of CII to other agencies, which will continue, and mechanisms to accord such data protected status are essential. Section 214(e)(2)(A) of the CIIA specifies 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." The proposed regulatory section conforms to this reality, and to Section 212(4)'s reference 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)."

18. §29.6 (b) Presumption of Protection. As presently drafted, this section reads "...information submitted...will be presumed to be treated as Protected CII..."

Whether a typo or not, the logic of this provision suggests that it be redrafted to insert the word AND, so as to read "will be presumed to be AND treated as...", thus asserting both the presumption of status as Protected CII by the DHS as well as the obligation to accord it appropriate treatment. Clarity in this section seems particularly important, since this provision in many ways is the lynch pin, setting out the primary custodial obligation of the DHS to CII data from the time of its submission.

19. §29.6(d)(3) A typographical error appears to exist in the enumeration of subsections; we believe these should be enumerated (1),(2),(3), rather than the present (1),(2),(1). A substantive issue also exists in this section with regard to acknowledgement of orally submitted CII. It is unclear when the Department's obligation of acknowledgement attaches: whether orally submitted data is to be acknowledged upon receipt, or whether it will be acknowledged only after the written follow up set out in 29.5(b)(3)(ii).

20. § 29.6(e)(1) and §29.7(d) Destruction of information. For consistency and clarity, the IT-ISAC believes the word "destroy" or derivatives should be substituted for "dispose" or derivatives in these sections. Since the Federal Records Act is cited, and "destruction" is a defined term in that statute, this usage will provide clearer indication of intent.

21. § 29.6(e)(1)(ii), in a related concern, the language should be adjusted to require the Program Manager, when determining information is not Protected CII, to notify any other government entity which may possess copies of that information and, if the submitter requests destruction, to require that entity to destroy that information. It may be that no such information exists, but the language of 29.5(d)(1) is not sufficiently clear in that regard.

22. §29.6(f) Determination of "bad faith." As drafted, this provision seems to allow the CII Program Manager to make a determination whether or not a CII submission is made "in good faith." The CHIA only provides one exception to the "good faith" language, and that is in the context of a **judicial** determination under Section 214 (a)(1)(C). The rationale for the inclusion of such a tool at the agency level is abundantly clear; the provision gives DHS a remedy against a party repetitively submitting information in bad faith solely to consume agency resources. In the IT-ISAC's view, concern that this section reflects an unauthorized departure from the statutory scheme can be solved by making clear that the exception does not apply if the information is in fact on its face Protected CII, by requiring minimal notice, and by providing a standard for good faith. Consistent with this concept, we suggest the following substitute language for the section:

29.6(f)

(1) In the event that the CII Program Manager determines that any information submitted (A) does not on its face qualify as Protected CII, and (B) was not submitted in good faith, because the character of the information submitted and circumstances of its submission preclude the possibility of it being protected as CII, the Program Manager shall notify the submitter that this section has been invoked.

(2) For any submission in which the he Program Manager has acted pursuant to clause (1) of this subsection, the Program Manager is not otherwise required to comply with the procedures of section 29.6(e). This is the only modification to the notice requirement of this subsection.

The IT-ISAC believes that inclusion of this approach would have the salutary benefit of setting out an administrative definition of "good faith."

23. § 29.6(g) Individuals authorized to remove protected status. This section provides that the Program Manager or his/her designee may remove the protected status of voluntarily submitted CII, but sets no standards for making such a determination. While the section's juxtaposition with the section authorizing determinations regarding "good faith" submission suggest a limited application of the authority (perhaps intended to apply ONLY to §29.6(f), in which case it should be redesignated as a subparagraph of that section), no such limitation or other qualification is set out in the section, which we strongly believe must be clarified.

24. § 29.7(e) Transmission of Information. As drafted, this provision seems to treat USPS first class mail as equally secure as registered or certified mail, as well as making it the equal of "secure electronic means". Since technology and recent legislative and regulatory practice in this area (e.g., the Y2K IRDA cited, supra.) provide for a range of secure electronic and paper transmittals of effective notice, the Department may wish to consider replacement of this language with a more generic approach, such as "reasonably secure means, to be designated by DHS."

25. §29.8(a) Authorization of access. The IT-ISAC believes this section should be stricken from the draft. The valid purposes for granting administrative access to Protected CII are enumerated in the subsequent paragraphs of §29.8. §29.8(a) appears on its face to authorize the grant of extraordinary access any circumstance; for example, to support a competitor (as this might support the promotion of trade, which is an "authorized government purpose"). Without the articulation of clear standards for the application of such broad administrative discretion, this section threatens to undermine the entire regulatory scheme.

26. § 29.8(f)(2) Whistleblowers. We believe that the "whistleblower" exception for subsequent dissemination of CII needs better definition; both as to the scope of coverage and as to the ends/purposes for which such information may be provided. Clear enumeration of proper "recipients" beyond the Inspector General appears appropriate.

27. §29.8(g)(1) FOIA requests. A procedure should be developed and the regulation adjusted to reflect the incorporation of notice to the submitter - without disclosing its identity to a requestor - if there is any FOIA proceeding (up to and including litigation), beyond the routine denial of an initial request for disclosure concerning the withholding of Protected CII.

28. §29.8(i) Use in Litigation. The phrase "for homeland security purposes" should be stricken, as it seems to invite litigation of the purpose of the submission, vitiating the presumption of validity in §29.6(b). The necessary requirements are already incorporated into the definition of "Protected CII" in §29.2(f).

29. § 29.8(j) Transmittals to Foreign Governments. Proposed section 29.8(j) appears to authorize the release of CII by the CII Program Manager 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 be made independently by the CII Program Manager. 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. In addition, the phrase "and under the same conditions" after the phrase "to the same extent" to make clear that all of the conditions of section 29.8(e) apply in releases by DHS to foreign governments under this section.

Information Technology - Information Sharing and Analysis Center

16 June 2003

Submitted on Behalf of the IT-ISAC By:

John T. Sabo, Chair
IT-ISAC Policy Committee
John.t.sabo@ca.com