

Douglas Kunze.txt

Subject: Comments on NPR 6 CFR 29 (72FR18524)
Date: Thu, 24 Apr 2003 08:30:42 -0400
From: "Doug Kunze" <drk@profsyseng.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>
CC: <responses@asisonline.org>

The attached file contains comments regarding an NPR that recently appeared in the Federal Register (72FR18524, April 15, 2003). The NPR deals with 6 CFR Part 29, Procedures for Handling Critical Infrastructure Information.

Thank you for the opportunity to provide my comments.

Douglas R. Kunze, CPP

Douglas Kunze <drk@profsyseng.com>
Director, Security Consulting Services
PSE, LLC

Douglas Kunze
Director, Security Consulting Services <drk@profsyseng.com>
PSE, LLC

Work Voice: 540.972.8048
Work Fax: 540.972.5459

Additional Information:
Version 2.1
Last Name Kunze
First Name Douglas
Revision 20030424T123042Z

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

REFERENCE: Federal Register
72FR18524 to 72FR18529
April 15, 2003

SUBJECT: Notice of Proposed Rule Making
6 CFR Part 29
Procedures for Handling Critical Infrastructure Information
Public Comments

Gentlemen:

The protection of information has been an important facet of the art of security since the establishment of the Fifth Profession in the earliest days of mankind. This protection is ever more important in today's security environment, especially information related to the protection of our critical infrastructures.

Two opposing ideas must be addressed by the proposed rule, protection of the information and its source, and timely dissemination of the information to entities required to protect the specific pieces and components of our infrastructures, especially the vast array of commercially and privately owned components.

COMMENT 1

The proposed rule, "establishes for Federal agencies the uniform procedures to implement" a program of protection for Critical Infrastructure Information (CII) that is voluntarily submitted to Federal agencies. In the second paragraph under **II. Notice of**

Proposed Rulemaking, it is stated that “These procedures apply to all Federal agencies” and to a list of other governments or government contractors. In the body of the proposed rule, at 29.2(d), a definition of an Information Sharing and Analysis Organization (ISAO) is provided. The definition “means any formal or informal entity or collaboration created or employed by public or private sector organizations” (emphasis added). There appears to be a conflict in applicability. The proposed rule is specific in its limited application to government. The definition implies that private sector organizations would also be regulated by this proposed rule.

These private sector organizations would be regulated if they collaborated for one or more of the following purposes:

- “Gathering and analyzing data to better understand security problems or interdependencies . . .to ensure the availability, integrity, and reliability” of the critical infrastructure
- “Communicating . . . CII to help prevent, detect, mitigate, or recover from the effects of a . . .problem”
- “Voluntarily disseminating CII to its members . . ., or any other entities that may be of assistance” in carrying out the above measures.

Such regulation is not in the scope of the proposed rule, as stated and should be struck. If such regulation were in the scope, it would place a blanket on such important organizations as ASIS International, a voluntary, member driven, organization of security managers with a long history of performing the tasks enumerated in the proposed rule, specifically for the purpose of protecting components of the critical infrastructures.

COMMENT 2

In **I. Background**, the proposed rule states “the Department relies upon the discretion of the submitter as to whether the volunteered information meets the definition of CII.” The proposed rule goes on to indicate in 29.2(f), and other paragraphs, that the CII Program

Manager may make a final decision that the information is not CII. The submitter has the expectation that the information and the submitter's identity will be protected. This apparent conflict should be resolved.

COMMENT 3

The proposed rule states, in 29.6(e), a process that must be followed by the CII Program Manager to notify the submitter of the determination and allow the submitter to provide additional justification. The stated provisions appear to be adequate.

COMMENT 4

Paragraph 29.4 establishes a management hierarchy, including the appointment of a CII Program Manager. One of the stated responsibilities of the CII Program Manager is to ensure that any "entity that works with Protected CII appoints one or more... CII Officer(s)." The CII Officer "shall be fully familiar with" the protective procedures established by the CII Program Manager. The definition of an ISAO, an entity, includes private sector organizations. Does this provision require private sector entities to employ a Federal government CII Officer? Who is responsible for the training of the CII Officer? What entity is responsible for the employment of the CII Officer? What entity is responsible for the cost of the CII Officer's program of responsibilities enumerated in the proposed rule?

COMMENT 5

Paragraph 29.5 designates the "DHS IAIP Directorate as the sole entity authorized to acknowledge and validate the receipt of Protected CII." "Information that is not submitted to the CII Program Manager.... will not qualify for protection under the CII Act of 2002." (29.5(c)) Further, if the information is submitted to a Federal agency, that agency "may not disseminate, distribute, or make public the information until the CII Program Manager has acknowledged and validated the information."(29.5(c)(2)) In the

event that CII is submitted to another Federal agency, the submitter must require the Federal agency, “pursuant to the submitter’s express direction,” to forward the information to the CII Program Manager. Using the definition of CII, it appears that the much of the voluntarily submitted CII will be time sensitive. What mechanisms will be used to expedite the acknowledgement, validation and dissemination of time sensitive information? Of other CII?

COMMENT 6

The proposed rule appears to intend that the CII Program Manager “validate” the content of the CII received (29.6(e)). However, throughout the proposed rule, it is noted that the CII Program Manager is the only entity to “acknowledge and validate the receipt” of CII. This language indicates that the CII Program Manager will validate the receipt, not the content of the CII (emphasis added). The proposed rule should be clarified.

COMMENT 7

Paragraph 29.5(b)(1-3) indicates that CII will be protected “only when” the information is forwarded to DHS “pursuant to the submitter’s express direction” and is marked in accordance with the Proposed Rule (29.5(b)(3)(i)). This provision could result in the submitter’s identity and the submitter’s information being disclosed to the public due to a procedural error on the part of the submitter. Paragraph 29.4(c) requires the appointment of knowledgeable CII Officers. An alternative is to have one or more CII Officers at Federal agencies with an assigned responsibility to make a preliminary decision regarding whether the submitted information contained CII, and a responsibility to forward all potential CII to the DHS CII Program Manager. In other words, make the receiving Federal agency responsible for forwarding the CII to the CII program Manager, not the submitter.

COMMENT 8

The proposed rule creates a new level of classification for information available within the government. Paragraph 29.7 creates new protection requirements for this new level of classification. DHS should look at the DOE protection requirements for UNCI or the NRC protection requirements for SGI. Both of these information protection programs deal with sensitive, unclassified information in various forms. Each of the programs could be used as a model for DHS and other Federal agencies CII protection programs. For example, the proposed rule requires that “(a)fter hours, Protected CII shall be stored in a secure container, such as a locked desk.” Other Federal information protection programs do not generally recognize a locked desk as a “secure container.”

COMMENT 9

Disclosure of or access to Protected CII should be limited to those with a need to know and who will not, overtly or covertly, disclose the information. Paragraph 29.8 sets the standard for need to know, but does not establish a standard for determining whether the recipient is sufficiently trustworthy and reliable to receive the CII.

COMMENT 10

Paragraph 29.3(c) restricts use of CII by Federal agencies. Specifically, a Federal agency “shall not utilize CII for regulatory purposes without the written consent of the submitter.” Is it the intent of the proposed rule to restrict the use of summary data or trend analysis? Federal agencies generally do not directly secure the infrastructure. Much of the protective action of Federal agencies is through protective regulations, which are based on information collection and dissemination, and law enforcement efforts.

COMMENT 11

The definition of CII contained in paragraph 29.2(b) includes records of past actions and incidents. The proposed rule requires CII be marked (29.6(c)) and stored (29.7(b)) in specific manners. It is suggested that DHS include an implementation period after the proposed rule becomes final to allow the retrieval, validation, marking, and storage of documents containing such past data.

Thank you for the opportunity to provide comments on the proposed rule. If you require additional information, I can be contacted at (540) 972-3093.

Sincerely,

Douglas R. Kunze, CPP

Cc: ASIS International at responses@asisonline.org