

Aerospace Industries Association.txt

Subject: AIA Comment to Proposed CII Rule RIN 1601-AA14

Date: Fri, 13 Jun 2003 14:39:00 -0400

From: "Jason Cervenak" <cervenak@aia-aerospace.org>

To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Attached, please find a copy of the Aerospace Industries Association's comments in response to the DHS proposed rulemaking for "Procedures for Handling Critical Information Infrastructure Information" 6 CFR Part 29 (RIN 1601-AA14). A hard copy of this letter is being mailed contemporaneously. Should you have any questions, please do not hesitate to contact me.

Jason Cervenak
Director, Intellectual Property and Industrial Security
Aerospace Industries Association
1000 Wilson Boulevard, Suite 1700
Arlington, VA 22209
ph - 703.358.1044
fx - 703.358.1144
email - cervenak@aia-aerospace.org

cii.pdf Name: cii.pdf
 Type: Acrobat (application/pdf)
 Encoding: base64
 Description: cii.pdf



June 13, 2003

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

Subject: Proposed Rulemaking for "Procedures for Handling Critical Infrastructure Information" 6 CFR Part 29 (RIN 1601-AA14).

Dear Sir:

The Aerospace Industries Association (AIA) appreciates the opportunity to provide comments in response to the Department's above referenced notice issued on April 15, 2003 (68 Fed.Reg. 18524-29) to implement Section 214 of the Homeland Security Act of 2002 (PL 107-296).

AIA represents over 230 of the nation's major manufacturers of commercial, military and business aircraft, helicopters, aircraft engines, missiles, spacecraft, materiel, ground and sea based military hardware, and related components and equipment. Together, our members' companies represent every facet of the aerospace industry. Additionally, and more importantly with regard to this matter, our member companies are the custodians of information related to the security of critical infrastructure or protected systems as defined by Section 212 of PL 107-296.

AIA appreciates the need for protecting our nation's critical infrastructure information (CII) and we fully realize that to do so, there needs to exist an open and unfettered communication structure in place between the private sector and the government; that communication structure depends upon both parties' confidence and trust in one another. While AIA believes that the proposed rule was drafted with the same spirit and intent of Section 214 of PL 107-296 and appreciates the Department's efforts to include industry in securing our homeland, there are areas that we would like to see clarified or modified to address industry's concerns. By addressing these concerns, the channels of communication would be more open and the proposed goal of protecting our nation's CII would be more fully accomplished. The underlying theme of our comments is that there needs to be adequate safeguards against both economic and physical liability and vulnerability in order for our members to be comfortable sharing critical infrastructure information with the Department.

Specific Comments to the Proposed Rule

1. In Section 29.1 we recommend adding the word "presumptive" to the third sentence so that it reads: "It is Department of Homeland Security (DHS) policy to encourage the voluntary

submission of *presumptive* CII by protecting that information from unauthorized disclosure to the fullest extent permitted by law.” By adding the word *presumptive*, it allows the submitter to be fully aware that the information voluntarily submitted may not meet the legal definition of “critical infrastructure information” as determined by the CII Program Manager.

2. In section 29.2, the term “debilitating impact” should be defined in detail so that the submitter has a point of reference to work from when submitting the *presumptive* CII to the Department. It is, or at least appears to be, apparent that CII is not intended to be another category of classified information, however, the term “debilitating impact” is an interesting corollary to the existing terms to assess the loss or compromise of information affecting our national security such as “damage”, “serious damage” and “exceptionally grave damage.” Not only would this clarification of the term aid submitters in knowing what exactly the Department is looking to receive, but it would also give the submitters greater guidance in their submissions to avoid a decision by the CII Program Manager that the submission does not meet the requirement for CII.

3. In Section 29.4, AIA is concerned that the use of a national level electronic database for CII as described by the section would presumably entail a large administrative bureaucracy unless the Department anticipates minimal voluntary submittals of *presumptive* CII from the private sector. The CIIMS appears to be more encumbering than the federal government imposes on a national level for the management of classified information. We are also troubled by a national database that centralizes the nation’s CII in a single location. Holding all of the nation’s CII in a single location would create a large security risk should individuals hostile to the nation’s homeland security interests inadvertently be granted access or surreptitiously gain access to such a database.

4. In Section 29.6, the determination that the information not deemed to be CII and was further not submitted in “good faith” lies exclusively with the CII Program Manager. While this exception is discretionary, it contradicts the spirit of cooperation between industry and the Department. In fact, this provision may very well have a chilling effect that would dissuade the private sector from submitting any information at all to the Department. More alarming is the provision that allows the CII Program Manager to make this determination without notifying the submitter. For these reasons, it is the recommendation of AIA that the paragraph be deleted. If it is not deleted, it should be altered in a way to make the process less worrisome to the submitters by putting in place adequate safeguards to ensure that the submitters are given proper notice and a right to appeal a determination by the CII Program Manager that information submitted was not in good faith.

Additionally, there should be a delineated standard using a set of established objective criteria that must be used by the CII Program Manager before he determines that submitted information was not done so in good faith. Once a determination is made by the CII Program Manager that information submitted was not in good faith, the submitter should be notified and granted a right to appeal the CII Program Manager’s decision prior to any release of the

submitter's data, either by submitting additional information that justifies its claim that the original information was in fact CII or by withdrawing and retracting the information.

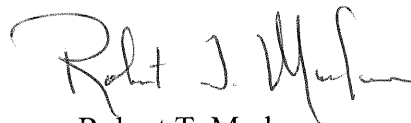
AIA fully realizes that this will create a more exhaustive evaluation process, but without the assurance of a fair and objective standard, industry is less likely to provide as much and as detailed information as possible. It is for this reason that the best course of action would be to delete the paragraph.

5. In Section 29.7, OMB Circular A-130 is a comprehensive requirements document for the protection of unclassified information. These requirements require security plans, risk analyses of the systems, training and other tasks. Implementation of the A-130 document for unclassified sensitive systems would incur significant cost to industry. Further, this requirement may not be achievable for some time at the state and local government level. We recommend that risk management principles be articulated rather than regulatory requirements.

6. In Section 29.8, CII is permitted to be transmitted to foreign governments without the written consent of the person or entity submitting such information to the same extent it may provide advisories, alerts, and warnings to other governmental entities as described in Sec. 29.8(e) of this chapter, or in furtherance of an investigation or the prosecution of a criminal act. While AIA understands the need for this type of exchange, industry will be reluctant to supply CII information to the Department without international government-to-government agreements in place to protect the transferred information.

Thank you for the opportunity to provide our comments. AIA would be pleased to provide subject matter experts to provide recommendations and suggestions to help foster dialogue between the Department and industry regarding these matters. If there are any questions concerning our comments on the proposed rule, please Contact Mr. Jason Cervenak, Director of Industrial Security at AIA. Mr. Cervenak can be reached at 703.358.1044. His email address is cervenak@aia-aerspace.org.

Sincerely,

A handwritten signature in dark ink, appearing to read "Robert T. Marlow". The signature is fluid and cursive, with the first name "Robert" being more prominent.

Robert T. Marlow
Vice President
Government Division