

From: Manja S. Sachet [mailto:manjas@u.washington.edu]
Sent: Thursday, May 20, 2004 4:34 PM
To: RegComments, CII
Subject: 6 CFR Part 29--Procedures for Handling Critical
InfrastructureInformation; Interim Rule

Comment:

This interim rule--establishing DHS policy and procedures for maintaining confidentiality of critical infrastructure information voluntarily submitted to the Department by private entities--is a thoughtful, balanced approach to the diverse needs of private business, government, and the public. The rule could, however, benefit from additional requirements in Section 29.5, Requirements for protection. Specifically, DHS should require a submitting entity to identify whether the CII is a trade secret, and should also identify the steps that the submitter itself takes to protect the CII, such as which types of individuals at the submitting entity have access to the CII, where the CII, if documented, is kept, etc. This type of information will better enable the Protected CII Program Manager to make more appropriate and accurate final decisions about whether to grant protected status to the CII.

In addition, I have reviewed public comments on the previous and present iterations of this rule. I share the concerns of commentators who critiqued the blanket protection against what seems to be all civil liability afforded to submitters of PCII. It is not necessary to provide such broad protections in order to encourage submissions of CII, and such broad protections could actually work against the public safety and interest. But this appears to be a matter to take up with Congress; the relevant provision appears in the Homeland Security Act of 2002 itself.

Thank you for your consideration.

Manja Sachet
2806 NW 68th Street
Seattle, WA 98117