



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

June 18, 2003

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

Subject: Notice of Proposed Rulemaking Implementing Section 214 of the
Homeland Security Act of 2002

Dear Sir/Madam:

The United States Department of the Treasury ("Treasury") is pleased to comment on the Department of Homeland Security's ("DHS") Notice of Proposed Rulemaking ("NPRM") implementing section 214 of the Homeland Security Act of 2002 (the "Act").

We strongly support the goals of the Act regarding the creation of a mechanism to voluntarily share information created in the private sector with the federal government. By fostering a climate where the private sector can work hand in hand with the public sector to share information regarding the Nation's critical infrastructure, the quality of the information received by the government can be greatly improved. This information will provide DHS with a critical new tool to protect not only the critical infrastructure of the United States, but also its citizens and to reduce the collateral damage the Nation and the economy may suffer as a result of an attack on the Nation's critical infrastructure. In addition, the Act will permit other agencies of the federal government, including Treasury, to foster a closer relationship with private industry to strengthen their ability to develop means to protect the Nation from terrorist attack.

I. Background

Treasury's interest in the NPRM stems, in part, from its continuing responsibilities under Presidential Decision Directive/NSC-63, "Critical Infrastructure Protection," dated May 22, 1998 ("PDD-63"). PDD-63 calls for a closely coordinated effort between government and the private sector to eliminate potential vulnerabilities to major sectors of the Nation's economy. PDD-63 identifies banking and finance as a major sector of the economy vulnerable to infrastructure attack. As part of the President's implementation scheme, PDD-63 designates Treasury as the lead agency for the banking and finance sector, and directs it to work with the private sector in addressing problems related to Critical Infrastructure Protection ("CIP"). PDD-63 also directs Treasury to focus on preventive measures as well as threat and crisis management.

Treasury has worked very closely with the banking and finance sector in exchanging information and in drafting a vulnerability assessment of the U.S. financial sector. Treasury also has worked and continues to work with the private sector to remediate any

identified vulnerabilities. Through its endeavors and based upon its longstanding expertise in developing policies and guidance for the financial services sector, Treasury has cultivated a positive and constructive working relationship with the providers of financial services in identifying and remedying infrastructure vulnerabilities.

Against this back drop, we offer the following comments for your consideration.

II. Comments

A. NPRM § 29.5 – Authority to Receive Critical Infrastructure Information (“CII”)

As a matter of policy, Treasury strongly supports NPRM § 29.5, which provides that CII shall receive the protections of section 214 of the Act, if such information is voluntarily submitted indirectly to DHS through a federal agency.

This provision will enhance Treasury’s ability to carry out its lead agency responsibilities under PDD-63. Historically, the banking and finance sector has been hesitant to release certain CII to Treasury because Treasury may be required to disclose such CII in response to a request made by a third party under the Freedom of Information Act. This hesitancy has complicated Treasury’s ability to work cooperatively with the sector in addressing problems related to CIP. NPRM § 29.5 removes the basis for any such tentativeness on the part of the organizations that comprise this sector, and will thus enhance Treasury’s ability to fulfill its responsibilities under PDD-63.

Treasury believes that NPRM § 29.5 also will enable DHS to make better use of CII and act more nimbly under section 214(a) of the Act if the financial services sector can voluntarily submit CII to DHS through Treasury with the full section 214 protections. Specifically, Treasury’s direct receipt of CII will immediately enable it to apply its expertise in not only analyzing and assessing such CII, but also identifying potential countermeasures that reduce vulnerabilities. As a result of working with the sector and its intimate knowledge of the workings of the financial markets in the United States (U.S.) and abroad, Treasury can aid DHS in its mission by using its resources and knowledge base to identify vulnerabilities that may be contained in the CII.

Once the CII has been analyzed, Treasury will promptly share its findings and propose countermeasures to DHS so that DHS could, as appropriate, issue notices and warnings related to the protection of the critical infrastructure in accordance with section 214(e)(2)(D) of the Act and NPRM § 29.7(e). As a result, Treasury believes that NPRM § 29.5 will enable DHS and the federal government, as a whole, to use its resources more efficiently by allowing departments and agencies that have specialized knowledge to immediately use their knowledge in protecting the Nation.

B. Points of Clarification

Treasury believes that the NPRM is well-reasoned and clear. There are, however, certain provisions that DHS may wish to clarify either in the regulation or in the preamble to the (interim) final rule.

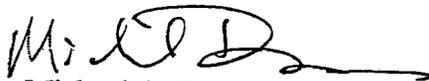
First, NPRM § 29.5(d)(2) provides that a federal agency forwarding CII to DHS “may not disseminate, distribute, or make public the information until [DHS] has notified the agency . . . that [DHS] has acknowledged and validated the information” pursuant to NPRM § 29.6. It is not clear whether the prohibition on dissemination and distribution extends to intra-agency dissemination and distribution. For example, if Treasury’s CII Officer receives CII from a submitter, can that Officer disseminate and distribute such CII internally for use consistent with PDD-63 before DHS acknowledges and validates the information? Treasury believes that the answer should be in the affirmative. Moreover, NPRM § 29.5(d)(2) could be construed as authorizing an agency to make public the CII, including protected CII, once DHS acknowledges and validates the information. It does not appear that this is DHS’ intent given NPRM § 29.8, which plainly restricts access to and disclosure of protected CII.

Second, NPRM § 29.7(e) prescribes the means by which protected CII can be transmitted. The means of delivery are restricted to U.S. first class, express, certified, or registered mail, and secure electronic means. DHS may wish to consider adding hand delivery given the fact that in certain instances it may be the swiftest and most secure means of transmission. Alternatively, DHS may wish to consider a more flexible approach by revising subsection (e) to reference transmission through such means contained in guidelines to be issued by the CII Program Manager or the Program Manager’s designee. This alternative would allow DHS to modify the methods that may be used to transmit CII without having to revise the regulation.

Third, NPRM § 29.8(c) authorizes the disclosure of protected CII to federal contractors after a CII Officer certifies that the contractor is performing services “in support of the purposes of DHS.” It appears that the intent underlying this section could be better accomplished by replacing “in support of the purposes of DHS” with “in support of the purposes described in § 29.2(h).” This suggested revision mirrors language contained in NPRM § 29.8(f)(2).

We hope these comments are helpful. If we can be of further assistance, please do not hesitate to contact us.

Sincerely,



Michael A. Dawson
Deputy Assistant Secretary
Critical Infrastructure Protection and
Compliance Policy