



CUNA & Affiliates
A Member of the Credit Union System

**Credit Union
National Association, Inc.**

601 Pennsylvania Ave. NW, South Bldg.
Suite 600
Washington, D.C.
20004-2601

Telephone:
(202) 638-5777
Fax:
(202) 638-7734

Web Site:
www.cuna.org

May 20, 2004

Janice Pesyna
Office of the General Counsel
Department of Homeland Security
Washington, D.C. 20528

Via E-mail: cii.regcomments@DHS.gov

Re.: Procedures for Handling Critical Infrastructure Information

To Whom It May Concern:

The Credit Union National Association (CUNA) is pleased to provide comments to the Department of Homeland Security (DHS) on the agency's interim rule regarding the receipt, care and storage of critical infrastructure information (CII) voluntarily submitted to the federal government through DHS by credit unions and other private sector entities. By way of background, CUNA is the largest credit union trade association, representing more than 90% of our nation's nearly 9,800 state and federal credit unions.

SUMMARY OF CUNA'S POSITION

- Credit unions want to continue their efforts to ensure CII is properly held, including partnering with the government by participating in the Protected CII Program. However, this interim rule should be modified to provide greater assurance to credit unions and other private sector entities submitting CII that their submissions will remain appropriately protected from unauthorized disclosure and only shared with other agencies and jurisdictions in a manner that preserves that confidentiality.
- DHS should publicize the Protected CII Program so that credit unions and other private sector entities understand what type of information DHS is seeking under the Program.



AMERICA'S
CREDIT UNIONS™

- The penalty sections should be modified to address what penalties apply if a third party recipient of information from DHS who is not an officer/employee of the U.S. government discloses that information in an unauthorized manner. In addition, the penalty sections should state that DHS will compensate private sector entities that incur losses as a result of disclosure of CII that they voluntarily submit.
- CUNA is concerned about the potential decrease in the coordination and control of CII if multiple agencies are involved in the collection of CII that they subsequently submit to DHS.
- The interim rule should clarify that an individual or entity making a voluntary submission that is later determined not to be Protected CII by DHS should not be held responsible; further, that information should still be handled in a confidential manner by DHS.

CUNA'S VIEWS

Section 214 of the Homeland Security Act of 2002 (Act), commonly referred to as the Critical Infrastructure Information Act of 2002 (CII Act), establishes a program that protects from disclosure to the general public any CII that is voluntarily provided to DHS. A strong network of public-private partnership arrangements is critical to the success of the Protected CII Program in order to safeguard our nation's vast critical infrastructure. This interim rule is significant because it provides DHS with the framework necessary to receive CII and protect it from disclosure to the general public.

We understand that one of the primary purposes underlying this interim rule is to enable DHS to use information obtained from individual private sector entities, combined with those from other entities, to create a broad perspective from which the government at various levels and private sector entities can gain a better understanding of "how to design and develop structures and improvements to strengthen and defend those infrastructure vulnerabilities from future attacks." CUNA and credit unions share this goal. Credit unions want to continue to do their part to assist in the war against terror and protect national security. In fact, CUNA is a founding member of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, a group of financial institution and other organizations that work with the U.S. Treasury Department to ensure the financial sector is doing what it can to prepare for and respond to terrorist activity.

In our view, for the Protected CII Program to be as effective as possible, the interim rule should be strengthened to provide greater assurance to the volunteer private sector entities submitting CII that their submissions will be beneficial to homeland security efforts, kept secure and confidential, and shared with other agencies and jurisdictions in a manner that preserves that confidentiality. In order to provide greater assurance to private sector entities, the interim rule should contain standards and procedures that DHS and any party to whom the information may be disclosed or redisclosed will follow to preserve the security and confidentiality of CII.

The interim rule indicates that CII covers vital physical or computer-based systems and assets, the incapacitation or destruction of which would have a debilitating impact on national security, national economic security, and national public health and safety, and way of life. That is an extremely broad definition. It is unclear as to what specific type of information might qualify as Protected CII under the interim rule. Credit unions and other financial institutions need more guidance about the types of information or the various scenarios that might arise where DHS would like a financial institution to submit information under this rule. Those examples should provide specific ideas about what might need to be done in response to certain types of information – such as when DHS might issue a warning to other financial institutions or when DHS might want to work with other agencies to provide a solution to a particular vulnerability. There is also some confusion about how this rule relates to the rules of the Office of Foreign Assets Control (OFAC). We recommend that DHS work with the Treasury Department to clarify this issue.

The interim rule states that “Information submitted to any other Federal agency pursuant to a Federal legal requirement is not to be marked as submitted or protected under the CII Act of 2002 or otherwise afforded the protection of the CII Act of 2002, provided, however, that such information, if it is separately submitted to DHS pursuant to these procedures, may upon submission to DHS be marked as protected CII or otherwise afforded the protections of the CII Act of 2002.” It is unclear from this language if an entity legally required to be submit CII to another federal agency would be able to circumvent the right of a party to access those records via the Freedom of Information Act (FOIA) request process by submitting that information to DHS under separate cover to qualify as Protected CII. The final rule should clarify this is not DHS’ intent.

CUNA suggests that DHS create model forms, including instructions and all the necessary disclosures, for submitters to use to reduce the potential for confusion as to whether the information is properly submitted so as to be accorded the protections of the CII Act.

CUNA believes that private sector entities should have the ability to be more involved in the disclosure determination process than the interim rule currently allows. The interim rule provides in Section 29.8(a) that “[t]he Under Secretary for IAIP [Information Analysis and Infrastructure Protection], or the Under Secretary’s designee, may choose to provide or authorize access to Protected CII when it is determined that this access supports a lawful and unauthorized Government purpose as enumerated in the CII Act of 2002, other law, regulation, or legal authority.” This is very expansive disclosure authority for DHS; and there is no provision for submitter participation in the process. Further, the Supplementary Information section of the interim rule states, “The Department [of Homeland Security] does agree that further disclosure of information beyond those entities or individuals that have entered into a formal agreement with the Department may require the permission of the submitter.” We very much agree with this position and urge DHS to codify it in the final rule. It is important that DHS develop standards on the disclosure determination process with input from private sector entities and that those standards are published.

There are two aspects of the penalties sections of the interim rule that we believe should be modified. First, if DHS discloses Protected CII to a third party not an officer or employee of the U.S. government, it is unclear what penalties apply if that third party discloses that information in an unauthorized manner. Second, in order to establish a robust Protected CII Program that encourages voluntary submissions, we recommend that the interim rule contain a provision requiring DHS to compensate private sector submitters for any losses resulting from any disclosure of that Protected CII.

CUNA is concerned about the provision enabling federal government agencies other than DHS acting as conduits for submission of CII to DHS, also known as indirect submissions. We are concerned about the potential decrease in coordination and control of CII that may result if multiple agencies are involved in the front-end collection of CII. The federal agency acting as a conduit should know precisely what procedures they are to follow. For indirect submissions, there should be an agreement under which the federal agency promises not to share the information with any entity except DHS, unless the submitter signs a written authorization.

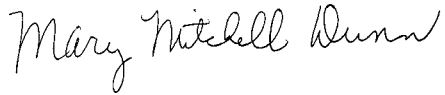
We suggest that Section 29.6 (Acknowledgement of Receipt, Validation, and Marking) more explicitly spell out that if a submission is determined not to be Protected CII that the submitter is not responsible and the information will still be handled by DHS in a confidential manner. Treating the information otherwise could not only put the submitter in a compromising position but could adversely impact the credibility of the individual and/or entity making the submission in an effort to assist DHS in its important mission. In addition, under the interim rule if the Protected Program Manager or the Manager's designee(s) makes an initial determination that the information submitted does not meet the requirements for protection under the CII Act, they must notify the submitter of that initial determination. It would be helpful if the notification included the reason underlying that determination. That way, submitters could make an informed decision regarding whether they should resubmit the information with an explanation of why it should qualify as Protected CII or whether they should withdraw the request. Further, the explanation as to why the information submitted does not meet the requirements would be helpful for submitters to understand more precisely what sort of information the DHS is seeking and provide information that would meet the requirements in the future.

Conclusion

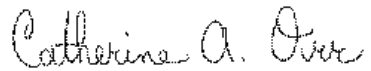
In conclusion, we support the efforts of DHS to make this country as secure as possible, including the vital critical infrastructure system through this interim rule. We believe that the changes to the interim rule as suggested above will facilitate the success of this important DHS program. Credit unions and other private sector entities already share CII with their regulators and information sharing and analysis organizations (ISAOs) as well as information sharing and analysis centers (ISACs). We urge DHS to coordinate with such organizations in developing its CII Program.

Thank you for the opportunity to share our comments, and we hope our letter helps your process. If you have questions about this letter, please feel free to contact me or Senior Regulatory Counsel Catherine Orr at (202) 638-5777.

Sincerely,

A handwritten signature in cursive script that reads "Mary Mitchell Dunn".

Mary Mitchell Dunn
Associate General Counsel and Senior Vice President

A handwritten signature in cursive script that reads "Catherine A. Orr".

Catherine A. Orr
Senior Regulatory Counsel