

Office of the President

PO Box 3000 • Merrifield VA • 22119-3000

May 5, 2004

Ms. Janice Pesyna
Office of the General Counsel
Department of Homeland Security
Washington, DC 20528

Re: RIN 1601-AA14

Dear Ms. Pesyna:

Navy Federal Credit Union provides the following comments in response to the Department of Homeland Security's (DHS) interim rule and request for comments on 6 CFR Part 29, *Protected Critical Infrastructure Information*. We serve the financial needs of Department of Navy personnel and their dependents in every state and in many locations overseas. Navy Federal is the nation's largest natural person credit union with over \$21 billion in assets and 2.4 million members.

Homeland security is vitally important to Navy Federal's mission and to the future of our nation. We understand the vision of Congress embodied in *The Homeland Security Act of 2002* (Act) that homeland security programs should include partnership arrangements between the public and private sectors. A successful program involving the protection of critical infrastructure information would be no exception. The Act serves as a solid foundation for homeland security programs. However, as programs are implemented and tested, DHS in the spirit of public and private cooperation, should not hesitate to request additional authorities from Congress as needs arise. While the Act provides flexibility for homeland security programs, some of our comments may require additional statutory authority.

Section 29.1 of 12 CFR Part 29 purports to implement "section 214 of Title II, Subtitle B, of the Homeland Security Act of 2002 through the establishment of uniform procedures for the receipt, care, and storage of critical infrastructure information (CII) voluntarily submitted to the Federal government . . ." Navy Federal strongly agrees with Congress that this program should be voluntary and based in public-private partnerships. We are very familiar with voluntarism. Our board of directors is comprised of unpaid volunteers elected from our membership. Other credit union volunteers assist with supervision and oversight activities. Navy Federal and other credit unions actively promote and encourage their members and employees to volunteer their time and resources to improve their communities and strengthen our nation. Credit unions have a long and rich tradition of volunteerism. However, DHS's interim rule, *Protected Critical Infrastructure Information*, does little to promote or encourage a public-private partnership culture that is dependent on voluntary CII submissions by private sector entities.

Ms. Janice Pesyna
Page 2
May 5, 2004

We believe that, if the CII program is to be effective, DHS must greatly strengthen the protections afforded by its interim rule to assure its volunteer partners that submissions will be secure and appropriately confidential; useful to homeland security efforts; and shared with other agencies and jurisdictions only in a manner that preserves information security, confidentiality, and integrity. Failure to provide adequate assurances to all partners in the CII program would likely lead to mediocrity, at best, and possibly result in future mandatory CII submissions that could destroy the potential for developing strong public-private partnerships. Traditionally, Government agencies have been reluctant to codify self-governance. Notwithstanding, we believe that for the CII program, DHS must codify self-governing procedures and standards to provide its private sector partners assurances that the program preserves information security, confidentiality, and integrity.

By definition, CII documents the vulnerabilities and weaknesses of its provider. The information may be highly sensitive in the competitive marketplace. It may also contain the essential ingredients for quality of life, or even life itself, for hundreds or thousands of persons. As such, we believe CII must be the subject of a comprehensive and detailed program that assures voluntary participants that their individual information will be useful and completely safeguarded against misuse and abuse of any kind. The interim rule does little to provide such assurances. For example, Section 29.8(a) provides that DHS may disclose CII to any person or entity "when it is determined [by DHS' Under Secretary for IAIP, or the Under Secretary's designee] that this access supports a lawful and authorized Government purpose as enumerated in the CII Act of 2002, **other law, regulation, or legal authority.**" (emphasis added) In the absence of binding standards for disclosure or access, the very lifeline of the private sector information submitter is in the hands of the Under Secretary for IAIP. The private sector partner has no input in the disclosure determination and is not even aware of any standards employed in the decision process. We strongly encourage DHS to involve its partners in the process.

Penalties enumerated in the interim final rule illustrate the one-sided approach to partnerships envisioned by DHS. Section 29.9(d) provides that an officer or employee of the United States who knowingly discloses unauthorized CII may be imprisoned for not more than one year. It is unclear whether the penalty applies to third parties after DHS discloses the information to them. There is no stated penalty in the interim regulation for unauthorized disclosures resulting from incompetence or mismanagement. In contrast, however, Section 29.5(e) subjects "any false representation" of volunteer partners/submitters to 18 U.S.C. 1001 and its provisions for imprisonment of up to five years. Additionally, the interim rule exercises little or no jurisdiction over the security, confidentiality, and integrity of the information after it has been disclosed to third parties such as state or local governmental units. As an incentive to establish a solid CII program, we believe DHS should be required to compensate private sector partners for any losses resulting from any disclosure of any information obtained in connection with the CII program.

Ms. Janice Pesyna

Page 3

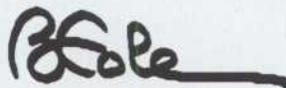
May 5, 2004

We understand that 6 CFR Part 29, *Protected Critical Infrastructure Information*, is intended to implement only Section 214, *Protection of Voluntarily Shared Critical Infrastructure Information*, of the Act. However, to fully evaluate CII protections within a framework of public-private partnerships, the entire CII program should be made available for review and comment. As a minimum, the CII program should fully address the following basic questions: What information does DHS need? How will DHS protect the information and assure its confidentiality both before and after it is shared with other agencies and jurisdictions? How will DHS use the information? It should also address the provisions of other sections of Title II, *Information Analysis and Infrastructure Protection*, particularly Sections 201 through 225 and the relationship of the CII program to the provisions of Title VIII, Subtitle I, *Information Sharing* (Sections 891 through 899). Rules promulgated to implement these additional sections of the Act may have a direct bearing on the adequacy of the interim rule that implements Section 214. We urge DHS to propose rules for public comment on all aspects of its CII program.

In the absence of incentives to establish true public-private partnerships involving the sharing, control, subsequent disclosure, and use of CII, we believe other groups such as information sharing and analysis organizations (ISAO) and information sharing and analysis centers (ISAC) will likely play pivotal roles in aggregating and analyzing infrastructure information in support of homeland security. The Act and the interim final rule acknowledge potential roles for ISAOs while *Presidential Decision Directive 63* (PDD-63) and the Presidentially sanctioned *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* stress the roles of ISACs in the nation's overall infrastructure protection strategies. Inadequate DHS assurances of the security, confidentiality, and integrity of CII at all levels will likely turn concerned private sector entities to ISAOs and ISACs for those assurances. We believe DHS should fully investigate the roles of ISAOs and ISACs in the CII program for homeland security and use them to the fullest extent practical as the voluntary sources of CII.

Navy Federal appreciates the opportunity to respond to the Department of Homeland Security's request for comments on provisions of its interim rule, *Protected Critical Infrastructure Information* (6 CFR Part 29).

Sincerely,



Brady Cole
Acting President/CEO

BC/bb