



DALE L. LEIGHTY
Chairman
DAVID HAYES
Chairman-Elect
TERRY JORDE
Vice Chairman
AYDEN R. LEE JR.
Treasurer
GEORGE G. ANDREWS
Secretary
C.R. CLOUTIER
Immediate Past Chairman

CAMDEN R. FINE
President and CEO

May 20, 2004

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

Re: Procedures for Handling Critical Infrastructure Information

Dear Ms. Pesyna:

The Independent Community Bankers of America (ICBA)¹ appreciates the opportunity to comment on procedures to implement section 214 of the Homeland Security Act of 2002 regarding the receipt, care, and storage of critical infrastructure information voluntarily submitted to the Department of Homeland Security (DHS). With the private sector owning 85% of the nation's critical infrastructure, the new procedures would increase communication and confidence between these entities and the federal agencies.

Overview

The ICBA supports the Department's proactive measures to obtain information regarding security threats and vulnerabilities by allowing organizations to voluntarily submit information used for the safety of critical infrastructure with an express statement noting that information is offered willingly, in expectation of protection from disclosure under the Critical Infrastructure Information Act of 2002. The key to the Protecting Critical Infrastructure Information (PCII) program lies in the confidentiality agreement between the private and public sectors and the non-disclosure of the information provided. Information is only used in the defense of the country and shared only with federal, state and local law enforcement. Furthermore, submitted information is not subject to Freedom of Information Act (FOIA) requests or disclosure without the express written consent of the submitter.

¹ ICBA represents the largest constituency of community banks in the nation and is dedicated exclusively to protecting the interests of the community banking industry. We aggregate the power of our members to provide a voice for community banking interests in Washington, resources to enhance community bank education and marketability, and profitability options to help community banks compete in an ever-changing marketplace.

Upon ratification of the Critical Infrastructure Information Act of 2002, the financial services sector became one of the 13 critical infrastructures of the United States. Additionally, Information Sharing Analysis Organizations (ISAO) were created. Entities such as these have enabled financial institutions to better communicate physical and cyber threats and computer vulnerabilities throughout the industry. The ICBA has enjoyed membership in the Financial Services Information Sharing and Analysis Center (FS/ISAC) for one year. Whereas ISAOs are government-created, further clarification is needed to determine whether information submitted anonymously to these organizations should be considered under PCII rules. It could be construed that by signing the membership agreement and adhering to the rules set forth by the ISAO, information has been voluntarily submitted for the security of the sector and stated implicitly. The ICBA contends that information provided to ISAOs should be utilized by DHS under PCII protection.

How PCII Affects Community Banks

ICBA members hold over \$728 billion in assets, a total number roughly \$300 billion less than three individual financial institutions with assets of about \$1 trillion. Accordingly, a single physical or cyber threat or incident that occurs against one community bank will not have as much impact as collective threats to specific areas or on a national scale. Were the latter to happen, a greater economic impact would be felt throughout the industry. Although smaller in asset size and in overall impact on the critical infrastructure, physical or cyber issues could deeply affect the people served by community banks.

Methods of Communication. Initially, it appears there are three different ways for community banks to communicate threats to authorities and for this reason, more clarification is requested. Threats could be assessed by DHS under the PCII program were banks to report suspicious activity directly to the agency. Community banks could also contact ICBA who, in turn, would forward the information to DHS. ICBA could additionally submit information to the FS/ISAC who would act as a conduit between the association and agency. This raises the question, though, of whether information submitted to an ISAO is protected information. Because Presidential Directives created ISAOs, submitting critical infrastructure information to a government entity such as the FS/ISAC might be protected, that is *if* ISAOs are considered government entities and not simply private companies. Clarification is needed regarding steps that must be taken to ensure confidentiality when information is submitted to DHS through an ISAO. For example, must the original submitter provide the “express statement” required by §29.5(a)(3) or may the ISAO provide it?

Turnaround Time for Processing Information. The ICBA is concerned with the amount of time it takes for submitted information to become protected under PCII rules. Without any public knowledge of timetables, the amount of time it takes for DHS to obtain information, process it, review the express statement requesting confidentiality, and declare it eligible under PCII is unknown currently. Additionally, were banks to utilize conduits such as ISAOs and trade associations – ICBA, for example – the process may be further slowed. ICBA believes that the most effective and efficient way for

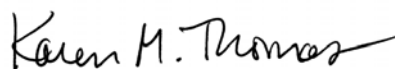
organizations to submit information is to contact DHS directly; however, if the other options described above exist, ICBA would partake in the process.

Information on a Need-to-Know Basis. Lastly, members of ICBA are interested in understanding whether there is an issue between information submitted to the FS/ISAC, which remains confidential, and DHS' "need-to-know" regarding information pertinent to national security. The FS/ISAC keeps anonymous from other members the name of the financial institution that reports threats or incidents specific to it (for example, a typical incident report might read, "Medium-Size FS/ISAC Member Institution Has Network Hacked"). However, maintaining the anonymity of the provider of the information could hamper DHS' ability to follow up on the threat. It appears to be in the best interest of all involved to submit the information to DHS due to its nature. ICBA suggests that ISAOs such as the FS/ISAC create a form for threats, alerts and incidents provided by members that will enable them to remain anonymous to other ISAO members, but enable information to be affiliated with its source for use under PCII and DHS.

Conclusion

The PCII program acts as a preventive step to ensure the security of our nation by opening the channels of communication between the public and private sector. The program enables private entities to voluntarily submit information to protect our nation's critical infrastructure. ICBA fully supports the Department of Homeland Security's efforts and looks forward to working with this and other federal agencies in the future. Thank you for the opportunity to comment. If you have any questions or need any additional information, please contact Matt Dellon, ICBA's Homeland Security Coordinator at 202-659-8111 or matt.dellon@icba.org.

Sincerely,



Karen M. Thomas
Executive Vice President
Director, Regulatory Relations Group